Bundessteuerberaterkammer
KÖRPERSCHAFT DES ÖFFENTLICHEN RECHTS

DEUTSCHER STEUERBERATER-VERBAND e.V.

Hinweise

für den Umgang mit personenbezogenen Daten durch Steuerberater und steuerberatende Berufsausübungsgesellschaften

Stand: September 2023

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: Benennung 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 Pass-word-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 7.1.7
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 seit dem 25. Mai 2018 anzuwendende Datenschutz-Grundverordnung (DSGVO) der Europäischen Union (EU) gibt europaweit einheitliche Vorgaben an den Umgang mit personenbezogenen Daten. Um dem Berufsstand der Steuerberater eine praxisgerechte Anwendung der Vorschriften zu ermöglichen, haben die Bundessteuerberaterkammer (BStBK) und der Deutsche Steuerberaterverband e.V. (DStV) gemeinsame Praxishilfen entwickelt, 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 steuerberatende Berufsausübungsgesellschaften.

Die DSGVO ist unmittelbar und vorrangig zu allen nationalen Regelungen zum Umgang mit personenbezogenen Daten anzuwenden, soweit sie nicht Öffnungsklauseln zur Regelung von Rechtsmaterien zugunsten des nationalen Rechts enthält. Ergänzend gilt in Deutschland u. a. das Bundesdatenschutzgesetz (BDSG), das auf Basis zweier EU-Datenschutz-Anpassungs- und -Umsetzungsgesetze (DSAnpUG-EU)[1] 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 des TTDSG auf Basis der E-Privacy-Richtlinie, deren Nachfolge-Verordnung (ePV) der EU, die derzeit auf der europäischen Ebene erarbeitet und abgestimmt werden. Diese Hinweise 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[2]

„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 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] 2. DSAnpUG-EU vom 20. November 2019, BGBl. I 2019, S. 1626 ff.

[2] Männliche Formen umfassen auch die adäquaten weiblichen und diversen Formen.

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

„Weitere Auftragsverarbeiter“ bezeichnet Subauftragsverarbeiter (Unterauftragnehmer), die durch Auftragsverarbeiter für die Umsetzung eines Auftrags eines Verantwortlichen bezüglich personenbezogener Daten in Anspruch genommen werden.

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“. Kein weiterer Auftragsverarbeiter ist hingehen der Lieferant, der für das Betreiben des Rechenzentrums die erforderliche Energie liefert.

„Remote-Zugriff“ bzw. „Fernzugriff“ bedeutet, dass auf den Datenbestand von einem beliebigen Ort aus über das Internet zugegriffen wird.

„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“ (pbD) 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, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder die Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, die Verbreitung und jede andere Form der Bereitstellung, den Abgleich, die Verknüpfung, die 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. Steuerberatende Berufsausübungsgesellschaften können als Personengesellschaften oder Kapitalgesellschaften[3] organisiert sein. Bei Personengesellschaften (insbesondere GbR, oHG, KG inkl. GmbH & Co. KG) sind die Gesellschafter die „Verantwortlichen“. Zu den Personengesellschaft zählen auch die Partnerschaften mit und ohne beschränkte Berufshaftung. Hier sind die Partner die „Verantwortlichen“. Bei Kapitalgesellschaften (insbesondere GmbH, UG (haftungsbeschränkt), AG und KGaA) ist die Kapitalgesellschaft als juristische Person der „Verantwortliche“ und wird von der Geschäftsführung vertreten.

8. „Auftragsverarbeiter“ ist jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Der Auftragsverarbeiter arbeitet dabei weisungsgebunden nach den Vorgaben des Verantwortlichen. Die Fachleistung des Steuerberaters ist keine Auftragsverarbeitung.

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.

---

[3] https://www.bstbk.de/downloads/bstbk/brennpunktthemen/BStBK_Berufsausuebungsgesellschaften_FAQ-Katalog.pdf - Seite 6 unter Ziff. II.

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 rechtmäßigen Verarbeitung der sie betreffenden personenbezogenen Daten in einem bestimmten Fall einverstanden ist. Hierbei muss der Zweck der Verarbeitung klar bestimmt sein. Die Einwilligung erlischt, sobald der Zweck der Verarbeitung erfüllt ist oder die Einwilligung mit Wirkung für die Zukunft widerrufen wird.

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 Wirtschaftstätigkeit 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 im Hinblick darauf, ob ein Verstoß gegen die DSGVO vorliegt oder ob Maßnahmen gegen Verantwortliche oder Auftragsverarbeiter mit der DSGVO im 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 eine oder auf der 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 Nachweis kann ggf. Einfluss auf die Höhe von Bußgeldern haben.

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 sollte der Beratungsumfang, d. h. die vereinbarte Leistung nach dem StBerG hervorgehen und die Zweckbindung sollte 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; dabei kann es notwendig sein, eine gesonderte Einwilligung einzuholen (siehe Ziff. 5.3).

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).

5. Mandatierung

5.1 Rechtsgrundlage im Mandatsverhältnis

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

Die personenbezogenen Daten, die durch den Steuerberater verarbeitet werden, umfassen die als Stammdaten des Mandanten und diejenigen Daten, die im Rahmen der Erbringung der Steuerberaterleistungen verarbeitet werden (z. B. Daten von Debitoren, Kreditoren, Kindern oder Beschäftigten des Mandanten). Rechtsgrundlage der Weitergabe von Gesundheitsdaten oder Daten zur Religionszugehörigkeit etc. (Daten nach Art. 9 Abs. 1 DSGVO) von Arbeitnehmern durch den Mandanten an den Steuerberater ist § 26 Abs. 3 BDSG[4].

Der Steuerberater führt die im Steuerberatungsgesetz festgelegten Beratungsleistungen weisungsfrei und eigenverantwortlich aus.

Der Mandatsvertrag sollte insbesondere den Beratungsgegenstand mit Bezeichnung von Art und Umfang der erbrachten Dienstleistung und durchzuführenden Tätigkeiten (Leistungszweck), die Zweckbindung und den Verweis auf die berufsrechtlichen Verschwiegenheitsverpflichtungen regeln. Klarstellend sollte auch die eigenverantwortliche, weisungsfreie Leistungserbringung aus der Mandatierung hervorgehen.

Aus dem Berufsrecht oder dem Datenschutzrecht ergeben sich keine Formanforderungen an den Mandatsvertrag. Aus Gründen der Nachweisbarkeit empfiehlt sich, zur Erfüllung der Rechenschaftspflicht nach Art. 5 Abs.2 DSGVO eine Vereinbarung in Textform abzuschließen.

