Bundessteuerberaterkammer
KÖRPERSCHAFT DES ÖFFENTLICHEN RECHTS

DEUTSCHER
STEUERBERATER-
VERBAND e.V.

Hinweise

für den Umgang mit personenbezogenen Daten durch Steuerberater und Steuerberatungsgesellschaften

Stand: April 2018

Inhalt

Checkliste:
Die wichtigsten To-Do‘s zur Umsetzung der DSGVO in Steuerberatungskanzleien

To-Do	**Gliederungs-ziffer**
Prüfen, ob Datenschutzbeauftragter (DSB) erforderlich ist	10.2.1
falls DSB erforderlich: Bestellung eines fachkundigen DSB	10.2.2 bis 10.2.4
falls DSB erforderlich: Meldung und Veröffentlichung der Kontaktdaten des DSB	10.2.5
Verarbeitungsverzeichnis erstellen	10.3.4
Prüfung und erforderlichenfalls Anpassung einer hinreichenden Datenschutzorganisation in der Kanzlei	10.1 bis 10.3.6
Datenschutzmanagement einrichten, Verantwortlichkeiten der Kanzleiangehörigen definieren und dokumentieren	10.3 bis 10.3.2
Prüfung der Schutzmaßnahmen; soweit nicht ausreichend vorhanden: Schutzmaßnahmen einschließlich Verschlüsselungsverfahren und sichere Password-Verfahren einrichten und dokumentieren	12.1 bis 12.4
Einhaltung des Datenschutzes auf Internetseiten prüfen und erforderlichenfalls anpassen	6.7
Dokumentation der Datenverarbeitungsgrundsätze und Schutzmaßnahmen	4. und 10.3.4
Auftragsverarbeitungsverträge mit Dienstleistern auf Vollständigkeit prüfen und erforderlichenfalls anpassen	7.1 bis 7.1.6
Verfahren zur Erfüllung der Informationspflichten einrichten und dokumentieren	9.1 bis 9.1.4
Verfahren zur Erfüllung der Auskunfts- und sonstigen Betroffenenrechte einrichten und dokumentieren	9.3 bis 9.9
Schulungsmaßnahmen einrichten und dokumentieren	10.3.3
Prüfen und dokumentieren, ob Datenschutz-Folgenabschätzung erforderlich ist	10.3.6
Meldeprozess von Datenschutzverletzungen vorbereiten und dokumentieren	11.1 bis 11.3
Aufbewahrungs- und Löschkonzept einrichten und dokumentieren	13.2

1. Einleitung

Die ab dem 25. Mai 2018 geltende Datenschutz-Grundverordnung (DSGVO) der Europäischen Union (EU) stellt neue Herausforderungen an den Umgang mit personenbezogenen Daten. Um dem Berufsstand der Steuerberater eine praxisgerechte Umstellung auf die neuen Vorschriften zu ermöglichen, entwickeln die Bundessteuerberaterkammer (BStBK) und der Deutsche Steuerberaterverband e.V. (DStV) gemeinsame Praxishilfen, die insbesondere den kleinen und mittelständischen Kanzleien bei der Organisation ihrer datenschutzrelevanten Arbeitsprozesse helfen sollen. Hierzu zählen auch die vorliegenden Hinweise für den Umgang mit personenbezogenen Daten durch Steuerberater und Steuerberatungsgesellschaften.

Die DSGVO ist ab dem 25. Mai 2018 unmittelbar und vorrangig zu allen nationalen Regelungen anwendbar, soweit sie nicht Öffnungsklauseln zur Regelung von Rechtsmaterien zugunsten des nationalen Rechts enthält. Sie ersetzt das bisherige Bundesdatenschutzgesetz in der Fassung vom 14. Januar 2003, das bis zum 24. Mai 2018 anzuwenden ist (BDSG-2003). Ergänzend gilt in Deutschland das neue nationale Bundesdatenschutzgesetz (BDSG-2018), das auf Basis des EU-Datenschutz-Anpassungs- und -Umsetzungsgesetz (DSAnpUG-EU) ergangen ist. Dieses füllt die Öffnungsklauseln der DSGVO auf nationaler Ebene aus.

Die DSGVO wird nach europarechtlichen Auslegungsgrundsätzen interpretiert. Diese können von den deutschen Auslegungsgrundsätzen (z. B. nach BGB und HGB) abweichen.

Die Hinweise erheben keinen Anspruch auf Vollständigkeit. Die Hinweise zum Internetauftritt der verantwortlichen Kanzlei beruhen auf den nationalen Vorschriften ohne Berücksichtigung der E-Privacy-Verordnung (ePV) der EU, deren Inhalt bei Verfassung der Hinweise noch nicht feststand. Sie geben die gemeinsame Meinung der BStBK und des DStV wieder. Jegliche Haftung für Schäden, die aufgrund einer abweichenden Interpretation entstehen, ist daher ausgeschlossen.

2. Begriffsbestimmungen[1]

„Verantwortlicher“ (Art. 4 Nr. 7 DSGVO) ist z. B. der Kanzleiinhaber, der Gesellschafter einer Sozietät oder Partnerschaftsgesellschaft bzw. die Steuerberatungs-GmbH, vertreten durch ihren Geschäftsführer.

„Beschäftigte“ sind in § 26 Abs. 8 BDSG-2018 definiert. Von den in dieser Norm genannten Beschäftigten können folgende in der Steuerberatungskanzlei vorkommen:

- Arbeitnehmer, einschließlich Leiharbeitnehmer im Verhältnis zum Entleiher,
- zu ihrer Berufsbildung Beschäftigte,
- Teilnehmer an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobung (Rehabilitandinnen und Rehabilitanden),

[1] Männliche Formen umfassen auch die adäquaten weiblichen Formen.

- Personen, die wegen ihrer wirtschaftlichen Unselbstständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten.

„Weitere Auftragsverarbeiter“ bezeichnet Subauftragsverarbeiter, die als Unterauftragnehmer personenbezogene Daten für Auftragsverarbeiter verarbeiten. Beispiel: Der Verantwortliche beauftragt den Cloud-Dienstleister zur Datenverarbeitung. Da der Cloud-Dienstleister kein eigenes Rechenzentrum vorhält, beauftragt dieser den Betreiber eines Rechenzentrums als „weiteren Auftragsverarbeiter“.

„Remotezugriff“ bzw. „Fernzugriff“ bedeutet, auf den Datenbestand von einem beliebigen Ort über das Internet oder eine andere Telekommunikationsmöglichkeit zuzugreifen.

„Schriftlich“ oder „Schriftform“ im Sinne der europäischen Auslegung bezeichnet sowohl Erklärungen, die durch eine natürliche Person eigenhändig unterzeichnetet sind, als auch solche, die ohne eigenhändige Unterschrift auf einem dauerhaften Datenträger abgegeben werden und für den Empfänger lesbar sind (z. B. E-Mail, Textdatei usw.).

Im Übrigen gelten die Begriffsbestimmungen, die in Art. 4 DSGVO verbindlich definiert sind. Diese lassen sich zum leichteren Verständnis wie folgt erläutern:

1. „Personenbezogene Daten“ sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen. Identifizierbar ist eine natürliche Person, wenn sie anhand der Informationen direkt oder indirekt bestimmt werden kann. Dies kann insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen geschehen. Diese Merkmale können Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität der natürlichen Person sein.

2. „Verarbeitung“ umfasst das Erheben, Erfassen, die Organisation, das Ordnen, die Speicherung, Anpassung oder Veränderung, das Auslesen, Abfragen, die Verwendung, Offenlegung durch Übermittlung, Verbreitung und jede andere Form der Bereitstellung, den Abgleich, die Verknüpfung, Einschränkung, das Löschen und die Vernichtung von personenbezogenen Daten. Die „Verarbeitung“ kann mit und ohne Hilfe automatisierter Verfahren ausgeführt werden.

3. „Einschränkung der Verarbeitung“ ist die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken.

4. „Profiling“ ist die automatisierte Verarbeitung personenbezogener Daten, um bestimmte persönliche Aspekte einer natürlichen Person zu bewerten. Hierzu gehören insbesondere die Analyse oder Vorhersage von Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechseln.

5. „Pseudonymisierung“ ist die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können. Die zusätzlichen Informationen

müssen gesondert aufbewahrt werden. Technische und organisatorische Maßnahmen müssen gewährleisten, dass die personenbezogenen Daten nicht ohne die gesondert aufzubewahrenden Informationen einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden können.

6. „Dateisystem“ ist jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind. Dabei spielt es keine Rolle, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet ist.

7. „Verantwortlicher“ ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Bei Einzelkanzleien ist der die Kanzlei führende Steuerberater „Verantwortlicher“ im Sinne des Datenschutzrechts. Bei Personengesellschaften sind die Gesellschafter der Sozietät bzw. Partnerschaftsgesellschaft oder der Steuerberatungsgesellschaft (z. B. OHG, KG) die „Verantwortlichen“. Bei Kapitalgesellschaften (z. B. Steuerberatungs-GmbH) ist die Kapitalgesellschaft „Verantwortliche“, die von der Geschäftsführung vertreten wird.

8. „Auftragsverarbeiter“ ist jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

9. „Empfänger“ ist jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, denen personenbezogene Daten offengelegt werden. Dies gilt unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Finanzämter, Gerichte und sonstige Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Recht der EU oder eines Mitgliedstaates möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger. Die Verarbeitung dieser Daten erfolgt durch die genannten Behörden im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung.

10. „Dritter“ ist jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.

11. „Einwilligung“ der betroffenen Person ist jede von ihr freiwillig und in informierter Weise abgegebene Willensbekundung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten in einem bestimmten Fall einverstanden ist.

12. „Verletzung des Schutzes personenbezogener Daten“ bezeichnet eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust, zur Veränderung oder unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

13. „Genetische Daten“ sind Daten zu genetischen Eigenschaften, die eindeutige Informationen über die Physiologie oder Gesundheit einer natürlichen Person liefern. Hierzu gehören insbesondere Daten, die aus der Analyse einer biologischen Probe von einer natürlichen Person gewonnen werden.

14. „Biometrische Daten“ sind Daten zu physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die ihre eindeutige Identifizierung ermöglichen oder bestätigen. Hierzu gehören insbesondere Gesichtsbilder und daktyloskopische Daten (z. B. Fingerabdrücke).

15. „Gesundheitsdaten“ sind personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person beziehen. Dies sind auch personenbezogene Daten, die sich auf die Erbringung von Gesundheitsdienstleistungen beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen.

16. „Hauptniederlassung“ bezeichnet im Regelfall die Niederlassung am Ort der Hauptverwaltung des Verantwortlichen oder Auftragsverarbeiters in der EU. Werden die Entscheidungen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten in einer anderen Niederlassung innerhalb der EU getroffen, so ist diese andere Niederlassung die Hauptniederlassung.

17. „Vertreter“ ist eine in der EU niedergelassene natürliche oder juristische Person, die nach schriftlicher Bestellung gem. Art. 27 DSGVO einen Verantwortlichen oder Auftragsverarbeiter in Bezug auf die nach der DSGVO obliegenden Pflichten vertritt.

18. „Unternehmen“ bezeichnet jede natürliche oder juristische Person, die eine wirtschaftliche Tätigkeit ausübt. Dies gilt unabhängig von ihrer Rechtsform. Eingeschlossen sind Personengesellschaften und Vereinigungen, die regelmäßig einer wirtschaftlichen Tätigkeit nachgehen.

19. „Unternehmensgruppe“ ist eine Gruppe, die aus einem herrschenden Unternehmen und von diesem abhängigen Unternehmen besteht.

20. „Verbindliche interne Datenschutzvorschriften“ sind Maßnahmen zum Schutz von personenbezogenen Daten, zu deren Einhaltung sich ein in der EU ansässiger Verantwortlicher oder Auftragsverarbeiter in Bezug auf die Datenübermittlung an außerhalb der EU ansässige Unternehmen derselben Unternehmensgruppe verpflichtet hat. Das gilt auch für Gruppen von Unternehmen, die eine gemeinsame Wirtshaftstätigkeit ausüben, auch wenn diese nicht im Sinne vorstehender Ziffer 19 als Unternehmensgruppe verbunden sind.