5.2 Fachleistung des Steuerberaters (keine Auftragsverarbeitung)

Die Leistung des Steuerberaters ist immer eine eigenverantwortlich erbrachte fachliche Beratung und ist somit keine Auftragsverarbeitung. Das ist auch in § 11 StBerG ausdrücklich geregelt. Dies gilt insbesondere auch für die Lohn- und Gehaltsabrechnung im Rahmen der Lohnbuchhaltung sowie für vereinbare Tätigkeiten gemäß § 57 Abs. 3 StBerG, die der Steuerberater nach dem Steuerberatungsgesetz (StBerG) immer eigenverantwortlich ausführen muss.[5] Damit muss der Steuerberater keine Verträge zur Auftragsverarbeitung mit seinen Mandanten abschließen. Im Fall des Abschlusses eines Vertrages zur Auftragsverarbeitung mit den Mandanten sind aufgrund der damit verbundenen weisungsabhängigen Verarbeitung berufsrechtliche Konsequenzen durch die zuständige Kammer bis hin zum Entzug der Zulassung denkbar.

---

[4] Siehe hierzu auch: Tätigkeitsbericht des Sächsischen Datenschutzbeauftragen 2017/2018, Teil 2, Ziff. 4.3.3., S. 211

[5] BT-Drs. 19/14909, S. 58f.; Kurzpapier Nr. 13 der Datenschutzkonferenz (DSK); Anhang B, u. a. abrufbar unter folgendem Link: https://www.lda.bayern.de/de/datenschutz_eu.html; Bayerisches Landesamt für Datenschutzaufsicht, FAQ zur DS-GVO, abrufbar unter dem folgenden Link: https://www.lda.bayern.de/media/FAQ_Steuerberater_keine_ADV.pdf ; ULD - Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Tätigkeitsbericht 2019, Ziffer 5.5.4; Bayerisches Landesamt für Datenschutzaufsicht (BayLDA), 8. Tätigkeitsbericht 2017/2018, Ziffer 9.1.

Auch die Überlassung von Software (ohne Gewinnerzielungsabsicht) stellt keine Auftragsverarbeitung im Rahmen der steuerlichen Beratung dar[6].

5.3 Mandanteninformationen

Durch den Mandatsvertrag ist der Steuerberater verpflichtet, den Mandanten auf rechtlich relevante Änderungen hinzuweisen. Entsprechende Mandanteninformationen bedürfen daher keiner weiteren datenschutzrechtlichen Grundlage. Aus der berufsrechtlichen Verpflichtung zur Beratung im Rahmen des Mandatsverhältnisses ergibt sich datenschutzrechtlich die Berechtigung, Mandanten über relevante steuerrechtliche Änderungen zu informieren.

Darüberhinausgehende werbende Inhalte darf der Verantwortliche mittels elektronischer Post (z. B. E-Mail) nur mit vorheriger Einwilligung der jeweiligen Empfänger versenden[7]. Der Verantwortliche muss die Einwilligung nachweisen (ggf. Double-Opt-In[8] bei digitaler Einwilligung) können und die Empfänger bei der Abgabe der Einwilligung auf ihr Recht zum jederzeitigen Widerspruch hingewiesen haben. Wird ein regelmäßiger Newsletter mit werblichen Inhalten auf Basis einer Einwilligung versendet, so ist in jedem Newsletter ein Abmeldelink aufzunehmen, über den der Widerruf der Einwilligung durchgeführt werden kann.

5.4 Elektronische Kommunikation

Bei Abschluss des Mandatsvertrages werden mit dem Mandanten die Wege und Regeln der elektronischen Kommunikation vereinbart.

Eine verschlüsselte E-Mail-Kommunikation mit Mandanten ist im Hinblick auf die berufsrechtlichen Verschwiegenheitspflichten dringend zu empfehlen. Über den Einsatz einer Ende-zu-Ende-Verschlüsselung ist aus Datenschutzsicht abhängig vom Risiko für die Rechte und Freiheiten der betroffenen Personen zu entscheiden. Ausreichend kann auch die sog. „Transportverschlüsselung“ sein.[9] Hierzu muss der Steuerberater sicherstellen, dass die E-Mail auf dem Transportweg verschlüsselt ist und sich die Server der E-Mail-Provider des Steuerberaters und des Empfängers in

---

6 Überlässt ein Steuerberater an den Mandanten im Rahmen des Mandatsverhältnisses Software ohne Gewinnerzielungsabsicht, so unterfällt diese Gestaltung nach der Bewertung durch den Hessischen Beauftragten für Datenschutz und Informationsfreiheit (51. Tätigkeitsbericht des Hessischen Beauftragten für Datenschutz und Informationsfreiheit, Ziffer 14.1 https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2023-04/51-taetigkeitsbericht-des-hbdi_0.pdf#page=217&zoom=auto,-341,595) nicht den Anforderungen einer Auftragsverarbeitung nach Art. 28 DSGVO. Den Ausführungen lag der Sachverhalt zugrunde, dass ein Steuerberater seinen Mandanten ein System zur Verfügung stellt, mit dem die Mandanten Dokumente in einen Cloud-Speicher laden können. Der Steuerberater übernimmt die vom Mandanten in den Cloud-Speicher geladenen Dateien dann in seine IT-Systeme. Das System dient vor allem der sicheren Übertragung von vertraulichen Unterlagen in einer geschützten und verschlüsselten Umgebung. Zwar wird vom Steuerberater für die Nutzung des Systems durch die Mandanten eine Vergütung verlangt. Diese orientiert sich aber an den Selbstkosten. Eine Absicht der Gewinnerzielung ist damit nicht verbunden. Zweck des Systems ist nicht die Verarbeitung der Daten nach Weisung des Mandanten, sondern vielmehr die sichere Übermittlung der Daten an den Steuerberater. Sie ist daher eine Nebenleistung des Steuerberatungsvertrages.

7 § 7 UWG

8 Double Opt-In umfasst eine Einwilligung des Empfangs an eine angegebene E-Mail-Adresse und die Bestätigung dieser E-Mail-Adresse über eine an diese Adresse gesandte E-Mail.

9 Vgl. Orientierungshilfe der DSK vom 16. Juni 2021 zu Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail unter https://www.datenschutzkonferenz-online.de/media/oh/20210616_orientierungshilfe_e_mail_verschluesselung.pdf.

Deutschland befinden. Will der Mandant eine Ende-zu-Ende-Verschlüsselung, so ist dem zu entsprechen.

Wird der Verzicht auf eine Ende-zu-Ende-Verschlüsselung der Kommunikation durch den Mandanten gewünscht, ist der Mandant auf die damit verbundenen Gefahren, z. B. die einer unbefugten Kenntnisnahme durch Dritte, hinzuweisen. Es ist ihm zu erläutern, dass diese Zustimmung durch ihn ohne Vertretungsmacht nicht für die Daten Dritter, wie z. B. von Beschäftigten, Kindern, Ehepartnern etc., abgegeben werden kann. Dieser Vorgang ist gesondert zu dokumentieren.

Die Zustimmung eines Beschäftigten zum unverschlüsselten Versand sollte grundsätzlich unmittelbar von diesem stammen. Veranlasst der Arbeitgeber eine solche Zustimmung des Beschäftigten, ist dies rechtlich problematisch und sollte daher nicht ohne weiteres berücksichtigt werden.

Da es sich bei Daten, die im Zusammenhang mit der Lohnbuchhaltung ausgetauscht werden, in der Regel um besonders schutzwürdige Daten handelt, sind hier besonders strenge Maßstäbe anzuwenden. Beim Einsatz einer Transportverschlüsselung ist zum Beispiel darauf zu achten, dass diese Daten beim Empfänger nur von der berechtigten Person abgerufen und damit zur Kenntnis genommen werden können, so sollte zum Beispiel keine Versendung an ein allgemein zugängliches Firmenpostfach (info@...) erfolgen.

Die obigen Ausführungen zur E-Mail-Kommunikation gelten sinngemäß auch für andere Formen der elektronischen Kommunikation (z. B. Nutzung von Datenräumen, Videokonferenzen). Eine Nutzung von Diensten, bei denen Daten unverschlüsselt außerhalb des Geltungsbereichs der DSGVO (zwischen-)gespeichert werden, ist datenschutzrechtlich bedenklich. Soweit sich unverschlüsselte Daten (zeitweise) außerhalb der Bundesrepublik Deutschland befinden, sind die weitergehenden Regelungen des Berufsrechts zusätzlich zu beachten.

Die Anforderungen an eine rechtskonforme Übermittlung werden auch durch den Einsatz von Portallösungen erfüllt, bei denen der Empfänger lediglich eine Information erhält, dass neue Inhalte hinterlegt wurden. Der Zugang erfolgt dann über eine Authentifizierung. Hier ist der Einsatz einer Zwei-Faktor-Authentifizierung zu empfehlen.

Auch beim Telefax handelt es sich um eine Form der elektronischen Kommunikation. Seine Verwendung erfüllt jedoch nicht die Anforderungen an eine Ende-zu-Ende-Verschlüsselung.

5.5 Zulässigkeit der Verarbeitung von personenbezogenen Daten zur Gratulation

Im Rahmen des Kanzleimarketings ist es angemessen, für die Pflege des Mandantenverhältnisses den Mandanten zu besonderen Anlässen per Briefpost zu kontaktieren, ohne dass dafür eine gesonderte Einwilligung des Mandanten erforderlich ist. Die Verwendung der im Rahmen des Mandatsverhältnisses erhobenen Daten des Mandanten können z. B. für Gratulationen (zu Geburtstagen, Jubiläen etc.) oder Einladungen z. B. zu Sommerfesten verwendet werden.[10] Der Steuerberater weist die betroffene Person darauf hin, dass sie die Möglichkeit zum Widerspruch haben, eine Begründung ist bei Widersprüchen gegen Direktwerbung nicht erforderlich[11] In den

[10] Zulässig nach den Grundsätzen der Zweckänderung gemäß Art. 6 Abs. 4 DSGVO.
[11] Art. 21 Abs. 3 DSGVO

Datenschutzhinweisen der Kanzlei an den Mandanten ist auf diese Form des Kanzleimarketings verpflichtend hinzuweisen.

6. Organisation in der Kanzlei

Unabhängig von den Regelungen zum Datenschutz sind Steuerberater aufgrund ihrer berufsrechtlichen Regelungen zur Verschwiegenheit und damit zum Datenschutz verpflichtet. § 62 StBerG bestimmt, dass die Beschäftigten in der Kanzlei und gemäß § 62a StBerG auch weitere Personen, die in einer sonstigen Hilfstätigkeit an der beruflichen Tätigkeit mitwirken, 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 vertrauliche Unterlagen, 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. Auch sollte der Serverraum nicht als Abstellkammer (z.B. für Reinigungsutensilien o.a.) verwendet werden. Durch die Maßnahmen soll verhindert werden können, so dass niemand unbemerkt die Kanzleiräume betreten kann. Besprechungsräume sollten so gelegt werden, dass für externe Besuchende durch das Aufsuchen der Besprechungsräume keine Kenntnis von anderen Mandaten ermöglicht wird.

6.2 Zugang (Benutzerverwaltung)

Der Zugang zu den IT-Systemen wird durch eine personenbezogene Benutzerverwaltung (Einzel-Account) gewährleistet. Der Benutzer ist verpflichtet, sich persönlich mit einem individuellen Benutzernamen und einem individuellen Passwort im System anzumelden.[12] Sofern technisch möglich, ist eine Zwei-Faktor-Authentifizierung einzusetzen (vgl. Ziffer 6.4.2). Bei Beschäftigten, die aus der Kanzlei ausscheiden, ist sicherzustellen, dass diesen auch die Zugangsberechtigungen bei eingesetzten Dienstleistern unverzüglich entzogen werden.

6.3 Zugriff (Rechteverwaltung)

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

- die Position innerhalb der Aufbauorganisation (z. B. Inhaber bzw. Geschäftsführer, Gruppenleiter, fachlicher Mitarbeiter etc., aber auch die Zugehörigkeit zu bestimmten Abteilungen),

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

- das berufliche Qualifikationsniveau (z. B. Berufsträger, Steuerfachwirt etc.),
- die 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. Die Überprüfung sollte entsprechend den Hinweisen unter Ziff. 6.6 dokumentiert werden.

6.3.2 Benutzerregelung, Zugriffsrechte

Im Rahmen eines risikobasierten Schutzkonzeptes (vgl. Ziffer 6.5) ist unter Berücksichtigung des Interesses des Mandanten, ggf. jederzeit Informationen zur beauftragten Angelegenheit zu bekommen, mandats- und auftragsbezogen zu prüfen, 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 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 (Remote-Verbindung)

Im Fall von Remote-Verbindungen sind weitere Sicherheitsmaßnahmen entsprechend dem Stand der Technik[13] erforderlich, um den Zugang von Unbefugten zu verhindern.

6.4.1 Berechtigte Nutzung von Endgeräten

Der Zugang zu internen IT-Systemen von außerhalb des Kanzlei-Netzes (LAN und WLAN) erfolgt nur durch Endgeräte, die von der Kanzlei zur Verfügung gestellt werden. Deren Einrichtung und Wartung erfolgt nur durch den Verantwortlichen bzw. einen von ihm beauftragten und überwachten IT-Dienstleister. Auch auf den für den Remote-Zugang zugelassenen Endgeräten ist eine personenbezogene Benutzerverwaltung einzurichten.