21. „Aufsichtsbehörde“ ist eine gem. Art. 51 DSGVO eingerichtete unabhängige staatliche Stelle, die für die Überwachung der Anwendung der DSGVO zuständig ist, damit die Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung geschützt werden und der freie Verkehr personenbezogener Daten in der EU erleichtert wird.

22. „Betroffene Aufsichtsbehörde“ ist eine Aufsichtsbehörde, die von der Verarbeitung personenbezogener Daten betroffen ist, weil

    (1) der Verantwortliche oder der Auftragsverarbeiter im Hoheitsgebiet des Mitgliedstaates dieser Aufsichtsbehörde niedergelassen ist,

    (2) diese Verarbeitung erhebliche Auswirkungen auf betroffene Personen mit Wohnsitz im Mitgliedstaat dieser Aufsichtsbehörde hat oder haben kann oder

    (3) eine Beschwerde bei dieser Aufsichtsbehörde eingereicht wurde.

23. „Grenzüberschreitende Verarbeitung“ bezeichnet zum einen die Verarbeitung personenbezogener Daten in mehreren Mitgliedstaaten, wenn der Verantwortliche oder Auftragsverarbeiter in mehreren Mitgliedstaaten niedergelassen ist.

    Zum anderen bezeichnet „grenzüberschreitende Verarbeitung“ die Verarbeitung personenbezogener Daten eines in der EU niedergelassenen Verantwortlichen oder Auftragsverarbeiters, wenn dies erhebliche Auswirkungen auf betroffene Personen in mehreren Mitgliedstaaten hat oder haben kann.

24. „Maßgeblicher und begründeter Einspruch“ bezeichnet einen Einspruch gegen einen Beschlussentwurf, mit dem ein Verstoß gegen die DSGVO festgestellt wird oder ob Maßnahmen gegen Verantwortliche oder Auftragsverarbeiter mit der DSGVO in Einklang stehen. Dabei muss aus dem Einspruch die Tragweite der Risiken klar hervorgehen, die von dem Beschlussentwurf in Bezug auf die Grundrechte und Grundfreiheiten der betroffenen Personen und ggf. den freien Verkehr personenbezogener Daten in der EU ausgehen.

25. „Dienst der Informationsgesellschaft“ ist gem. Art. 1 Nr. 1 Buchst. b der Richtlinie (EU) 2015/1535 jede Dienstleistung der Informationsgesellschaft, d. h. jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung.

26. „Internationale Organisation“ bezeichnet eine völkerrechtliche Organisation und ihre nachgeordneten Stellen. „Internationale Organisation“ ist zudem jede sonstige Einrichtung, die durch oder auf Grundlage einer Übereinkunft geschaffen wurde, die durch zwei oder mehr Länder geschlossenen wurde.

3. Grundsätze zur Datenverarbeitung

Der Verantwortliche muss die Einhaltung der nachfolgenden Grundsätze nachweisen können (**Rechenschaftspflicht** gem. Art. 5 Abs. 2 DSGVO). Eine Veröffentlichung ist nicht erforderlich, jedoch kann eine Datenschutzaufsichtsbehörde die Vorlage eines Nachweises verlangen.

Der Verantwortliche muss die **Rechtmäßigkeit der Verarbeitung** personenbezogener Daten nachweisen können. Der Verantwortliche muss im Verhältnis zu den betroffenen Personen die Verarbeitung nach den Grundsätzen von Treu und Glauben durchführen.

Bei eigenen Beschäftigten kann dies beispielsweise über den Nachweis des Beschäftigungsverhältnisses (Arbeitsvertrag) erfolgen, bei Daten aus dem Mandatsverhältnis über den Mandatsvertrag. Aus ihm sollten der Beratungsumfang, d. h. die vereinbarte Leistung nach dem StBerG hervorgehen und die Zweckbindung vereinbart werden. Die berufsrechtlich flankierenden Verschwiegenheitsmaßnahmen und die strafrechtliche Sanktionierungsandrohung gem. § 203 StGB sind darüber hinaus zu beachten.

Die Verarbeitung personenbezogener Daten (pbD) hat **transparent** gegenüber den betroffenen Personen unter Berücksichtigung der berufsrechtlichen Verschwiegenheit zu erfolgen.

Die Verarbeitung pbD hat **zweckgebunden** zu erfolgen. Die konkreten Zwecke werden in der Regel durch den Mandatsauftrag vorgegeben. Werden Daten für weitere Zwecke, z. B. für Werbung, verarbeitet, müssen hierfür die gesetzlichen Rechtmäßigkeitsanforderungen beachtet und die Einhaltung der Rechte der betroffenen Person sichergestellt werden.

Bei der Umsetzung des Mandatsvertrages dürfen nur Daten verarbeitet werden, die dafür erforderlich sind **(Datenminimierung und Datensparsamkeit)**. Nicht für die Mandatsbearbeitung erforderliche Unterlagen und Daten müssen an den Mandanten zurückgegeben bzw. gelöscht werden.

Personenbezogene Daten müssen korrigiert werden können, wenn sie sich als unrichtig herausstellen **(Richtigkeit)**.

Zur Umsetzung der Vorgabe der **Speicherbegrenzung** ist ein Löschkonzept zu erarbeiten. In diesem Konzept sind Löschfristen unter Berücksichtigung gesetzlicher Aufbewahrungsfristen zu definieren und die Verfahren zur Löschung festzulegen.

Die Sicherheit der Daten und der Schutz vor unbefugten Zugriffen und Datenverlust müssen gewährleistet sein **(Integrität und Vertraulichkeit)**.

4. Grundsätze der Sicherheit bei der Verarbeitung personenbezogener Daten

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten (Art. 32 Abs. 1, 1. Halbsatz DSGVO).

Siehe im Weiteren das Muster für ein Verzeichnis der Verarbeitungstätigkeiten (Ziff. 10.3.5 Muster: Verzeichnis der Verarbeitungstätigkeiten).

5. Mandatierung

5.1 Rechtsgrundlage aus Mandatsverhältnis

Rechtsgrundlage zur Verarbeitung der anfallenden personenbezogenen Daten ist der Mandatsvertrag (Art. 6 Abs. 1 Buchst. b) DSGVO).

Es ist zu unterscheiden zwischen den Daten, die als Stammdaten des Mandanten verarbeitet werden und denen, die im Rahmen der Erbringung der Steuerberaterleistungen verarbeitet werden (z. B. Debitoren, Kreditoren oder Beschäftigte des Mandanten).

Der Steuerberater führt die im Steuerberatungsgesetz festgelegten Beratungsleistungen weisungsfrei und eigenverantwortlich aus. Daher genügt es, wenn der Beratungsgegenstand, die Zweckbindung und der Verweis auf die berufsrechtlichen Verschwiegenheitsverpflichtungen vereinbart werden.

Aus dem Berufsrecht oder Datenschutzrecht ergeben sich keine Formanforderungen an den Mandatsvertrag. Aus Gründen der Nachweisbarkeit empfiehlt sich eine schriftliche Vereinbarung.

Auch im Hinblick auf das Datenschutzrecht sollte insbesondere der Beratungsgegenstand mit Bezeichnung von Art und Umfang der erbrachten Dienstleistung und durchzuführenden Tätigkeiten (Leistungszweck) vereinbart werden.

5.2 Fachleistung des Steuerberaters (keine Auftragsverarbeitung)

Die Leistung des Steuerberaters ist eine eigenverantwortlich erbrachte fachliche Beratung und ist somit keine Auftragsverarbeitung. Dies gilt auch für die Lohn- und Gehaltsabrechnung, die der Steuerberater nach dem Steuerberatungsgesetz (StBerG) eigenverantwortlich ausführt.[2]

6. Organisation in der Kanzlei

Unabhängig von den Regelungen zum Datenschutz sind Steuerberater aufgrund ihrer berufsrechtlichen Regelungen zur Verschwiegenheit und damit zum Datenschutz verpflichtet. Paragraf 62 StBerG bestimmt, dass die Beschäftigten in der Kanzlei entsprechend zu belehren sind und dass der Steuerberater auf die Einhaltung dieser Verschwiegenheit hinzuwirken hat. Des Weiteren sind die Beschäftigten auf die Einhaltung der Vertraulichkeit nach der DSGVO zu verpflichten. Diese Verpflichtungen gelten auch innerhalb der Kanzlei.

6.1 Zutritt

Der Zutritt zu den Räumlichkeiten, in denen sich Daten oder IT-Systeme befinden, wird mittels technischer und organisatorischer Mittel abgesichert. Dabei wird sichergestellt, dass Unbefugte keinen Zutritt zu Unterlagen und IT-Systemen haben.

6.2 Zugang (Benutzerverwaltung)

Der Zugang zu den IT-Systemen wird durch eine personenbezogene Benutzerverwaltung (Einzelaccount) gewährleistet. Der Benutzer ist verpflichtet, sich persönlich mit einem individuellen Benutzernamen und einem individuellen Passwort im System anzumelden.[3]

6.3 Zugriff (Rechteverwaltung)

Der Verantwortliche gewährleistet daher durch die Zugriffsorganisation, dass der Zugriff auf schutzwürdige Daten nur erfolgt, wenn dieser zur Erledigung der Aufgaben notwendig ist.

6.3.1 Rollenkonzept

Bei der Einrichtung und Pflege der Zugriffsberechtigungen kommt ein Rollenkonzept zum Einsatz. Dabei werden durch den Verantwortlichen die Benutzer in Berechtigungsgruppen eingeteilt. Diese

---

[2] Kurzpapier Nr. 13 der Datenschutzkonferenz (DSK); Anhang B, u. a. abrufbar unter folgendem Link: https://www.lda.bayern.de/de/datenschutz_eu.html

[3] Zu den Verschlüsselungsanforderungen siehe unten Ziffer 12.3 Verschlüsselungsanforderungen.

leiten sich aus den unterschiedlichen Funktionen und Einsatzbereichen der Benutzer in der Kanzlei (Rollen) ab. Kriterien sind dabei unter anderem:

- Position innerhalb der Aufbauorganisation (z. B. Inhaber bzw. Geschäftsführer, Gruppenleiter, fachlicher Mitarbeiter etc. aber auch die Zugehörigkeit zu bestimmten Abteilungen),
- berufliches Qualifikationsniveau (z. B. Berufsträger, Steuerfachwirt etc.),
- Position innerhalb der Ablauforganisation (z. B. Sachbearbeiter Buchführung etc.).

Für jede Benutzergruppe (Rolle) werden dann die notwendigen Rechte definiert und zugeteilt. Im Anschluss an diese Rechtevergabe werden diese benutzerbezogen durch den Verantwortlichen überprüft und auf der Ebene des einzelnen Benutzers eingeschränkt bzw. erweitert.

6.3.2 Benutzerregelung, Zugriffsrechte

Unter Berücksichtigung des Interesses des Mandanten, ggf. jederzeit Informationen zur beauftragten Angelegenheit zu bekommen, wird mandats- und auftragsbezogen geprüft, ob ein Zugriff auf die Daten durch einen Benutzer notwendig und sinnvoll ist. Nur wenn dies der Fall ist, wird ein Zugriff ermöglicht.

Soweit der Zugriff nicht aufgrund der o. g. Kriterien beschränkt wird, werden die Beschäftigten durch regelmäßige Unterrichtung darauf hingewiesen, dass ein Zugriff trotz der technischen Möglichkeiten nur im Rahmen der eigenen Aufgabenerfüllung zu erfolgen hat.

Zusätzlich zu diesen allgemeinen Regelungen wird in jedem Einzelfall geprüft, ob das Risiko einer Interessenkollision oder ein privates Interesse des Benutzers an den Daten vorliegen könnte. Dabei reicht ein nicht unerhebliches abstraktes Risiko aus, um in diesen Fällen den Zugriff nicht zu gewähren.

Gleiches gilt, soweit der Mandant oder anderweitig betroffene Personen den Zugriff durch bestimmte Benutzer nicht wünschen.

Sollte trotz eines bestehenden Risikos eine Bearbeitung der Angelegenheit durch diesen Benutzer (z. B. Mitarbeiter) von einer betroffenen Person (z. B. Mandanten) ausdrücklich gewünscht werden, wird vor Erteilung einer Zugriffsberechtigung eine Interessensabwägung durch den Verantwortlichen vorgenommen.

6.4 Zugang von außerhalb der Kanzlei (Remoteverbindung)

Im Fall von Remoteverbindungen sind weitere Sicherheitsmaßnahmen entsprechend dem Stand der Technik erforderlich, um den Zugang von Unbefugten zu verhindern.

6.4.1 Berechtigte Endgeräte

Der Zugang auf interne IT-Systeme von außerhalb des Kanzlei-Netzes (LAN und WLAN) erfolgt nur durch Endgeräte, für die die Kanzlei ein Nutzungsrecht hat. Deren Einrichtung und Wartung

erfolgt nur durch den Verantwortlichen bzw. einen von ihm beauftragten und überwachten IT-Dienstleister. Auch auf den für den Remotezugang zugelassenen Endgeräten ist eine personenbezogene Benutzerverwaltung einzurichten.

6.4.2 Zweistufiges Anmeldekonzept

Bei der Anmeldung am Server im Rahmen des Remotezugangs kommt ein Konzept von „Wissen und Besitz“ zum Einsatz. Voraussetzung für die Anmeldung ist somit eine Hardware-ID (z. B. auf einer Smartcard) und ein Passwort. Alternativ können auch Anmeldungsprozeduren eingesetzt werden, die die gleichzeitige Nutzung zweier verschiedener Endgeräte (z. B. Notebook und Smartphone) voraussetzen.

6.5 Risikobasierte Schutzkonzepte

Für die Festlegung der Zugriffsberechtigungen sind die Mandanten und die schutzbedürftigen Daten in verschiedene Risikoklassen einzuteilen.

Das mandatsbezogene Risiko ergibt sich dabei aus der Person des Mandanten (z. B. politisch exponierte Personen) oder deren Geschäftstätigkeit (z. B. Tätigkeiten im Bereich von Forschung und Entwicklung). Die Schutzbedürftigkeit der Daten ergibt sich aus ihrer Bedeutung für das Leben und die wirtschaftlichen Verhältnisse des Mandanten.

Als schutzwürdig werden darüber hinaus Daten Drittbetroffener angesehen, die im Rahmen des Mandatsverhältnisses überlassen werden. Dies betrifft insbesondere die Daten der Beschäftigten des Mandanten, die im Rahmen der Lohnbuchhaltung überlassen und verarbeitet werden.

Die Zugriffsberechtigungen werden entsprechend der Risikoklassen eingeschränkt. Dabei wird auch ein Verlust bei der Informationsbereitschaft in Kauf genommen.

Beispiel: Einteilung der Risikoklassen

Risikoklasse 1 – hohes Risiko

Personenbezogene Daten unterliegen einem Geschäfts- oder Betriebsgeheimnis, bei deren Bekanntwerden oder Verlust ein wirtschaftlich erheblicher Schaden droht.

Schadensträchtige Datenkategorien wie Bankverbindungsdaten, Kreditkartendaten etc. und/oder sensible Datenkategorien (Daten über rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische, biometrische Daten, Gesundheitsdaten, sexuelle Orientierung).

Daten aus der Privatsphäre einer politisch exponierten oder öffentlich bekannten Person.

Risikoklasse 2 – mittleres Risiko

Personenbezogene Daten unterliegen dem Berufsgeheimnis (Mandatsverhältnis), jedoch keine schadensträchtigen Datenkategorien und keine sensiblen Datenkategorien.

Risikoklasse 3 – geringes Risiko

Daten unterliegen nicht dem Berufsgeheimnis, keine schadensträchtigen Datenkategorien und keine sensiblen Datenkategorien.

6.6 Dokumentation und Kontrolle

Die Zugriffe auf Daten werden fortlaufend aufgezeichnet und dokumentiert. Anlassbezogen wird die Einhaltung der Regelungen zum Datenzugriff durch den Verantwortlichen oder den Datenschutzbeauftragten kontrolliert.

Des Weiteren erfolgt regelmäßig oder anlassbezogen eine Kontrolle und ggf. eine Anpassung der Berechtigungen durch den Verantwortlichen.

Soweit die in diesem Kapitel beschriebenen Maßnahmen systemseitig dokumentiert werden, bedarf es keiner gesonderten Dokumentation.

6.7 Außenauftritt der Kanzlei

Der Datenschutz und die Verschwiegenheitspflicht sind auch bei der Behandlung von personenbezogenen Daten beim Außenauftritt des Steuerberaters (z. B. Internetseiten, Kanzleibroschüre, Soziale Medien) zu beachten.

6.8 Rechtskonforme Newsletter

Bei der Anmeldung zum Bezug eines Newsletters ist eine doppelte Bestätigung der Anmeldung erforderlich, man spricht hierbei vom sog. Double-Opt-In-Verfahren.

Beim „Double-Opt-in“ muss die Eintragung in eine Newsletter-Abonnentenliste in einem zweiten Schritt (deshalb Double) bestätigt werden. Hierzu wird in der Regel eine E-Mail-Nachricht mit der Bitte um Bestätigung an die eingetragene E-Mail-Adresse gesendet. Die Registrierung beim „Double-Opt-in“ erfolgt erst dann, wenn sie mit dieser E-Mail bestätigt wird.

7. Einbindung von Dienstleistern

Kanzleien können Dienstleister mit der Verarbeitung von personenbezogenen Daten betrauen. Diese können in Abhängigkeit von der konkreten Ausgestaltung als Auftragsverarbeiter, als gemeinsame Verantwortliche oder als Verantwortliche tätig sein.

7.1 Auftragsverarbeiter

Bei der Auftragsverarbeitung bestimmt der Verantwortliche (Kanzlei) den Zweck der Datenverarbeitung, während der Auftragsverarbeiter die Leistung weisungsgemäß durchführt. Somit sind z. B. die Leistungen von Rechenzentren, externen IT-Dienstleistern, Google-Analytics und vergleichbare Tracking-Tools, Aktenvernichtungsunternehmen, Letter-Shops, E-POST, Internet-Service-

Providern und Application-Service-Providern (ASP) Auftragsverarbeitung. Fernwartungen und Wartungen vor Ort an Applikationen mit personenbezogenen Daten sind ebenfalls Auftragsverarbeitung.

Die Verantwortung für den rechtskonformen Umgang mit den personenbezogenen Daten verbleibt vollumfänglich bei dem Verantwortlichen (Kanzlei). Dies gilt unabhängig von einer Haftung des Auftragsverarbeiters.

Andere Post- und Telekommunikationsdienstleistungen sind grundsätzlich keine Auftragsverarbeitung.

7.1.1 Anforderung an die Auswahl des Auftragsverarbeiters

Aus der Verantwortlichkeit der Kanzlei folgt, dass diese nur mit Auftragsverarbeitern zusammenarbeitet, die durch geeignete technische und organisatorische Maßnahmen hinreichende Garantien dafür bieten, dass die Verarbeitung im Einklang mit dem Datenschutzrecht erfolgt.

Geeignete Garantien bieten insbesondere Zertifizierungen und die Einhaltung genehmigter Verhaltensregeln. Darüber hinaus kommen Vor-Ort-Audits und Selbstauskünfte des Auftragsverarbeiters in Betracht.

7.1.2 Vertrag zur Auftragsverarbeitung

Die Inhalte des Vertrags zur Auftragsverarbeitung müssen mindestens den Vorgaben des Art. 28 DSGVO entsprechen.[4]

Sofern im Zusammenhang mit der Beauftragung personenbezogene Daten verarbeitet werden, die der beruflichen Verschwiegenheit unterliegen, ist eine Ergänzung bzgl. der Verpflichtung des Auftragsverarbeiters um § 203 StGB und § 62a StBerG erforderlich. Für den Abschluss des Vertrages sowie eventueller Änderungen/Ergänzungen kommt neben der Schriftform auch die Textform in Frage. Die Unterlagen sind aufzubewahren.

[4] Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) hat ein Muster für einen Auftragsverarbeitungsvertrag auf seinen Webseiten veröffentlicht (www.lda.bayern.de). Wenn dieses Muster angewendet wird, muss als Anlage hierzu die in Ziff. 7.1.3 dargelegte Zusatzvereinbarung zum Auftragsverarbeitungsvertrag zur Einhaltung der Pflichten aus § 203 StGB und § 62a StBerG abgeschlossen werden.

7.1.3 Muster: Zusatzvereinbarung zum Auftragsverarbeitungsvertrag

Anlage zum Vertrag zur Auftragsverarbeitung vom ……

Vereinbarung
über die Verpflichtung zur Wahrung des Berufsgeheimnisses nach §§ 203 und 204 StGB einschließlich Belehrung über die strafrechtlichen Folgen einer Pflichtverletzung (§ 62a StBerG)

I. Der Auftraggeber belehrt die Firma

……..……
– nachstehend Auftragsverarbeiter genannt –

gem. § 62a Abs. 3 Satz 2 Nr. 1 Steuerberatungsgesetz (StBerG) über die strafrechtlichen Folgen aus §§ 203 und 204 Strafgesetzbuch (StGB) wie folgt:

1. Offenbart der Auftragsverarbeiter ein in Ausübung oder bei Gelegenheit der Auftragsverarbeitung bekannt gewordenes fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, welches den Berufsträgern des Auftraggebers anvertraut wurde, kann dies mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe bestraft werden (§ 203 Abs. 1, Abs. 4 Satz 1 StGB). Die Strafandrohung gilt auch für Personen, die für den Auftragsverarbeiter an der Auftragsverarbeitung mitwirken (§ 203 Abs. 4 Satz 1 StGB).

2. Geheimnisse sind alle Informationen, die nur einem beschränkten Personenkreis bekannt sind und an deren Geheimhaltung derjenige, den die Informationen betreffen (Geheimnisträger), ein sachlich begründetes Interesse hat. Hierzu gehören insbesondere alle Informationen über Mandatsverhältnisse zum Auftraggeber bzw. zu den Berufsträgern des Auftraggebers.

3. Handelt es sich beim Auftragsverarbeiter nicht um eine natürliche Person, trifft die Strafandrohung die für den Auftragsverarbeiter mitwirkenden natürlichen Personen.

4. Im Fall der Einschaltung Dritter (z. B. Subunternehmer) macht sich der Auftragsverarbeiter bzw. die für ihn handelnde Person bei Strafandrohung von Freiheitsstrafe bis zu einem Jahr oder Geldstrafe strafbar, wenn der Dritte unbefugt ein bei der Ausübung oder bei Gelegenheit seiner Tätigkeit bekannt gewordenes fremdes Geheimnis offenbart und der Auftragsverarbeiter nicht dafür Sorge getragen hat, dass der Dritte zur Geheimhaltung verpflichtet wurde (§ 203 Abs. 1, Abs. 4 Satz 2 Nr. 2 StGB).

5. Die angedrohte Strafe beträgt bis zu zwei Jahren oder Geldstrafe, wenn der Täter gegen Entgelt oder in der Absicht handelt, sich zu bereichern oder durch die Tat einen anderen zu schädigen (§ 203 Abs. 6 StGB). Gleiches gilt, wenn der Täter ein dem Berufsträger anvertrautes fremdes Geheimnis unbefugt verwertet (§ 204 StGB).

II. Der Auftragsverarbeiter verpflichtet sich gegenüber dem Auftraggeber sowie den beim Auftraggeber tätigen Berufsgeheimnisträgern wie folgt:

1. Der Auftragsverarbeiter wirkt als Dienstleister an den Tätigkeiten der Berufsgeheimnisträger mit, die einer beruflichen Verschwiegenheitsverpflichtung unterliegen. Der Auftragsverarbeiter wahrt in Kenntnis der strafrechtlichen Folgen einer Verletzung der Verschwiegenheitspflicht fremde Geheimnisse, die ihm zugänglich gemacht werden.

2. Der Auftragsverarbeiter ist befugt, weitere Personen (Dritte) zur Erfüllung des Vertrages heranzuziehen. Beim Einsatz von Dritten (z. B. weitere Auftragsverarbeiter) verpflichtet sich der Auftragsverarbeiter, diese in Textform unter Belehrung über die strafrechtlichen Folgen einer Pflichtverletzung zur Verschwiegenheit zu verpflichten, soweit diese Dritten im Rahmen ihrer Tätigkeit Kenntnis von fremden Geheimnissen erlangen könnten. Der Auftragsverarbeiter informiert den Auftraggeber über jede beabsichtigte Hinzuziehung von weiteren Auftragsverarbeitern. Der Auftraggeber kann hierbei in begründeten Einzelfällen die Hinzuziehung untersagen.