[13] Hinweise zum Stand der Technik gibt Teletrust: https://www.teletrust.de/publikationen/broschueren/stand-der-technik/

6.4.2 Zweistufiges Anmeldekonzept (2-Faktor-Authentifizierung, 2FA)

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

6.4.3 Datenschutz bei Tätigkeiten außerhalb von Kanzleien

6.4.3.1 Unterscheidung von Homeoffice und mobilem Arbeiten

Für das Arbeiten außerhalb der Betriebsstätte gibt es unterschiedliche Bezeichnungen: Homeoffice, Telearbeit, Remote-Arbeit, mobiles Arbeiten. Gesetzlich definiert ist derzeit nur Telearbeit in § 2 Abs. 7 ArbStättV:

> „*Telearbeitsplätze sind vom Arbeitgeber fest eingerichtete Bildschirmarbeitsplätze im Privatbereich der Beschäftigten, für die der Arbeitgeber eine mit den Beschäftigten vereinbarte wöchentliche Arbeitszeit und die Dauer der Einrichtung festgelegt hat. Ein Telearbeitsplatz ist vom Arbeitgeber erst dann eingerichtet, wenn Arbeitgeber und Beschäftigte die Bedingungen der Telearbeit arbeitsvertraglich oder im Rahmen einer Vereinbarung festgelegt haben und die benötigte Ausstattung des Telearbeitsplatzes mit Mobiliar, Arbeitsmitteln einschließlich der Kommunikationseinrichtungen durch den Arbeitgeber oder eine von ihm beauftragte Person im Privatbereich des Beschäftigten bereitgestellt und installiert ist*.“

Wichtig ist dabei, dass dem Arbeitgeber bei Telearbeit auch die Verpflichtung zur vollständigen Ausstattung des dortigen Arbeitsplatzes, also auch z. B. Bürostuhl und Arbeitstisch, obliegt. Während bei der ausschließlichen Telearbeit die gesamte Arbeitsleistung von Beschäftigten aus dem Homeoffice erbracht wird, ist hiervon die Unterform der alternierenden Telearbeit zu unterscheiden. Bei der alternierenden Telearbeit erbringen Beschäftigte einen Teil ihrer Arbeitsleistung aus dem Homeoffice und einen anderen Teil ihrer Arbeitsleistung in der Kanzlei vor Ort. Arbeiten Beschäftigte außerhalb der Kanzleiräumlichkeiten, verfügen aber nicht über einen durch den Arbeitgeber fest eingerichteten Arbeitsplatz, so wird dies als mobiles Arbeiten bezeichnet. Weitere Beispiel für mobiles Arbeiten können auch das Arbeiten in der Bahn, im Flugzeug, im Hotel auf Dienstreisen, aber auch in den Räumlichkeiten des Mandanten sein.

Es wird in den vorliegenden Hinweisen daher allgemein von „mobilem Arbeiten“ gesprochen, um nicht durch Begrifflichkeiten weitere und dann oft unbeabsichtigte rechtliche Verpflichtungen einzugehen. Vom Begriff des mobilen Arbeitens wird dann nicht nur die Leistungserbringung von Zuhause aus umfasst, sondern generell das Arbeiten außerhalb der Kanzleiräumlichkeiten. Zu beachten ist, dass bei Tätigkeiten außerhalb von Deutschland auch weitere Punkte, wie sozialversicherungsrechtliche, lohnsteuerrechtliche oder berufsrechtliche Aspekte, zu berücksichtigen sind.

6.4.3.2 Zulässigkeit der Arbeit als mobiles Arbeiten

Grundsätzlich wird im Arbeitsvertrag geregelt, wo die vertraglich geschuldete Arbeitsleistung erbracht wird. Außer in den Fällen, in denen der Gesetzgeber, z. B. wie in den Fällen einer

pandemischen Lage, für bestimmte Tätigkeiten die Erbringung der geschuldeten Leistung in den Räumen des Arbeitgebers untersagt, ist eine Leistungserbringung außerhalb der vereinbarten Räumlichkeiten nur in beiderseitigem Einverständnis möglich, sofern nicht die arbeitgeberseitige Dispositionsbefugnis greift. Weitere arbeitsrechtliche Aspekte sind gegebenenfalls zu beachten.

Datenschutzrechtlich bleibt der Arbeitgeber auch bei Tätigkeiten außerhalb der Kanzleiräume weiterhin für die Einhaltung der datenschutzrechtlichen und berufsrechtlichen Anforderungen verantwortlich. Dies umfasst alle Grundsätze der DSGVO:

Eine systematische Prüfung der Datenschutzgrundsätze[14] zeigt, dass mobile Arbeit lediglich eine Auswirkung auf die bereits getroffenen Informationssicherheitsmaßnahmen von Verarbeitungstätigkeiten hat. Ist eine Verarbeitungstätigkeit personenbezogener Daten in den Kanzleiräumen zulässig, so gilt dies grundsätzlich auch für Tätigkeiten außerhalb der Kanzleiräume, wenn die erforderlichen technischen und organisatorischen (Schutz-)Maßnahmen von der Kanzlei ergriffen worden sind.

6.4.3.3 Bestimmung der erforderlichen technischen und organisatorischen Maßnahmen

Die erforderlichen technischen und organisatorischen (Schutz-)Maßnahmen müssen von der Kanzlei im Rahmen einer Datenschutz-Risikobeurteilung bestimmt werden (Art. 24 Abs. 1 DSGVO und Art. 32 Abs. 1 DSGVO). Dabei fließen auch die Anforderungen an die berufsrechtliche Verschwiegenheits- und Aufbewahrungspflicht mit ein, die letztendlich auch nicht-personenbezogene Informationen umfassen. Hierbei sollten die konkreten Schwachstellen mindestens für die folgenden Bedrohungen bestimmt werden[15]:

- Offenbarung personenbezogener Daten
- Diebstahl von Eigentum der Kanzlei und von personenbezogenen Daten
- Verlust von Eigentum der Kanzlei und von personenbezogenen Daten
- Nicht-autorisierte Nutzung der Kanzlei-IT
- Abhorchen von personenbezogenen Daten bei der Übermittlung
- Aushorchen der Mitarbeiter im Homeoffice/am mobilen Arbeitsplatz

Es gibt zu den datenschutzrechtlichen Anforderungen an die Maßnahmen auch Checklisten und weitere Informationen der Datenschutzaufsichtsbehörden[16], die dabei herangezogen werden können.

6.4.3.4 Beispiel zur Identifikation einer Schwachstelle

Bei der Bestimmung der Schwachstellen beim mobilen Arbeiten entstehen durch das häusliche Umfeld Szenarien, die im reinen Kanzleiumfeld nicht relevant sind. So werden in Haushalten z. B. Sprachassistenten zur Steuerung von IT oder auch Haushaltsgeräten verwendet. Es müssen von

---

[14] Siehe Kapitel 3 zu Artikel 5 DSGVO.

[15] Eine umfassende Übersicht kann z. B. beim BSI eingesehen werden: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/04_OPS_Betrieb/OPS_1_2_4_Telearbeit_Edition_2021.pdf?__blob=publicationFile&v=2

[16] Siehe https://www.lda.bayern.de/media/checkliste/baylda_checkliste_homeoffice.pdf; https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BlnBDI-Heimarbeit.pdf; https://lfd.niedersachsen.de/download/157542/Datenschutz_im_Homeoffice.pdf

der Kanzlei also Maßnahmen (Arbeitsanweisungen) vorgegeben werden, die gewährleisten, dass personenbezogene Daten beim mobilen Arbeiten während Telefonaten oder Videokonferenzen nicht unbefugt durch Sprachassistenten im dortigen Umfeld aufgenommen und eventuell sogar in unsichere Drittstaaten übermittelt werden.