3. Der Auftragsverarbeiter ist verpflichtet, sich nur insoweit Kenntnis von fremden Geheimnissen zu verschaffen, als dies zur Vertragserfüllung erforderlich ist. Er wird angemessene organisatorische und technische Maßnahmen zum Schutz der fremden Geheimnisse und vertraulichen Informationen einhalten und dabei akzeptierte Sicherheitsstandards nach dem jeweils aktuellen Stand der Technik anwenden.

4. Die Pflicht zur Verschwiegenheit besteht auch nach Beendigung des Auftragsverhältnisses zeitlich unbegrenzt fort.

5. Die Pflicht zur Verschwiegenheit gemäß den vorstehenden Absätzen besteht nicht, soweit der Auftragsverarbeiter aufgrund einer behördlichen oder gerichtlichen Entscheidung zur Offenlegung von vertraulichen Informationen des Auftraggebers verpflichtet ist. Soweit dies im Einzelfall zulässig und möglich ist, wird der Auftragsverarbeiter den Auftraggeber über die Pflicht zur Offenlegung vorab in Kenntnis setzen.

6. Der Auftragsverarbeiter ist verpflichtet sicherzustellen, dass die Auftragsverarbeitung nur durch einen zur Verschwiegenheit verpflichteten Personenkreis durchgeführt wird.

.....
(Ort, Datum)

....
(Unterschrift Auftragsverarbeiter) (Unterschrift Auftraggeber)

7.1.4 Kontrolle

Der Verantwortliche muss die vertragsgemäße Erfüllung der Auftragsverarbeitung kontrollieren. Hierfür muss der Auftragsverarbeiter dem Verantwortlichen alle notwendigen Informationen zur Verfügung stellen.

Die Kontrollen können insbesondere durch die Vorlage von Zertifikaten, die Prüfung von Selbstauskünften oder Inspektionen (Vor-Ort-Audits) erfolgen.

Die Kontrollen sind zu dokumentieren.

7.1.5 Remoteverbindung für Dienstleister

Bei Fernwartungen ist zu gewährleisten, dass diese erst nach Freigabe durch den Verantwortlichen gestartet und jederzeit unterbrochen werden können. Der Wartungsvorgang ist zu protokollieren. Eine Vereinbarung dieser Protokollierung im Auftragsverarbeitungsvertrag kann sinnvoll sein.

7.1.6 Weitere Auftragsverarbeiter (Subauftragsverarbeiter)

Die Beauftragung weiterer Auftragsverarbeiter durch die Auftragsverarbeiter der Kanzlei darf nur mit schriftlicher (oder elektronischer) Zustimmung erfolgen. Bei Abschluss eines Vertrags zur Auftragsverarbeitung sind die beauftragten weiteren Auftragsverarbeiter zu benennen. Hat der Verantwortliche dem Auftragsverarbeiter eine allgemeine Genehmigung zur Hinzuziehung weiterer Auftragsverarbeiter erteilt, so hat der Auftragsverarbeiter den Verantwortlichen über jede beabsichtigte Hinzuziehung eines weiteren Auftragsverarbeiters zu informieren. Der Verantwortliche kann hierbei in begründeten Einzelfällen die Hinzuziehung untersagen.

7.1.7 Einbindung von Dienstleistern außerhalb Deutschlands

Sollte die Verarbeitung durch den Dienstleister außerhalb Deutschlands erfolgen, sind weitere gesetzliche Vorgaben beispielsweise aus dem Berufsrecht oder der AO zu beachten.

Erfolgt eine Verarbeitung außerhalb der EU/des EWR, müssen zusätzlich die Vorgaben aus der DSGVO (Kapitel V) berücksichtigt werden.

7.2 Gemeinsame Verantwortliche (Shared Services)

Legen zwei oder mehr Verantwortliche die Zwecke und Mittel der Verarbeitung fest, so sind sie gemeinsame Verantwortliche.[5] Sie legen in einer Vereinbarung in transparenter Weise fest, wer von ihnen welche Verpflichtung aus der DSGVO erfüllt.

Beispiel: Kanzleiverbund, der sich einer gemeinsamen Stelle für IT-Dienstleistungen bedient.

[5] Art. 26 Abs. 1 Satz 1 DSGVO.

7.3 Verantwortliche (Fremde Fachleistung)

Die Einbeziehung eines Berufsgeheimnisträgers (StB, RA, WP, externe Betriebsärzte), Inkassobüros mit Forderungsübertragung, Bankinstituts für den Geldtransfer, Postdienstes für den Brieftransport etc. ist keine Auftragsverarbeitung. Es handelt sich um die Inanspruchnahme fremder Fachleistungen bei einem eigenständig Verantwortlichen.

Für die Verarbeitung (einschließlich Übermittlung) personenbezogener Daten muss eine Rechtsgrundlage gem. Art. 6 DSGVO gegeben sein, z. B. die Einwilligung der betroffenen Person oder die Wahrung berechtigter Interessen des Verantwortlichen (Kanzlei).

8. Einsatz von Software

Der Verantwortliche muss bei der Auswahl und beim Einsatz von Softwarelösungen prüfen, ob mit diesen die Anforderungen der DSGVO erfüllt werden können.

9. Informationspflichten bei Datenerhebung und Betroffenenrechte

Den Auskunfts- und Informationspflichten ist in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache nachzukommen. Die Übermittlung der Information erfolgt in Abstimmung mit der betroffenen Person schriftlich oder in anderer Form, ggf. auch elektronisch.

9.1 Informationspflichten

Die neuen Informationspflichten gelten nur für Datenerhebungen ab dem 25. Mai 2018, zuvor erhobene Bestandsdaten sind ausgenommen.

9.1.1 Umfang der Informationspflicht

Folgende Informationen müssen der betroffenen Person gegeben werden, unabhängig davon, bei wem die Daten erhoben werden:

1. Verantwortlicher (Name und Kontaktdaten, ggf. auch des Vertreters)
2. Kontaktdaten des Datenschutzbeauftragten (funktionsbezogene E-Mail-Adresse ist ausreichend, unter der der Datenschutzbeauftragte erreichbar ist, z. B. datenschutz@.....de)
3. Zwecke und Rechtsgrundlagen (z. B. Einkommensteuererklärung, Mandatsvertrag)
4. Datenkategorien
5. Berechtigte Interessen
6. Empfänger oder Kategorien von Empfängern (z. B. Sachbearbeiter, Auftragsverarbeiter)
7. Drittstaatentransfer

Folgende Informationen sind der betroffenen Person mitzuteilen, wenn sie notwendig sind, eine faire und transparente Verarbeitung zu gewährleisten:

- geplante Speicherdauer oder, falls dies nicht möglich ist, die Kriterien für die Festlegung der Speicherdauer,
- Betroffenenrechte: Auskunft-, Löschungs-, Einschränkungs- und Widerspruchsrechte sowie das Recht auf Datenübertragbarkeit,
- Recht auf jederzeitigen Widerruf der Einwilligung,
- Beschwerderecht bei einer Aufsichtsbehörde,
- Pflicht des Verantwortlichen zur Bereitstellung der Daten (nur bei Direkterhebung),
- Angabe der Datenquelle (nicht bei Direkterhebung),
- im Fall einer automatisierten Entscheidungsfindung aussagekräftige Informationen über die angewendete Logik, Tragweite und angestrebten Auswirkung einer solchen Verarbeitung.

9.1.2 Ausnahmen

Die Informationen müssen nicht gegeben werden, wenn die betroffene Person bereits über die Informationen verfügt.

In Fällen der Dritterhebung ist auf eine Information zu verzichten, sofern die personenbezogenen Daten einer berufsrechtlichen Verschwiegenheitspflicht unterliegen. Der Verantwortliche muss prüfen, ob durch eine Informationsweitergabe das Berufsrecht verletzt wird, und er muss eine solche Verletzung verhindern.

Beispiel: Lohn- und Gehaltsabrechnung

Im Rahmen der Betreuung von Lohnmandaten erhebt, verarbeitet oder nutzt der Steuerberater personenbezogene Daten von Beschäftigten des Mandanten. In dieser Konstellation wird das Bestehen des Mandatsverhältnisses durch das Berufsgeheimnis geschützt. Eine Information an den Beschäftigten durch den Steuerberater ist nicht zulässig, außer der Mandant hat den Steuerberater von seiner berufsrechtlichen Verschwiegenheit entbunden. In der Praxis wird häufig eine konkludente Entbindung von der Verschwiegenheitspflicht anzunehmen sein, wenn z. B. der Mandant seine Beschäftigten bei Rückfragen an den Steuerberater verweist.

Beispiel: Private Steuererklärung

Im Rahmen der Erstellung privater Steuererklärungen werden vom Steuerberater nicht nur personenbezogene Daten des Mandanten erhoben, es werden auch personenbezogene Daten von Dritten erhoben und verarbeitet. In diesen Fällen darf der Steuerberater die Dritten über die Datenerhebung nicht informieren, eine Information der Dritten durch den Mandanten ist aber möglich.

9.1.3 Zeitpunkt

Im Fall der Direkterhebung müssen diese Informationen der betroffenen Person zum Erhebungszeitpunkt gegeben werden.

Werden die personenbezogenen Daten nicht direkt erhoben, so müssen die Informationen der betroffenen Person gegeben werden

a) unter Berücksichtigung der spezifischen Umstände der Verarbeitung der personenbezogenen Daten innerhalb einer angemessenen Frist nach Erlangung der personenbezogenen Daten, längstens jedoch innerhalb eines Monats,

b) falls die personenbezogenen Daten zur Kommunikation mit der betroffenen Person verwendet werden sollen, spätestens zum Zeitpunkt der ersten Mitteilung an sie, oder,

c) falls die Offenlegung an einen anderen Empfänger beabsichtigt ist, spätestens zum Zeitpunkt der ersten Offenlegung.

9.1.4 Arbeitshilfe – Verfahrensdokumentation zur Erfüllung der Informationspflichten

1. **Sind die personenbezogenen Daten bei der betroffenen Person selbst erhoben worden oder bei einem Dritten?**

□ Die personenbezogenen Daten sind bei der betroffenen Person selbst erhoben worden (Beispiele: Mandant, Kanzleibeschäftigte): ► wenn ja, weiter mit Ziff. 2

□ Die personenbezogenen Daten sind bei einem Dritten erhoben worden (Beispiel: Beim Mandanten werden die Daten eines Beschäftigten des Mandanten erhoben) ► wenn ja, weiter mit Ziff. 3

2. Direkterhebung: Datenerhebung bei der betroffenen Person

2.1 Es besteht keine Informationspflicht, soweit

□ die betroffene Person über die Information bereits verfügt,

□ die Informationserteilung eine vertrauliche Übermittlung von Daten an öffentliche Stellen gefährden würde oder

□ die Informationserteilung die Ausübung oder Verteidigung zivilrechtlicher Ansprüche beeinträchtigen würde und das berechtigte Interesse der betroffenen Person an der Informationserteilung nicht überwiegt.

2.2 Ist die Informationspflicht nicht gem. Ziff. 2.1 ausgeschlossen, müssen der betroffenen Person folgende Informationen mitgeteilt werden:

□ Verantwortlicher und Vertreter: Name und Kontaktdaten des Verantwortlichen und ggf. seines Vertreters, ggf. Firmenname (§ 17 HGB) oder Vereinsname (§ 57 BGB)

□ Kontaktdaten des Datenschutzbeauftragten, sofern vorhanden (funktionsbezogene, nicht-personifizierte E-Mail-Adresse ist ausreichend, unter der der Datenschutzbeauftragte erreichbar ist, z. B. datenschutz@.....de)

□ Zwecke und Rechtsgrundlagen der Datenverarbeitung (z. B. Zweck: Erfüllung des Mandatsvertrages, Rechtsgrundlage: Art. 6 Abs. 1 Buchst. b) DSGVO)

□ Ggf. die „berechtigten Interessen“, wenn Rechtsgrundlage der Datenverarbeitung die Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten ist

□ Ggf. Empfänger oder Kategorien von Empfängern, wenn die personenbezogenen Daten der betroffenen Person an Dritte übermittelt werden (z. B. Datenempfänger: Finanzbehörden)

□ Ggf. bei Drittstaatentransfer: Die Absicht, personenbezogene Daten in einen Staat außerhalb der EU/des EWR zu verarbeiten, ist der betroffenen Person mitzuteilen. Ferner ist mitzuteilen, ob ein Angemessenheitsbeschluss der EU-Kommission vorliegt oder nicht. Liegt kein Angemessenheitsbeschluss vor, muss auf geeignete Garantien des Verantwortlichen oder Auftragsverarbeiters im Drittstaat verwiesen und mitgeteilt werden, wie diese erhältlich sind.

Für eine faire und transparente Verarbeitung müssen ferner mitgeteilt werden:

□ Dauer der Speicherung personenbezogener Daten oder – falls Speicherdauer nicht festgelegt werden kann – die Kriterien für die Festlegung der Dauer (z. B. Hinweis auf ein vorgehaltenes Aufbewahrungs- und Löschkonzept unter Berücksichtigung der Aufbewahrungspflichten nach HGB und AO)

□ Hinweis auf die Rechte der betroffenen Person auf Auskunft, Berichtigung, Löschung, Einschränkung der Datenverarbeitung, Widerspruch gegen Datenverarbeitung sowie auf Datenübertragbarkeit

□ Hinweis auf das Recht zur Beschwerde bei einer Aufsichtsbehörde für den Datenschutz

□ Ggf. Hinweis auf die Pflichten des Verantwortlichen, personenbezogene Daten an Dritte bereitzustellen und die möglichen Folgen einer Nichtbereitstellung (z. B. Pflicht zur Bereitstellung unterschriebener Vollmachten des Mandanten)

□ Ggf. Hinweis auf das Recht, eine zuvor erteilte Einwilligung zu widerrufen, wenn die Einwilligung Rechtsgrundlage der Datenverarbeitung ist

3. Dritterhebung: Datenerhebung bei einem Dritten

3.1 Es besteht <u>keine</u> Informationspflicht, soweit

□ Informationen offenbart würden, die durch einen Mandanten an den Steuerberater als Berufsgeheimnisträger im Rahmen des Mandatsverhältnisses übermittelt wurden, soweit nicht im Einzelfall das Interesse der betroffenen Person an der Informationserteilung überwiegt,

□ auf andere Art und Weise erlangte Informationen offenbart würden, die dem Berufsgeheimnis des Steuerberaters unterliegen, soweit nicht das Interesse der betroffenen Person an der Informationserteilung überwiegt,

□ die betroffene Person über die Information bereits verfügt,

□ die Informationserteilung unmöglich ist oder einen unverhältnismäßigen Aufwand erfordert oder

□ die Informationserteilung die Ausübung oder Verteidigung zivilrechtlicher Ansprüche beeinträchtigen würde und das berechtigte Interesse der betroffenen Person an der Informationserteilung nicht überwiegt.

3.2 Ist die Informationspflicht <u>nicht</u> gem. Ziff. 3.1 ausgeschlossen, müssen der betroffenen Person folgende Informationen mitgeteilt werden:

□ die oben in Ziff. 2 genannten Informationen <u>und</u>

□ die Kategorien der erhobenen personenbezogenen Daten (z. B. Namen, Adress- und Kontaktdaten, Bankverbindung, Qualifikationen, Steuermerkmale, Lohngruppen, Arbeitszeiten, Tätigkeitsbereiche, Konfession, Krankmeldungen, gesundheitliche Beeinträchtigungen)

9.2 Datenschutzhinweis und Impressum auf der Website[6]

Auf jeder Seite müssen die Datenschutzhinweise und das Impressum erreichbar sein (z. B. im Footer).[7] Die Datenschutzhinweise müssen enthalten:

- Namen und Kontaktdaten des Verantwortlichen, ggf. Firmenname gem. § 17 Abs. 1 HGB
- ggf. die Kontaktdaten des Datenschutzbeauftragten; ausreichend ist eine nicht-personifizierte E-Mail-Adresse, unter welcher der Datenschutzbeauftragte erreichbar ist (z. B. datenschutz@.....de)
- Hinweis auf den Zweck und den Umfang der Verarbeitung sowie auf die dafür herangezogenen Rechtsgrundlagen
- Hinweis auf das berechtigte Interesse, insofern die Datenerhebung auf einem berechtigten Interesse des Verantwortlichen oder eines Dritten beruht, Art. 6 Abs. 1 Buchst. f) DSGVO
- ggf. die Nennung der Dienstleister, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeiten
- ggf. die Empfänger oder Kategorien der Empfänger von Betroffenendaten
- ggf. die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland zu übermitteln und zugleich die Information, ob ein Angemessenheitsbeschluss der Kommission vorhanden ist oder nicht; ist kein Angemessenheitsbeschluss vorhanden, ist auf geeignete oder angemessene Garantien hinzuweisen und anzugeben, wo und auf welche Weise diese verfügbar sind
- Hinweis auf die geplante Speicherdauer oder, falls dies nicht möglich ist, die Kriterien für die Festlegung der Speicherdauer
- Hinweis auf die Auskunfts-, Löschungs-, Einschränkungs- und Widerspruchsrechte sowie auf das Recht auf Datenübertragbarkeit
- Hinweis auf das Recht zum jederzeitigen Widerruf einer Einwilligung und die Tatsache, dass die Rechtmäßigkeit der Verarbeitung auf Grundlage der Einwilligung bis zum Widerruf unberührt bleibt
- Hinweis auf das Beschwerderecht bei der Aufsichtsbehörde

---

[6] Hier ist die weitere Entwicklung mit Blick auf die E-Privacy-Verordnung (ePV) zu beachten.

[7] Im Übrigen sind noch weitere Pflichten ohne unmittelbaren Bezug zum Datenschutzrecht zu beachten, die im Rahmen dieser Hinweise nicht behandelt werden (Pflichtangaben auf der Website (z. Z. § 5 TMG, DL-InfoV), Urheberrechte, Namens- und Bildrechte Dritter, ggf. Nennung des Verantwortlichen für journalistisch-redaktionelle Inhalte (§ 55 Abs. 2 RStV), berufsrechtliche Angaben, Pflichtangaben nach Verbraucherstreitbeilegungsgesetz (VSBG) und ODR-Verordnung, allgemeines Wettbewerbsrecht usw.).

Der Datenschutzhinweis der Kanzlei muss nach § 13 TMG u. a. folgende Angaben enthalten: Angaben zum Verantwortlichen, Art und Umfang der Datenverarbeitung, Angaben zur Datenübermittlung an Dritte (z. B. durch Einbindung von PlugIns oder Tracking Tools), Informationen zum Widerspruchsrecht.

9.3 Rechte betroffener Personen

Jede betroffene Person kann die nachfolgend aufgeführten Betroffenenrechte (Art. 15 bis 21 DSGVO) jederzeit ausüben. Da die betroffene Person Anfragen an den Verantwortlichen leicht (ohne große Hürden) stellen können muss, empfiehlt es sich, hierzu einen entsprechenden Prozess einzuführen.

9.3.1 Identitätsprüfung

Übt eine betroffene Person ein Betroffenenrecht aus, so muss der Verantwortliche die Identität der betroffenen Person feststellen. Dabei ist eine Plausibilitätsprüfung ausreichend. Verwendet die betroffene Person beispielsweise eine Adresse, mit der sie zuvor mit dem Verantwortlichen korrespondiert hat, darf eine Auskunft an diese Adresse versendet werden.

Kann der Verantwortliche die Identität nicht feststellen, so muss die Ausübung eines Betroffenenrechts verweigert, die anfragende Person unterrichtet und der Vorgang dokumentiert werden.

9.3.2 Versagungsgrund Berufsrecht

Ferner muss der Verantwortliche überprüfen, ob die Ausübung eines Betroffenenrechts im Konflikt mit dem Berufsrecht steht. Ist dies der Fall, so muss der betroffenen Person die Ausübung ihres Betroffenenrechts verweigert, sie muss unterrichtet und der Vorgang muss dokumentiert werden.

9.3.3 Fristwahrung und Protokollierung

Ein Betroffenenrecht muss in der Regel spätestens innerhalb eines Monats gewährt werden (Art. 12 Abs. 3 DSGVO).

Alle Vorgänge im Zusammenhang mit Betroffenenrechten müssen nachvollziehbar dokumentiert werden.

9.4 Auskunftsrechte

Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob die betreffenden personenbezogenen Daten verarbeitet werden.

9.4.1 Form und Inhalt der Auskunft

Der Verantwortliche muss der betroffenen Person Auskunft über die zu ihr verarbeiteten personenbezogenen Daten geben und folgende Informationen zur Verfügung stellen, sofern sie Gegenstand der Anfrage sind (Art. 15 Abs. 1 DSGVO):

a) die Verarbeitungszwecke;

b) die Kategorien personenbezogener Daten, die verarbeitet werden;

c) die Empfänger oder Kategorien von Empfängern (z. B. Finanzbehörden, Sozialversicherungsträger etc.), gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen;

d) falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

e) das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;

f) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;

g) wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten (z. B. Rückmeldungen von Finanzbehörden und Sozialversicherungsträgern);

h) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gem. Art. 22 Abs. 1 und 4 und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person (z. B. automatisierte Bewerber-Auswahl-Verfahren auf Kanzleiwebseiten).

9.4.2 Auskunftsverweigerung

Die Auskunft muss verweigert werden, wenn sie in Konflikt mit den Rechten und Freiheiten anderer betroffener Personen oder mit dem Berufsrecht steht.

9.4.3 Arbeitshilfe – Verfahrensdokumentation zur Erfüllung der Auskunftspflichten

1. **Arbeitsanweisung für Kanzleiangehörige für das Verhalten im Fall eines Auskunftsbegehrens:**

□ keine Auskunftserteilung über personenbezogene Daten und Mandatsgeheimnisse am Telefon, sofern Anrufer nicht als persönlich bekannter Mandant erkannt wird

□ keine Auskunftserteilung per unverschlüsselter E-Mail, sofern auskunftsbegehrender Mandant nicht zuvor in unverschlüsselte E-Mail-Korrespondenz eingewilligt hat

□ im Zweifel Telefonnotiz aufnehmen, Rückruf ankündigen und Auskunftsmöglichkeit durch Berufsträger prüfen lassen ► weiter mit Ziff. 2

2. Es besteht keine Pflicht zur Auskunftserteilung, soweit

□ Informationen offenbart würden, die durch einen Mandanten an den Steuerberater als Berufsgeheimnisträger im Rahmen des Mandatsverhältnisses übermittelt wurden, soweit nicht das Interesse der betroffenen Person an der Informationserteilung überwiegt,

□ auf andere Art und Weise erlangte Informationen offenbart würden, die dem Berufsgeheimnis des Steuerberaters unterliegen, soweit nicht das Interesse der betroffenen Person an der Informationserteilung überwiegt,

□ die Daten nur deshalb gespeichert sind, weil sie aufgrund von Aufbewahrungsvorschriften nicht gelöscht werden dürfen und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde, sowie eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist oder

□ die Daten ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde, sowie eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist.

► Besteht keine Auskunftspflicht:

□ Die Gründe der Auskunftsverweigerung müssen dokumentiert werden.

□ Die Ablehnung der Auskunftserteilung muss gegenüber der betroffenen Person begründet werden, sofern damit nicht der mit der Auskunftsverweigerung verfolgte Zweck gefährdet wird.

► Besteht eine Auskunftspflicht: weiter mit Ziff. 3

3. Besteht eine Auskunftspflicht, muss Auskunft über folgende Informationen gegeben werden:

□ die Verarbeitungszwecke

□ die Kategorien personenbezogener Daten, die verarbeitet werden

□ die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen

□ falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer

□ das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung

□ das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde

□ wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten

Form der Auskunftserteilung

□ Auskunft wird elektronisch beantragt (z. B. per E-Mail): Bereitstellung in einem gängigen elektronischen Format (z. B. als PDF durch Übersendung oder Bereitstellung zum Download), sofern die betroffene Person nicht ein anderes Format angibt

□ Auskunft wird in sonstiger Weise begehrt: Übersendung oder Bereitstellung einer lesbaren Kopie auf Papier

9.5 Recht auf Berichtigung

Berichtigungen müssen vor ihrer Umsetzung geprüft werden.