Die Einflussnahme und Kontrollmöglichkeiten des Arbeitgebers in den privaten Räumen der Beschäftigten sind naturgemäß eingeschränkt, sodass eine Gestattung der mobilen Arbeit durch den Arbeitgeber von der Beachtung der Sicherheitsvorgaben abhängig gemacht werden sollte.

Die betroffenen Mitarbeiter müssen dazu geschult werden, damit sie in der Lage sind, die getroffenen erforderlichen technischen und organisatorischen Maßnahmen umzusetzen.

6.4.3.5 Weitergabe der privaten Kontakt- oder Kommunikationsdaten von Beschäftigten

Auch beim mobilen Arbeiten sind die Vorgaben zur Datenminimierung zu beachten. Dies betrifft insbesondere die privaten Kontakt- oder Kommunikationsdaten von Beschäftigten wie Telefonnummern oder private E-Mail-Adressen, die an Mandanten, andere Kanzleimitarbeiter oder Lieferanten weitergegeben werden sollen. Dies kann vermieden werden, indem die Beschäftigten durch die Kanzlei mit den entsprechenden Geräten (z. B. Diensthandy, Dienst-E-Mail-Adresse) ausgestattet werden. Jede andere Gestaltung unter Einbindung der privaten Kontakt- und Kommunikationsdaten bringt datenschutzrechtliche Anforderungen mit sich, die kaum noch rechtskonform darstellbar sind.

6.4.3.6 Überprüfung der Einhaltung der Datenschutzmaßnahmen bei mobilem Arbeiten

Die Kanzlei ist als Verantwortliche nach der DSGVO verpflichtet sicherzustellen, dass personenbezogene Daten datenschutzkonform verarbeitet werden. Sie muss dies auch nachweisen können (Art. 24 Abs. 1 DSGVO). Wurde von der Kanzlei ein Datenschutzbeauftragter benannt, so umfasst dessen Aufgabenbereich die Überprüfung der Einhaltung der Datenschutzvorschriften auch beim mobilen Arbeiten (Art. 39 Abs. 1 lit. b) DSGVO).

Ein unangemeldeter Besuch in den Privaträumen eines Beschäftigten durch den Arbeitgeber tangiert viele rechtliche Themen. Selbst die Aufnahme der Gestattung eines Zutrittsrechts zur Überprüfung der Einhaltung der Schutzmaßnahmen zur Datenverarbeitung innerhalb der Wohnung des Beschäftigten schließt nicht aus, dass die Rechte anderer Mitbewohnender entgegenstehen können, über die die Beschäftigten selbst nicht disponieren können. Es empfiehlt sich daher, in die Vereinbarung zur Gestattung des mobilen Arbeitens aufzunehmen, welche Schutzmaßnahmen die Beschäftigten – abhängig von den konkreten Umständen vor Ort - einzuhalten haben und dass sie ggf. für die Einhaltung nachweispflichtig sind[17]Auch kann ein regelmäßiges Selbstaudit der Beschäftigten vereinbart werden, bei dem das Vorhandensein und die Verwendung bestimmter Schutzmaßnahmen durch die Beschäftigten bestätigt werden.

Im Rahmen einer Prüfung durch die zuständige Datenschutzaufsichtsbehörde kann es erforderlich sein, dass ein Behördenmitarbeiter Zutritt zu den privaten Räumlichkeiten der Beschäftigten verlangt. In der Praxis wird dies nur bei schwerwiegenden Vorkommnissen in Betracht kommen. In diesen Fällen ist dann auch davon auszugehen, dass die Behörde im Rahmen der Amtshilfe

[17] Hinsichtlich der Einzelheiten verweisen wir auf unsere Prüfliste zum Datenschutz im Homeoffice/beim mobilen Arbeiten.

polizeiliche Unterstützung zur Umsetzung einfordert. Für diese Extremfälle sind die Beschäftigten darauf hinzuweisen, dass unverzüglich die Kanzleileitung zu informieren ist, um ggf. eine rechtliche Prüfung der Vereinbarkeit mit den Beschränkungen des § 29 Abs. 3 Satz 1 BDSG[18] herbeizuführen.

6.4.3.7 Einzelthemen

6.4.3.7.1 Transport und Entsorgung

Dürfen Beschäftigte Unterlagen und Datenträger zum Zwecke der mobilen Arbeit aus den Kanzleiräumen mitnehmen, sind Vorgaben zu treffen, wie diese beim Transport zu schützen sind, z. B. durch nicht einsehbare Behältnisse. Hinsichtlich der Entsorgung, z. B. von Papier-Dokumenten oder Datenträgern, sind die gleichen Vorgaben wie in den Kanzleiräumen zu beachten, damit z. B. Unterlagen nicht ungeschreddert über die private Papierentsorgungstonne der Beschäftigten entsorgt werden. Informationen, die der berufsrechtlichen Verschwiegenheit unterliegen und im Anschluss in einer Abfallentsorgung entsorgt werden sollen, sind mindestens mit Sicherheitsstufe P4 (Partikelgröße max. 160 mm²)[19] zu shreddern[20]. Bei Entsorgung über den Hausmüll empfiehlt sich die Verwendung der Sicherheitsstufe P5 (Partikelgröße max. 30 mm²). Bei Beauftragung eines externen Aktenvernichtungsunternehmens ist zusätzlich darauf zu achten, dass die Vernichtung nach Schutzklasse 3 zu erfolgen hat. Wenn dies beim mobilen Arbeiten nicht gewährleistet werden kann, ist die Entsorgung über den Rücktransport in die Kanzleiräume sicherzustellen.

6.4.3.7.2 Keine Nutzung privater Geräte der Beschäftigten

Auch das mobile Arbeiten erfolgt nur durch Endgeräte, die von der Kanzlei zur Verfügung gestellt werden. Deren Einrichtung und Wartung erfolgt nur durch den Verantwortlichen bzw. einen von ihm beauftragten und überwachten IT-Dienstleister. Auch auf zugelassenen Endgeräten ist eine personenbezogene Benutzerverwaltung einzurichten. Von einer Erlaubnis zur privaten Nutzung dieser Endgeräte wird abgeraten.

6.4.3.7.3 Erfassung der Arbeitszeit

Auch bei mobilen Tätigkeiten außerhalb der Kanzleiräume ist der Arbeitgeber für die Einhaltung gesetzlicher Arbeitszeitvorschriften verantwortlich und muss dies auch nachweisen können. Dies berechtigt aber nicht zu Maßnahmen, die zu einer Dauerüberwachung der Beschäftigten führen, wie z. B. eine Anweisung, dauerhaft die Videokamera eines IT-Systems angeschaltet zu lassen. Hier können auch eigene Zeitaufschreibungen der Beschäftigten Berücksichtigung finden, die durch den Arbeitgeber auf Plausibilität geprüft werden können.