Der Verantwortliche muss auf Anfrage der betroffenen Person unrichtige oder unvollständige personenbezogene Daten unverzüglich berichtigen oder vervollständigen.

9.6 Recht auf Löschen/Recht auf Vergessenwerden

9.6.1 Löschungsverweigerung

Eine Löschung darf nicht vorgenommen werden, wenn sie im Konflikt mit anderen rechtlichen Verpflichtungen steht.

Beispiel: Ein ehemaliger Mitarbeiter des Mandanten verlangt die Löschung von Dokumenten mit seinen Daten, für die eine Aufbewahrungsfrist einzuhalten ist.

Des Weiteren darf die Löschung aus eigenen Interessen verweigert werden.

Beispiel: Der Mandant verlangt eine vollständige Löschung seiner Daten, obwohl er die Rechnung über eine Gestaltungsberatung noch nicht ausgeglichen hat. Der Verantwortliche benötigt die Daten zur zivilrechtlichen Durchsetzung seines Vergütungsanspruchs.

9.6.2 Löschungsumfang

Sofern die Löschanfrage der betroffenen Person berechtigt ist, müssen alle personenbezogenen Daten der betroffenen Personen aus den Datenbeständen gelöscht werden.

9.7 Recht auf Einschränkung der Verarbeitung

Unter Einschränkung der Verarbeitung ist z. B. die Beschränkung von Zugriffsrechten auf Mandantendaten zu verstehen.

Beispiel: Trotz Löschungswunsch des ehemaligen Mandanten werden die Daten aus eigenen Interessen weiter aufgehoben und der Zugriff auf den Berufsträger beschränkt.

Der Verantwortliche muss prüfen, ob die gesetzlichen Voraussetzungen zur Einschränkung der Verarbeitung der personenbezogenen Daten der betroffenen Person vorliegen (Art. 18 Abs. 1 DSGVO). Bei positiver Prüfung muss der Verantwortliche die Verarbeitung personenbezogener Daten der betroffenen Person aussetzen.

9.8 Recht auf Datenportabilität

Der Verantwortliche muss auf Antrag der betroffenen Person die sie betreffenden personenbezogenen Daten, in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung stellen.

Verlangt die betroffene Person eine Übermittlung ihrer Daten an einen Dritten, so muss der Verantwortliche dem nachkommen.

Beispiel: Der Mandant wechselt den Steuerberater. Die Verpflichtung zur Herausgabe der Handakte folgt aus § 66 Abs. 2 StBerG i. V. m. §§ 667, 675 BGB.

9.9 Widerspruchsrecht

Der Verantwortliche muss im Falle eines berechtigten Widerspruchs die Verarbeitung der personenbezogenen Daten der betroffenen Person beenden.

Beispiel: Der Mandant widerruft seine Einwilligung zum Erhalt eines Newsletters. Wenn er trotz Widerrufs den Newsletter weiter erhält, kann er dieser Verarbeitung seiner personenbezogenen Daten widersprechen.

Ausnahmsweise muss die Verarbeitung dann nicht beendet werden, wenn der Verantwortliche zwingende schutzwürdige Gründe für die Verarbeitung nachweisen kann, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen. Die Verarbeitung darf entgegen einem Widerspruch fortgesetzt werden, wenn diese der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dient.

10. Datenschutzorganisation

10.1 Kanzleileitung

Die Kanzleileitung ist verantwortlich für das Datenschutzmanagement in der Kanzlei.

10.2 Datenschutzbeauftragter

Sofern dies gesetzlich gefordert ist, hat die Kanzleileitung einen Datenschutzbeauftragten zu benennen.

10.2.1 Kriterien zur Benennung

Gemäß § 38 BDSG-2018 ist ein Datenschutzbeauftragter durch den Verantwortlichen zu bestellen, wenn dieser in der Regel mindestens 10 Personen mit der automatisierten Verarbeitung beschäftigt. Die Voraussetzungen richten sich an der Personenanzahl aus, unabhängig von deren arbeitsrechtlichem Status oder deren Arbeitszeit. Auch Auszubildende, Praktikanten, freie Mitarbeiter, Teilzeitkräfte oder Rechtsreferendare etc. sind zu berücksichtigen.

Noch nicht abschließend geklärt ist, ob der/die Kanzleiinhaber mitzurechnen ist/sind.

Darüber hinaus ist ein Datenschutzbeauftragter zu benennen, wenn der Verantwortliche eine Verarbeitung vornimmt, die der Datenschutz-Folgenabschätzung (DSFA) unterliegt, § 38 BDSG-2018 *(siehe unten Ziff. 10.3.6*). Steuerberater benötigen für ihre Kerntätigkeit keine DSFA (siehe dazu auch die Arbeitshilfe des BayLDA „Anforderungen für Steuerberater“: https://www.lda.bayern.de/de/kleine-unternehmen.html). Die Notwendigkeit könnte sich jedoch aus einem anderen Kontext (z. B. Videoüberwachung) ergeben und sollte dann entsprechend geprüft werden.

10.2.2 Interner oder externer Datenschutzbeauftragter

Für den Verantwortlichen besteht die Möglichkeit der Bestellung eines internen oder externen Datenschutzbeauftragten.

Datenschutzbeauftragter 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/-Betreuer.

10.2.3 Anforderung an die Person des Datenschutzbeauftragten

Der Datenschutzbeauftragte muss auf der Grundlage seiner beruflichen Qualifikation und des Fachwissens benannt werden. Das erforderliche fachliche Niveau bestimmt sich nach den Datenverarbeitungsvorgängen und dem erforderlichen Schutz der verarbeiteten personenbezogenen Daten. Der Datenschutzbeauftragte muss seine Aufgaben unabhängig erfüllen können. Ein Interessenkonflikt mit anderen Aufgaben darf nicht bestehen. Verwandtschaftsverhältnisse sind unbeachtlich.

10.2.4 Benennung

Die Benennung eines Datenschutzbeauftragten sollte aus Beweisgründen schriftlich erfolgen.

10.2.5 Veröffentlichung und Meldung der Kontaktdaten

Der Verantwortliche muss die Kontaktdaten des Datenschutzbeauftragten veröffentlichen und sie der zuständigen Aufsichtsbehörde mitteilen. Eine funktionsbezogene E-Mail-Adresse, unter der der Datenschutzbeauftragte erreichbar ist, ist ausreichend (z. B. datenschutz@.....de).

10.2.6 Stellung des Datenschutzbeauftragten

Der Verantwortliche muss sicherstellen, dass der Datenschutzbeauftragte seine Aufgaben rechtskonform erfüllen kann. Hierzu gehört

- die frühzeitige Einbindung des Datenschutzbeauftragten in Datenschutzvorhaben,
- die Bereitstellung der erforderlichen Ressourcen zur Aufgabenerfüllung,
- die Bereitstellung der Ressourcen zur Fortbildung des Datenschutzbeauftragten,
- die Unabhängigkeit des Datenschutzbeauftragten bei der Ausübung seiner Aufgabe,
- das Verbot, den Datenschutzbeauftragten zu benachteiligen,
- das Recht, dass der Datenschutzbeauftragte direkt bei der Kanzleileitung vortragen kann,
- das Recht, dass betroffene Personen sich direkt an den Datenschutzbeauftragten wenden können,

- die Wahrung der Geheimhaltung und der Vertraulichkeit durch den Datenschutzbeauftragten,

- der Ausschluss von Interessenkonflikten des Datenschutzbeauftragten bei der Wahrnehmung anderer Aufgaben.

10.2.7 Aufgaben des Datenschutzbeauftragten

Der europäische Verordnungsgeber beschreibt den Mindestumfang der Aufgaben des Datenschutzbeauftragten in Art. 39 DSGVO.

10.3 Datenschutzmanagement

Zur Wahrung der Rechte der betroffenen Personen muss der Verantwortliche ein Datenschutzmanagement einführen.

Ein evtl. vorhandener Datenschutzbeauftragter ist nicht Teil des Datenschutzmanagements der Kanzlei.

10.3.1 Plan-Do-Check-Act-Zyklus (PDCA)

Das Datenschutz-Management kann sich beispielsweise am Prinzip des PDCA-Zyklus orientieren:

Plan
- Erhebung und Dokumentation der Stammdaten des Verantwortlichen
- Bestimmung und Dokumentation des räumlichen und sachlichen Anwendungsbereichs
- Bestimmung und Dokumentation der Datenschutzanforderungen
- Erstellung des Verzeichnisses der Verarbeitungstätigkeiten
- Erhebung und Dokumentation der
  - betroffenen Personen und ihre personenbezogenen Daten
  - Hardware und Software
  - Auftragsverarbeiter und Garantien
  - Datenübermittlungen
- Durchführung einer Datenschutz-Risikoanalyse
- Erstellung einer Erklärung zur Anwendbarkeit

Do
- Umsetzung eines Datenschutz-Risikobehandlungsplans
- Mitarbeiterschulung, Training und Awareness
- Betrieb der Datenschutzprozesse (z. B. Einhaltung der Betroffenenrechte, Pflege des Verzeichnisses der Verarbeitungstätigkeiten)

Check
- Interne Datenschutz-Audits

Act
- Mechanismus zur Behandlung von Abweichungen und Nicht-Konformitäten

10.3.2 Verantwortlichkeiten

Die Gesamtverantwortung für den Datenschutz verbleibt beim Verantwortlichen (Kanzleileitung). Sie geht auch nicht auf den evtl. vorhandenen Datenschutzbeauftragten über.

Zuständigkeiten für Verpflichtungen aus der DSGVO können delegiert werden. Dies ist klar zu kommunizieren und zu dokumentieren.

10.3.3 Mitarbeiterschulung und -sensibilisierung

Der Verantwortliche muss sicherstellen, dass alle Beschäftigten bei der Einstellung über den Kanzlei-Datenschutz allgemein und rollenspezifisch unterrichtet werden. Die Unterrichtung erfolgt in dem Umfang, dass der Beschäftigte in der Lage ist, seine Aufgaben im Datenschutz zu erfüllen.

Eine neue Unterrichtung muss erfolgen, wenn

- rollenspezifische Datenschutzregelungen verändert worden sind,
- sich der Aufgabenbereich des Mitarbeiters verändert oder
- der Mitarbeiter dies wünscht, weil er sich unsicher fühlt.

Hiervon unabhängig müssen Datenschutzschulungen regelmäßig wiederholt werden. Aus- und Fortbildungsmaßnahmen im Datenschutz sollten in geeigneter Weise dokumentiert werden.

10.3.4 Verzeichnis der Verarbeitungstätigkeiten

Der Verantwortliche muss ein Verzeichnis der Verarbeitungstätigkeiten führen. Dieses Verzeichnis ist die wesentliche Grundlage für die Erfüllung der Verpflichtungen nach der DSGVO. Es ermöglicht eine strukturierte Datenschutzdokumentation und den Nachweis, dass der Verantwortliche seiner Rechenschaftspflicht nachkommt.

Das Verzeichnis ist regelmäßig zu überprüfen und bei Veränderung zu aktualisieren.

Das Verzeichnis der Verarbeitungstätigkeiten des Verantwortlichen muss die Angaben nach Art. 30 Abs. 1 DSGVO enthalten. Diese sind im nachfolgenden Muster enthalten.

Die Dokumentation der Löschfristen erfolgt ausschließlich in einem separaten Dokument (siehe unten Ziff. 13.2 Löschkonzept).

Das Verzeichnis der Verarbeitungstätigkeiten ist schriftlich oder elektronisch so zu führen, dass unmittelbar auf diese Angaben von der Kanzleileitung oder dem Datenschutzbeauftragten zurückgegriffen werden kann.

Auf Anfrage wird das Verzeichnis der zuständigen Aufsichtsbehörde zur Verfügung gestellt.

10.3.5 Muster: Verzeichnis der Verarbeitungstätigkeiten

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	

Das Muster ist außerdem über die Webseiten der BStBK und des DStV abrufbar:

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

https://www.dstv.de/fuer-die-praxis/arbeitshilfen-praxistipps

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

10.3.6 Datenschutz-Folgenabschätzung

Der Verantwortliche prüft, ob eine DSFA erforderlich ist. Diese ist dann durchzuführen, wenn durch die Verarbeitung für die betroffene Person voraussichtlich ein hohes Risiko für deren Rechte und Freiheiten entsteht. Ein hohes Risiko kann insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung vorliegen.

Leistungen des Steuerberaters im Rahmen der berufsrechtlichen und sonstigen gesetzlichen Vorgaben bei der Berufsausübung (z. B. StBerG; AO) stellen kein hohes Risiko dar, da er sich ausschließlich im gesetzlichen Rahmen bewegt und daher per se angemessene Schutzmaßnahmen vorhanden sind. Eine DSFA ist daher nicht erforderlich.[8]

Etwas anderes gilt, wenn neue Technologien, die kein anerkannter Standard sind, verwendet werden oder Verarbeitungen außerhalb der üblichen Berufsausübung vorgenommen werden (z. B. großflächige Videoüberwachung). Ist eine DSFA durchzuführen, ist der Rat des Datenschutzbeauftragten einzuholen. Sofern ein solcher noch nicht bestellt ist, ist ein Datenschutzbeauftragter zu benennen (siehe oben Ziff. 10.2).

[8] Siehe BayLDA: https://www.lda.bayern.de/media/muster_4_steuerberater.pdf

11. Meldeprozess bei Schutzverletzungen (Datenpannen)

An die Melde- und Dokumentationspflichten werden formell und inhaltlich unterschiedlich hohe Anforderungen gestellt.

11.1 Meldung der Datenschutzverletzung gegenüber der Aufsichtsbehörde

Begründet wird die Meldepflicht an die Aufsichtsbehörde mit Eintritt einer Datenschutzverletzung; darunter wird allgemein die Vernichtung, der Verlust, die Veränderung oder die unbefugte Offenlegung personenbezogener Daten verstanden, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

Die Meldepflicht besteht jedoch nicht, sofern sie voraussichtlich nur ein geringfügiges Risiko für die Rechte der betroffenen Personen darstellt, also die Datenpanne voraussichtlich nicht zu physischen, materiellen oder immateriellen Schäden des Mandanten führt. Wann ein solches für die Meldepflicht erforderliches Risiko im Einzelnen anzunehmen ist, lässt die DSGVO offen. Das ein Risiko begründende Zusammenspiel aus Schwere und Eintrittswahrscheinlichkeit wird durch die Aufsichtsbehörden erst noch zu konkretisieren sein.

Formell muss die Meldepflicht keinen Formanforderungen genügen; aus Beweisgründen sollte die gewählte Form jedenfalls dokumentationsfähig sein (etwa Schriftform, elektronische Form). Sie hat darüber hinaus unverzüglich und möglichst binnen 72 Stunden zu erfolgen. Die Frist beginnt in dem Zeitpunkt, in dem die Verletzung dem Verantwortlichen bekannt wurde.

Inhaltlich werden die Anforderungen der Meldepflicht dahingehend ausgestaltet, dass der Steuerberater die Art der Verletzung (die mindestens die Art der Verletzung und die ungefähre Anzahl der betroffenen Personen umfasst), die wahrscheinlichen Folgen und die durch ihn ergriffenen Abhilfemaßnahmen zu beschreiben hat. Darüber hinaus hat er den Datenschutzbeauftragten zu benennen. Da der Gesetzgeber genauere Angaben nicht gemacht hat, werden für die weitere Auslegung die Ausführungen der Aufsichtsbehörden sowie die der Datenschutzverbände heranzuziehen sein.

11.2 Meldung der Datenschutzverletzung gegenüber den betroffenen Personen

Über die Datenschutzverletzung hat der verantwortliche Steuerberater auch die betroffenen Personen zu unterrichten, sofern die Datenschutzverletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen zur Folge hat. Auch der Begriff des hohen Risikos wird durch die Aufsichtsbehörden und die Datenschutzverbände erst noch zu konkretisieren sein.

Auch bei hohen Risiken kann die Benachrichtigungspflicht entfallen: Eine Informationspflicht darf unterbleiben, wenn der Verantwortliche vorab durch eine Verschlüsselung oder nachträglich durch geeignete Sicherheitsmaßnahmen dafür gesorgt hat, dass das hohe Risiko „aller Wahrscheinlichkeit nach“ nicht mehr besteht. Die Informationspflicht kann auch wegfallen, wenn diese nur mit einem unverhältnismäßig hohen Aufwand umgesetzt werden könnte. In diesen Fällen genügt eine öffentliche Bekanntmachung durch den Verantwortlichen etwa über die Unternehmenswebsite.

11.3 Dokumentation der Datenschutzverletzung

Um der Aufsichtsbehörde die Kontrolle über die Einhaltung der Meldepflicht zu ermöglichen, hat der Verantwortliche schließlich jede Verletzung des Schutzes personenbezogener Daten zu dokumentieren. Die Dokumentationspflicht besteht im Gegensatz zur Meldepflicht nicht erst dann, wenn ein Risiko für die Rechte und Freiheiten der betroffenen Person zu erwarten sind, sondern bei jeder Datenschutzverletzung. Von der Dokumentationspflicht umfasst sind die mit der Verletzung in Zusammenhang stehenden Fakten, deren Auswirkungen und die ergriffenen Abhilfemaßnahmen. Die daraus hervorgehende Aufzeichnung hat der Verantwortliche zunächst nur zu verwahren, bis die Aufsichtsbehörde sie zu Kontrollzwecken ausdrücklich verlangt.

12. Weitergabe von Daten

Zu gewährleisten ist, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Verpflichtung zur Vertraulichkeit und Integrität, Art. 32 Abs. 1 Lit. b) DSGVO).

12.1 Schutzmaßnahmen

Eine geeignete Schutzmaßnahme ist insbesondere die Verwendung von Verschlüsselungsverfahren, die dem jeweiligen Stand der Technik entsprechen. Dies gilt auch für den Transport von Daten auf mobilen Datenträgern (z. B. USB-Stick). Des Weiteren sind Dateien und Datenträger vor Weitergabe auf Virenfreiheit zu überprüfen.

Vor einer Übermittlung ist immer nochmals die Überprüfung des/der Empfänger vorzunehmen, damit die Daten in die richtigen Hände gelangen.

12.2 Exkurs: Umgang mit E-Mails

Der Umgang mit E-Mails könnte z. B. wie folgt geregelt werden:

- Offensichtlich unsinnige E-Mails, insbesondere solche von unbekannten Absendern, sind ungeöffnet zu löschen.

- Auch bei E-Mails von vermeintlich bekannten bzw. vertrauenswürdigen Absendern ist stets zu prüfen, ob die Nachricht inhaltlich und sprachlich zum Absender passt und ob die Anlage auch erwartet wurde.

- Beim Eintreffen mehrerer E-Mails mit gleichlautendem Betreff ist besondere Achtsamkeit geboten.

- E-Mails von unbekannten Absendern, die zwar nicht offenkundig sinnlos, aber auch nicht mit einer (qualifizierten) elektronischen Signatur versehen sind, sind mit Vorsicht zu behandeln.

- E-Mail-Anhänge sind nur dann zu öffnen, wenn sie von einem vertrauenswürdigen Absender stammen und vorher auf Viren, Trojaner etc. untersucht wurden.

- Vertrauliche Nachrichten und Anlagen sind nur verschlüsselt per E-Mail zu versenden.

- Der Versand von ausführbaren Programmen (*.com, *.exe) und Skriptsprachen (*.vbs, *.bat) ist zu vermeiden und falls trotzdem nötig, ist dieser wie bei Office-Dateien (*.doc, *.xls, *.ppt) vorher mit dem Empfänger abzustimmen.

- Aufforderungen zur Weiterleitung einer E-Mail mit Viruswarnung, Anhängen etc. an Geschäftspartner, Freunde, Bekannte oder Kollegen sind grundsätzlich nicht zu befolgen.

- Auch bei E-Mails sind die Aufbewahrungspflichten gemäß Berufsrecht und Steuerrecht zu beachten.

- Der Spam-Ordner ist regelmäßig auf relevante Posteingänge zu überprüfen.

In Ausnahmefällen kann mit dem Mandanten vereinbart werden, dass vertrauliche Nachrichten und Anlagen, die keine personenbezogenen Daten Dritter enthalten, unverschlüsselt versendet werden. Dies sollte dokumentiert werden.

Bei Verschlüsselung von E-Mails, E-Mail-Anhängen etc. ist zu beachten, dass die Betreffzeile in der Regel nicht verschlüsselt wird. Dadurch können u. U. Rückschlüsse auf den Inhalt einer verschlüsselten Mail gezogen werden.

12.3 Verschlüsselungsanforderungen

12.3.1 Vergabe von Passwörtern

Ein Passwort dient zur Authentifizierung, also zum Nachweis der Identität der Person und der dieser Person zugeteilten Berechtigungen.

Auf der Internetseite des Bundesamtes für Sicherheit in der Informationstechnologie (BSI, www.bsi-fuer-buerger.de) werden die jeweils aktuellen sicheren Passwortverfahren dargestellt. Weitere Empfehlungen sind auf den Seiten von Deutschland sicher im Netz (DsiN, www.sicher-im-netz.de) abrufbar.

12.3.2 Anforderungen an electronic-Banking

Soweit der Steuerberater Zahlungen für seine Mandanten auf elektronischem Weg erledigt, sind dem Vertrauensverhältnis entsprechend besondere Sicherheitsmechanismen einzurichten. Diese können aus der Einschaltung eines sicheren Serviceproviders oder der Nutzung von E-Banking-Programmen und der zusätzlich gesicherten Aufbewahrung der Zugangs- und Transaktionscodes bestehen.

Es ist darauf zu achten, dass bei allen Browser- oder Client-basierten E-Banking-Systemen eine Verschlüsselung der Datenübertragung seitens der Banken gewährleistet ist.

Um die Gefahr von Phishing und Pharming zu vermeiden, sind die von den Banken zur Verfügung gestellten Zugangsberechtigungen nicht weiter zu geben bzw. nicht ungeschützt im Computer zu hinterlegen.

12.4 Webformulare

Bei der datenschutzrechtlichen Gestaltung von Webformularen (z. B. Kontaktformulare, Anmeldeformulare, Rückrufformulare, Online-Bewerbungsmasken) sind die folgenden Aspekte zu beachten:

- Diese Formulare müssen vor dem Hintergrund der Datenminimierung auf die erforderlichen Angaben beschränkt werden.

- Im Datenschutzhinweis des Internetauftritts muss ein Hinweis auf die bei der Nutzung des Formulars entstehende Datenverarbeitung erfolgen.

- Der Internetauftritt muss zudem über eine Seitenverschlüsselung verfügen.

Auch bei Logins zu geschlossenen Benutzerbereichen oder Filesharing-Plattformen[9] ist die Sicherstellung der nach aktuellem Stand der Technik verschlüsselten Übertragung der Daten zu prüfen.

13. Aufbewahrungsfristen

Die Aufbewahrungsfristen richten sich nach dem Zweck der Verarbeitung. Diese können sich aus den rechtlichen Aufbewahrungspflichten, den Einwilligungen der betroffenen Personen sowie aus der Erforderlichkeit zur Vertragsabwicklung ergeben.

Jede Kanzlei muss als Verantwortliche im Verarbeitungsverzeichnis u. a. die Fristen aufführen, nach deren Ablauf die Löschung der verschiedenen Datenkategorien vorgesehen ist. Grundsätzlich muss die Löschung vorgesehen werden, wenn der Zweck und Rechtsgrund der Datenverarbeitung wegen Zeitablaufs wegfällt (Grundsatz der Rechtmäßigkeit der Verarbeitung).

13.1 Aufbewahrungspflichten

Zunächst ergeben sich Aufbewahrungspflichten aus Steuer- und Handelsrecht. Dabei ist zu beachten, dass Aufbewahrungspflichten des Mandanten häufig im Rahmen des Auftrages vom Steuerberater übernommen werden.