---

[18] Gegenüber den in § 203 Abs. 1, 2a und 3 des Strafgesetzbuchs genannten Personen oder deren Auftragsverarbeitern bestehen die Untersuchungsbefugnisse der Aufsichtsbehörden gemäß Artikel 58 Abs. 1 Buchstabe e und f der Verordnung (EU) 2016/679 nicht, soweit die Inanspruchnahme der Befugnisse zu einem Verstoß gegen die Geheimhaltungspflichten dieser Personen führen würde.

[19] DIN 66399 ISO/IEC 21964.

[20] So der Bundesbeauftragte für Datenschutz und Informationssicherheit in einer Broschüre, auf die er verweist und an der er mitwirkte: https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Technik/Datenschutzgerechte-Datentr%C3%A4gervernichtung.html mit Verweis auf https://www.gdd.de/gdd-arbeitshilfen/gdd-ratgeber/datenschutzgerechte-datentraegervernichtung-4-aufl-2019-1 und dort Seite 28 und auch der Hessische Beauftragte für Datenschutz und Informationsfreiheit im Tätigkeitsbericht 2020 unter Ziffer 11.7 (Seite 111).

6.4.3.7.4 Videokonferenzen

Bei Videokonferenzen mit Beschäftigten außerhalb der Kanzleiräume ist ein System einzusetzen, bei dem der Hintergrund durch die Beschäftigten so einstellbar ist, dass diese selbst entscheiden, ob Details aus der Privatwohnung erkennbar sind oder nicht.

6.5 Risikobasierte Schutzkonzepte

Für die Festlegung der Zugriffsberechtigungen (vgl. Ziffer 6.3.2) 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 (vgl. Ziff. 5.3).

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, Tracking Tools auf Webseiten ohne eigene Zwecke[21], Aktenvernichtungsunternehmen, Letter-Shops, E-POST, Internet-Service-Providern und Application-Service-Providern (ASP) Auftragsverarbeitung. Fernwartungen und Wartungen vor Ort an Applikationen mit personenbezogenen Daten gelten gemäß den deutschen Aufsichtsbehörden ebenfalls als Auftragsverarbeitung[22].

---

[21] Google Analytics behält sich selbst eigene Zwecke vor, sodass dessen Einsatz nicht mehr als Auftragsverarbeitung subsumiert werden kann.

[22] DSK-Kurzpapier Nr. 13 vom 16. Januar 2018 (s. o.).

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

Erforderlich ist der Abschluss eines Vertrages zur Auftragsverarbeitung zumindest in Textform. Die Inhalte des Vertrags müssen mindestens den Vorgaben des Art. 28 DSGVO entsprechen.

Die EU-Kommission hat mittlerweile von ihrer Möglichkeit Gebrauch gemacht, Standardvertragsklauseln gemäß Art. 28 Abs. 6 DSGVO zu veröffentlichen[23]. Deren Anwendung ist jedoch nicht verbindlich. Es gibt auch Musterverträge von Verbänden[24], die eingesetzt werden können. In jedem Fall sind solche Vorgaben auf den tatsächlichen Fall anzupassen.

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 die Vereinbarung eventueller Änderungen/Ergänzungen kommt neben der Schriftform auch die Textform in Frage. Die Unterlagen sind aufzubewahren.

7.1.3 Muster: Zusatzvereinbarung zum Auftragsverarbeitungsvertrag (nicht anwendbar auf die EU-Standardvertragsklauseln gem. Art. 28 Abs. 6 DSGVO)

Anlage zum Dienstleistungsvertrag vom ……

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

[23] https://eur-lex.europa.eu/eli/dec_impl/2021/915/oj

[24] Hier z. B. des bitkom https://www.bitkom.org/Bitkom/Publikationen/Praxisleitfaeden-zur-Auftragsverarbeitung

I. Der Auftraggeber belehrt die Firma

……..……
– nachstehend Dienstleister 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 Dienstleister ein in Ausübung oder bei Gelegenheit der Dienstleistung 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 Dienstleister an der Dienstleistung mitwirken oder für ihn tätige Datenschutzbeauftragte (§ 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 Dienstleister nicht um eine natürliche Person, trifft die Strafandrohung die für den Dienstleister mitwirkenden natürlichen Personen.

4. Im Fall der Einschaltung Dritter (z. B. Subunternehmer) macht sich der Dienstleister 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 Dienstleister 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 Jahre 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 Dienstleister verpflichtet sich gegenüber dem Auftraggeber sowie den beim Auftraggeber tätigen Berufsgeheimnisträgern wie folgt:

1. Der Dienstleister wirkt an den Tätigkeiten der Berufsgeheimnisträger mit, die einer beruflichen Verschwiegenheitsverpflichtung unterliegen. Der Dienstleister wahrt in Kenntnis der strafrechtlichen Folgen einer Verletzung der Verschwiegenheitspflicht und unter Berücksichtigung der mit dem Auftraggeber vereinbarten Vertragsbestimmungen zur Verschwiegenheit fremde Geheimnisse, die ihm zugänglich gemacht werden. Der Dienstleister wird verpflichtet, die zur Verfügung

gestellten Mandantendaten nicht in anderem als dem vertraglich beschriebenen Umfang zu nutzen.

2. Der Dienstleister ist befugt, weitere Personen (Dritte) zur Erfüllung des Vertrages heranzuziehen. Beim Einsatz von Dritten (z. B. Subunternehmer) verpflichtet sich der Dienstleister, 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.

3. Der Dienstleister ist verpflichtet, sich nur insoweit Kenntnis von fremden Geheimnissen zu verschaffen, als dies zur Vertragserfüllung erforderlich ist. Der Auftraggeber wird dem Dienstleister nur insoweit Kenntnis von fremden Geheimnissen verschaffen, als dies zur Vertragserfüllung erforderlich ist. Der Dienstleister 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 Dienstleistungsverhältnisses zeitlich unbegrenzt fort.

5. Die Pflicht zur Verschwiegenheit gemäß den vorstehenden Absätzen besteht nicht, soweit der Dienstleister 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 Dienstleister den Auftraggeber über die Pflicht zur Offenlegung vorab in Kenntnis setzen.

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

.....
(Ort, Datum)

....
(Unterschrift Dienstleister) (Unterschrift Auftraggeber)

Hinweis: die Belehrung kann auch in Textform erfolgen. Allerdings sollte der Zugang beim Dienstleister nachweisbar sein.

7.1.4 Kontrolle

Der Verantwortliche muss die vertragsgemäße Erfüllung der Auftragsverarbeitung regelmäßig, und im Fall von Datenschutzverletzungen durch den Dienstleister idealerweise unverzüglich,

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 Remote-Verbindung 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)

In der Praxis ist es in der Regel angezeigt, in den Auftragsverarbeitungsvertrag eine Regelung aufzunehmen, die bestimmt, dass die Beauftragung weiterer Auftragsverarbeiter durch die Auftragsverarbeiter der Kanzlei nur mit schriftlicher (oder elektronischer) Zustimmung erfolgt. Bei Abschluss eines Vertrags zur Auftragsverarbeitung sind die beauftragten weiteren Auftragsverarbeiter zu benennen. Erteilt der Verantwortliche dem Auftragsverarbeiter eine allgemeine Genehmigung zur Hinzuziehung weiterer Auftragsverarbeiter, so hat der Auftragsverarbeiter den Verantwortlichen über jede beabsichtigte Hinzuziehung eines weiteren Auftragsverarbeiters zu informieren, um sicherzustellen, dass der Verantwortliche in begründeten Einzelfällen die Hinzuziehung untersagen kann. Die vertraglich zu regelnde Reaktionszeit für die Untersagung sollte nicht zu kurz bemessen sein.