Die Aufbewahrungsfrist läuft nicht ab, solange die Unterlagen für Steuern von Bedeutung sind, deren Festsetzungsfrist noch nicht abgelaufen ist (Ablaufhemmung).

---

[9] Z. B. Adisson OneClick, DATEV Unternehmen online, hmd.NetArchiv, andere ASP-Lösungen etc.

Schriftstücke (Daten), die der Verantwortliche aus Anlass seiner beruflichen Tätigkeit vom Auftraggeber oder für ihn erhalten hat (Handakte gem. § 66 StBerG), sind grundsätzlich für die Dauer von 10 Jahren nach Auftragsbeendigung aufzubewahren. Diese Verpflichtung erlischt bei Übergabe der Handakten an den Mandanten. Die Aufbewahrungspflicht erlischt zudem 6 Monate, nachdem der Mandant die Aufforderung erhalten hat, die Handakten in Empfang zu nehmen.

Somit ist eine Aufbewahrungsfrist von 10 Jahren unabdingbar. Es empfiehlt sich jedoch, eine Löschung erst nach einem pauschalen Sicherheitszuschlag (z. B. aus Gründen der Ablaufhemmung) von 4 Jahren vorzunehmen.

Nach diesem Zeitraum von 14 Jahren ist einzelfallbezogen zu prüfen, ob Rechtfertigungsgründe für eine weitere Aufbewahrung vorliegen. Dabei ist eine ggf. längere Verjährungsfrist z. B. nach BGB zu beachten.

Rechtfertigungsgründe können sich u. a. aus folgenden Sachverhalten ergeben:

- Dokumentation einer Geschäftsaufgabeerklärung (Folgewirkung auch für Erben),
- Pensionszusage,
- Grundstückskaufvertrag,
- Absicherung der Verfolgungsmöglichkeit von titulierten Vergütungsansprüchen,
- Änderung aufgrund neuer Tatsachen,
- Verteidigungsmöglichkeiten gegen denkbare Haftungsforderungen des Mandanten wegen erst zukünftig eintretenden Schäden.

Dokumente mit personenbezogenen Daten, die nicht nach Steuer-, Handels- oder Berufsrecht aufbewahrungspflichtig sind, dürfen nur so lange aufbewahrt werden, wie hierfür ein Rechtfertigungsgrund vorliegt.

Beispiel: Unterlagen eines abgelehnten Bewerbers sollten spätestens 6 Monate nach Zugang des Absageschreibens gelöscht werden, sofern keine Ansprüche wegen Benachteiligung nach dem Allgemeinen Gleichbehandlungsgesetz (AGG) geltend gemacht werden. Dies müsste nach dem AGG innerhalb von 2 Monaten nach Zugang der Ablehnung erfolgen. Eine weitere Karenzzeit von bis zu 4 Monaten erscheint jedoch angemessen, um in Zweifelsfällen Unsicherheiten im Hinblick auf den Zugangszeitpunkt der Ablehnung ausräumen zu können.

13.2 Löschkonzept

Im Verarbeitungsverzeichnis müssen die vorgesehenen Löschfristen für die verschiedenen Datenkategorien festgehalten sein (Art. 30 Abs. 1 Satz 2 Buchst. f) DSGVO). Dies kann durch Verweis auf ein separates Dokument erfolgen.

Ein Muster ist über die Webseiten der BStBK und des DStV abrufbar:

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

https://www.dstv.de/fuer-die-praxis/arbeitshilfen-praxistipps

Aufgrund der Rechenschaftspflicht muss der Verantwortliche die geeigneten technischen und organisatorischen Maßnahmen zur Einhaltung des Grundsatzes zur zeitlichen „Speicherbegrenzung" nachweisen können (Art. 5 Abs. 2 DSGVO). Der Zeitpunkt der Löschung (Löschfristen) bestimmt sich aus dem Zeitpunkt der Zweckerfüllung der Verarbeitung unter Berücksichtigung der Aufbewahrungspflichten (siehe Ziff. 13.1).

Bei den zu dokumentierenden Löschfristen wird eine Karenzzeit von weiteren 6 Monaten als vertretbar angesehen, nach deren Ablauf die Dokumente mit personenbezogenen Daten unwiederbringlich gelöscht sein müssen. Die Karenzzeit ist erforderlich, um im Rahmen der EDV-Organisation ein sicheres und praktikables Löschverfahren zu ermöglichen und um ggf. fälschlicherweise oder unbeabsichtigt gelöschte Dokumente wiederherstellen zu können.

Zu den Grenzen einer zulässigen Aufbewahrungsdauer sind die künftige Rechtsprechung und Veröffentlichungen der Datenschutzbehörden zu beachten.

Dokumente, die keine personenbezogenen Daten enthalten, müssen nicht gelöscht werden. Daher ist es zulässig, als Alternative zur Löschung die Anonymisierung von Dokumenten vorzusehen (z. B. durch Schwärzung der personenbezogenen Daten).

Im Rahmen der Kanzleiorganisation muss die Dokumentation der Löschung sichergestellt werden.

14. Beendigung des Mandats

Es empfiehlt sich bereits im Steuerberatungsvertrag Regelungen zur Kündigung des Mandatsverhältnisses schriftlich zu vereinbaren.

Das beendete Mandatsverhältnis ist inaktiv zu setzen und als beendet zu kennzeichnen.

Die Zugangs- und Zugriffsberechtigungen für Beschäftigte sind einzuschränken. So sollten insbesondere neue Beschäftigte keinen Zugriff auf nicht mehr bestehende Mandate haben.

15. Datenschutz im Beschäftigungsverhältnis

Der Beschäftigtendatenschutz (Mitarbeiterdatenschutz) ist in der DSGVO nicht eigenständig geregelt worden. Die Regelungsbefugnis wurde durch eine Öffnungsklausel an die Mitgliedstaaten zurückgespielt. Der Art. 88 DSGVO erlaubt den Mitgliedstaaten für den Beschäftigtendatenschutz einzelstaatliche Sonderregelungen zu schaffen, davon wurde in § 26 BDSG-2018 Gebrauch gemacht.

Der Beschäftigtendatenschutz ist auch bei ausgeschiedenen Beschäftigten sicherzustellen.

Der Verantwortliche muss geeignete Maßnahmen ergreifen, um sicherzustellen, dass die Grundsätze der DSGVO, insbesondere die des Art. 5 DSGVO[10] eingehalten werden. Gerade die dort geregelten Vorgaben der Zweckbindung („geeignet"), der Pflicht zur Datenminimierung („mildestes Mittel") und der Verarbeitung nach Treu und Glauben („angemessen") entsprechen weitgehend den von der deutschen Rechtsprechung bereits in der Vergangenheit aufgestellten Anforderungen an die Verhältnismäßigkeit.

Auch im Beschäftigungsverhältnis gilt die Vorgabe, dass über jede beabsichtigte Verarbeitung personenbezogener Daten zu informieren ist. Es ist jedoch zu beachten, dass die Betroffenenrechte (vgl. Ziff. 9) nur bedingt auf das Arbeitsverhältnis übertragbar sind.

Für eine private Nutzung betrieblicher Kommunikationsmedien (z. B. E-Mail) sind klare Vereinbarungen hinsichtlich der dabei entstehenden Daten zu treffen. Im Zweifel ist von einer Erlaubnis der privaten Nutzung abzuraten.

15.1 Rechtsgrundlagen für die Verarbeitung und Auswertung von Beschäftigtendaten

Personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz, einer Betriebs- oder Dienstvereinbarung erforderlich ist.[11] Zusätzlich kann eine Verarbeitung zur Wahrung berechtigter Interessen erfolgen.[12] Hier ist zu beachten, dass die betroffene Person ein Widerspruchsrecht hat.[13]

Die Verarbeitung personenbezogener Daten von Beschäftigten kann auch auf der Grundlage einer Einwilligung erfolgen. Dabei ist zu beachten, dass diese Einwilligung freiwillig und nachweisbar erklärt wird und nicht mit anderen Vereinbarungen gekoppelt wird. Der Arbeitgeber hat den Beschäftigten über den Zweck der Datenverarbeitung und über sein Widerrufsrecht[14] in Textform aufzuklären.

Freiwilligkeit im Beschäftigungsverhältnis kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen. Dies ist z. B. denkbar bei der Einwilligung zur notwendigen Protokollierung der privaten Internetnutzung.

---

[10] Grundsätze für die Verarbeitung personenbezogener Daten.
[11] § 26 Abs.1 Satz 1 BDSG-2018.
[12] Art. 6 Abs. 1 lit. f) DSGVO.
[13] Art. 21 Abs. 1 DSGVO.
[14] Art. 7 Abs. 3 DSGVO.

Eine Auswertung personenbezogener Daten von Beschäftigten zur Aufdeckung von Straftaten und schwerwiegende vertragliche Pflichtverletzungen darf nur erfolgen, wenn[15]

- dokumentierte tatsächliche Anhaltspunkte einen entsprechenden Verdacht begründen,
- die Verarbeitung zur Aufdeckung erforderlich ist und
- das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

Hierfür ist eine umfassende Dokumentation und genaue Verhältnismäßigkeitsprüfung unumgänglich.

15.2 Umgang mit Bewerberdaten

Auch in Bewerbungssituationen greift bereits der Beschäftigtendatenschutz.

Neben den arbeitsrechtlichen Anforderungen zur Zulässigkeit von Fragen sind bei der Erhebung von Bewerberdaten auch die datenschutzrechtlichen Vorgaben zur Datenminimierung und zu den Löschfristen zu beachten.

15.3 Bilder und Kontaktdaten von Beschäftigten

Eine Datenverarbeitung ist (nur) auf rechtmäßige, nach Treu und Glauben und nachvollziehbare Weise zu einem vorher festgelegten Zweck und nicht über das notwendige Maß hinaus zulässig. Daher ist es erlaubt, die beruflichen Kontaktdaten von Beschäftigten, die Ansprechpartner für Externe sind, bekannt zu geben. In diesem Fall dürfen der Name, die Funktion und der Tätigkeitsbereich des jeweiligen Beschäftigten, sowie die dienstlichen Kontaktdaten wie E-Mail-Adresse, Telefon- und Faxnummer veröffentlicht werden.

Die Kontaktdaten weiterer Beschäftigter – z. B. die Buchführungskraft ohne Kontakt zu Mandanten – dürfen nur mit deren freiwillig erteilter Einwilligung veröffentlicht werden.

Weitergehende Daten oder Fotos dürfen nur mit Einwilligung des Beschäftigten veröffentlicht werden und nur, sofern dies der Aufgabenerfüllung dient. Bei der Wahl von Form und Inhalt der Internetveröffentlichung muss das Interesse an einer Bekanntgabe mit der Fürsorgepflicht des Arbeitgebers abgewogen werden. So kann z. B. die vollständige Namensangabe auch Stalking gegenüber Beschäftigten oder die Veröffentlichung von E-Mail-Adressen zu einer rapiden Zunahme von Spam-Mails führen.

[15] § 26 Abs. 1 Satz 2 BDSG-2018.

16. Kanzleiübertragung

Bezüglich der Kanzleiübertragung decken sich die datenschutzrechtlichen Regelungen mit den berufsrechtlichen Grundsätzen.[16] Es ist zu beachten, dass sich durch eine Kanzleiübertragung die Aufbewahrungs- und Löschfristen nicht automatisch verlängern.

Die vorliegenden Hinweise wurden von dem gemeinsamen Arbeitskreis der Bundessteuerberaterkammer und des Deutschen Steuerberaterverbandes e.V. erstellt. Diesem gehören an:

StBin Dipl.-Ök. Frauke Kaps-Offeney
RA Rudi Kramer
Dipl.-Staatswissenschaftler Dirk Munker
StB Dipl.-Volksw. Wolf Dieter Oberhauser
Dipl.-Ök. Stephan Rehfeld
RAin Nicole Schmidt, LL.M.

Ansprechpartner in der BStBK:
RAin Claudia Kalina-Kerschbaum, LL.M.
RA Martin Kader

Ansprechpartner beim DStV e.V.:
RA Dipl.-Verw. (FH) Christian Michel

[16] Siehe Hinweise der BStBK für die Praxisübertragung, Berufsrechtl. Handbuch.