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.

Die EU-Kommission hat in 2021 neue, an die DSGVO angepasste Standarddatenschutzklauseln veröffentlicht[25], die bei der Drittstaatenübermittlung herangezogen werden können, um eine der über Art. 46 Abs. 2 lit. c DSGVO geeignete Garantie sicherzustellen.

Aufgrund des Urteils des EuGH vom 16. Juli 2020[26] („Schrems II“), sind außer bei einem Angemessenheitsbeschluss nach Art. 45 DSGVO zusätzliche Maßnahmen zu ergreifen, um sicherzustellen, dass im empfangenen Drittstaat ein angemessenes Datenschutzniveau besteht.

---

[25] https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=de&uri=CELEX%3A32021D0914

[26] C-311/18 - https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1

Bezogen auf Datenübermittlungen aus dem Raum der EU/ des EWR in die USA ist durch die EU-Kommission ein Verfahren zum Beschluss eines angemessenen Schutzniveaus eingeleitet worden[27]. Dieses ist bis zum Stand der Veröffentlichung dieser Hinweise noch nicht abgeschlossen.

7.2 Gemeinsame Verantwortliche (Shared Services)

Legen zwei oder mehr Verantwortliche die Zwecke und Mittel der Verarbeitung fest, so sind sie gemeinsame Verantwortliche.[28] 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, aber auch die Nutzung von Facebook Fanpages.[29] Nach Auffassung der Aufsichtsbehörden handelt es sich auch um Gemeinsame Verantwortliche, wenn Dienste auf der Webseite eingebunden sind, die sich ausdrücklich eigene Verarbeitungszwecke vorbehalten (z. B. Google Analytics).[30]

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 eigenständigen Verantwortlichen.[31]
Für die Verarbeitung (einschließlich Übermittlung) personenbezogener Daten muss eine Rechtsgrundlage gemäß 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[32].

Exkurs: Schutz der IT-Infrastruktur vor Schadsoftware

Zur Bestimmung der erforderlichen Maßnahmen zum Schutz einer Kanzlei-IT-Infrastruktur vor Schadsoftware muss eine Datenschutz-Risikoanalyse nach Art. 32 DSGVO durchgeführt und regelmäßig wiederholt werden. Bei neuen Bedrohungen, wie es z. B. der Fall war bei dem Trojaner Emotet, oder Bedrohungen, bei deren Risikobeurteilung oder Risikobehandlung in der Kanzlei nicht

---

27 https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7631
28 Art. 26 Abs. 1 Satz 1 DSGVO.
29 EuGH, Urteil vom 5. Juni 2018, Az: C-210/16; BVerwG, Urteil vom 11. September 2019 – 6 C 15/18.
30 Siehe Beschluss der DSK (Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder) vom 12. Mai 2020, S. 2 – 3 Abschnitt II.
31 Kurzpapier Nr. 13 der Datenschutzkonferenz vom 16. Januar 2018, Anhang B
32 Die Regelungen des Art. 25 DSGVO sind zu beachten.

ausreichend Erfahrung besteht, empfiehlt sich als vertrauenswürdige Informationsquelle z. B. das Bundesamt für Sicherheit in der Informationstechnik (BSI)[33].

9. Informationspflichten bei Datenerhebung und Betroffenenrechte

Den Betroffenenrechten, z. B. der Erfüllung der Auskunfts- und Informationspflichten, ist in präziser, transparenter, verständlicher und leicht zugänglicher Form sowie in einer klaren und einfachen Sprache Geltung zu verschaffen. Die Übermittlung der Informationen erfolgt in Abstimmung mit der betroffenen Person schriftlich oder in anderer Form, ggf. auch elektronisch.

9.1 Informationspflichten

Über die Informationspflichten werden die datenschutzrechtlichen Transparenzanforderungen umgesetzt. Die betroffenen Personen sind bei der ersten Datenerhebung oder bei einer Zweckänderung zu informieren.

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 bei Verantwortlichen mit Sitz außerhalb der EU/des EWR)

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, Zahlungsdienstleister)

7. Drittstaatentransfer

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

- geplante Speicherdauer oder – falls dies nicht möglich ist – die Kriterien für die Festlegung der Speicherdauer,

[33] Zielgruppenorientierte Informationen zum Emotet-Trojaner können unter https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2018/BSI_warnt_vor_Emotet.html abgerufen werden, m. w. N.

- Betroffenenrechte: Auskunfts-, 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 angestrebte Auswirkung einer solchen Verarbeitung.

9.1.2 Ausnahmen

Die Informationen müssen nicht gegeben werden, wenn die betroffene Person bereits über diese Informationen verfügt. Hierüber muss ein Nachweis geführt werden können.

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 die berufsrechtliche Verschwiegenheit verletzt wird, und er muss eine solche Verletzung verhindern.

Beispiel: Lohn- und Gehaltsabrechnung

Im Rahmen der Betreuung von Lohnmandaten verarbeitet 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, es sei denn, 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 bei der betroffenen Person erhoben, so müssen ihr die Informationen 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.

□ durch die Informationserteilung die öffentliche Sicherheit oder Ordnung gefährdet würde und die Interessen des Verantwortlichen an der Nichterteilung der Information die Interessen der betroffenen Person überwiegen.

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) Dabei ist zu beachten,

dass die DSGVO hier mit „Vertreter“ in Art. 4 Nr. 17 die Person meint, die durch den Verantwortlichen außerhalb der EU gemäß Art. 27 DSGVO bestellt wurde.

□ Kontaktdaten des Datenschutzbeauftragten – sofern vorhanden (funktionsbezogene, nichtpersonifizierte 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 einem 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.

□ 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

□ Ggf. Hinweis auf Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling (involvierte Logik, Tragweite und angestrebte Auswirkungen)

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 nicht gem. Ziff. 3.1 ausgeschlossen, müssen der betroffenen Person folgende Informationen mitgeteilt werden:

□ die oben in Ziff. 2 genannten Informationen und

□ 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 auf der Webseite[34]

Von jeder Seite aus müssen die Datenschutzhinweise erreichbar sein (z. B. im Footer).[35] 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

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

[35] Im Übrigen sind noch weitere Pflichten ohne unmittelbaren Bezug zum Datenschutzrecht zu beachten, die im Rahmen dieser Hinweise nicht behandelt werden (Pflichtangaben auf der Webseite (z. B. § 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 dem Verbraucherstreitbeilegungsgesetz (VSBG) und ODR-Verordnung, allgemeines Wettbewerbsrecht usw.).

- Hinweis auf das berechtigte Interesse, sofern 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 EU-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

Der Datenschutzhinweis der Kanzlei muss nach Art. 13, 14 DSGVO 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. Besteht keine andere Möglichkeit der Identifizierung (vorhandene Angaben zu Kommunikationskanälen), so kann der Verantwortliche auch einen amtlichen Ausweis einsehen oder eine Kopie (geschwärzt um die nicht relevanten Angaben) verlangen.

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). Diese Frist kann um weitere zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist. Der Verantwortliche unterrichtet die betroffene Person innerhalb eines Monats nach Eingang des Antrags über eine Fristverlängerung, zusammen mit den Gründen für die Verzögerung. Stellt die betroffene Person den Antrag elektronisch, so ist sie nach Möglichkeit auf elektronischem Weg zu unterrichten, sofern sie nichts anderes angibt.

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 der 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 im Ausnahmefall (z. B bei unzumutbar hohem Aufwand) die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen[36]

□ – 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

[36] EuGH, Urteil vom 12. Januar 2023, C-154/21, unter: https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62021CJ0154

□ 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 nichts anderes angibt. □ Auskunft wird in sonstiger Weise begehrt: Übersendung oder Bereitstellung einer lesbaren Kopie auf Papier □ Daten von Dritten sind unkenntlich zu machen

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 Widerruf und Widerspruch

Die betroffene Person kann jederzeit die Verarbeitung auf Basis einer Einwilligung durch Widerruf beenden lassen. Der Widerruf kann gegenüber dem Verantwortlichen mittels der bekannten Kommunikationswege erklärt werden.

> **Beispiel:** Der Mandant widerruft seine Einwilligung zum Erhalt eines Newsletters mit werblichen Inhalten. In diesem Fall darf dem Mandanten mit Wirkung für die Zukunft kein Newsletter mehr übersandt werden.

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

> **Beispiel:** Der Mandant widerspricht der Gratulation zu persönlichen Ereignissen (z. B. Geburtstag, Hochzeitstag etc.) durch den Steuerberater. Zukünftig dürfen keine entsprechenden Glückwünsche mehr ausgesprochen werden.

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 ist ein Datenschutzbeauftragter durch den Verantwortlichen zu bestellen, wenn dieser in der Regel mindestens 20 Personen[37] ständig mit der automatisierten Verarbeitung beschäftigt. Die Voraussetzungen richten sich an der Personenanzahl aus, unabhängig von deren arbeitsrechtlichem Status oder deren Arbeitszeit. Auch Kanzleiinhaber, Auszubildende, Praktikanten, freie Mitarbeiter, Teilzeitkräfte oder Rechtsreferendare etc. sind zu berücksichtigen.

Darüber hinaus ist ein Datenschutzbeauftragter zu benennen, wenn der Verantwortliche eine Verarbeitung vornimmt, die der Datenschutz-Folgenabschätzung (DSFA) unterliegt, § 38 BDSG (siehe unten Ziff. 10.3.6). Steuerberater benötigen für ihre Kerntätigkeit keine DSFA (siehe dazu auch die Arbeitshilfe des BayLDA „Anforderungen für Steuerberater“[38]). Die Notwendigkeit könnte sich jedoch aus einem anderen Kontext, z. B. bei permanenter Videoüberwachung von Personen, 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 Fachkenntnisse verfügt. Ausgeschlossen sind jedoch z. B. die Mitglieder der Kanzleileitung (Verantwortliche), Beschäftigte in leitender Funktion, der IT-Administrator/-Betreuer oder der Personalverantwortliche.

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.

---

[37] Änderung von 10 auf 20 Personen durch das 2. DS-AnpUG, s. o. Fn 1

[38] https://www.lda.bayern.de/media/muster_4_steuerberater.pdf

Der Datenschutzbeauftragte muss seine Aufgaben unabhängig und bezogen auf die Priorisierung und Bewertung seiner Tätigkeit weisungsfrei erfüllen können. Ein Interessenkonflikt mit anderen Aufgaben darf nicht bestehen. Verwandtschaftsverhältnisse sind unbeachtlich.

10.2.4 Benennung

Die Benennung eines Datenschutzbeauftragten sollte aus Beweisgründen zumindest in Textform 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 auf diese Angaben von der Kanzleileitung oder dem Datenschutzbeauftragten unmittelbar 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 bzw. Firma der verantwortlichen natürlichen oder juristischen Person	
Ansprechperson	
Postadresse	
Telefon	
E-Mail-Adresse	

Datenschutzbeauftragter (soweit DSB benannt wurde)	
Nachname, Vorname (Funktion ausreichend, z. B. Daten-schutzbeauftragter)	
Kontaktdaten, wie z. B. Postadresse, Telefon oder E-Mail-Adresse (Funktionsadresse genügt, z. B. Daten-schutzbeauftragter@Kanzlei.de)	

Verarbeitungstätigkeit lfd. Nr. 1: Lohnbuchhaltung von Mandanten	
Zwecke der Verarbeitung	Erstellung der Lohnbuchhaltung, insb. • Berechnung der Lohn- und Gehaltsansprüche • Berechnung von Abgaben und Steuern • Erstellung und Bereitstellung der Lohn- und Gehaltsnachweise • Beratung zur steuerlichen Gestaltung arbeits-rechtlicher Sachverhalte
Kategorien betroffener Personen	Beschäftigte von Mandanten
Kategorien von personenbezogenen Daten	Stammdaten der Beschäftigten, inkl. Angaben zu Familienstand, Schwerbehinderteneigenschaften und Kirchensteuerpflicht sowie Sozialdaten

	Ansprechpersonen im erforderlichen Schriftverkehr mit externen Stellen Zeitaufzeichnungen für Abrechnungserstellung
Kategorien der Empfänger, denen personenbezogene Daten übermittelt werden	• Personalabteilung • Rechnungswesen • Sozialversicherungsträger • Finanzbehörden • Kreditinstitute • Versicherungen • Gerichte • Gläubiger • IT-Dienstleister (soweit vorhanden)
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 QS-/QM-Handbuch)	
Zwecke der Verarbeitung	Erstellen von Finanzbuchhaltung und 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

	• IT-Dienstleister (soweit vorhanden)
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/themen/brennpunktthemen/datenschutz

www.stbdirekt.de

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 (Organisation zum Umgang mit Datenschutzvorfällen)
    - 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 grundsätzlich kein hohes Risiko dar, da er sich ausschließlich im gesetzlichen Rahmen bewegt und daher per se angemessene Schutzmaßnahmen vorhanden sind. Auch die Durchführung einer Lohnbuchhaltung geht über die allgemeinen Gefahren, die üblicherweise mit Datenverarbeitungstätigkeiten einhergehen, nicht hinaus.[39] Eine DSFA ist daher nicht erforderlich.[40]

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).

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 begründendes 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.

---

[39] LAG Rheinland-Pfalz, Urteil vom 29.08.2022 Az 3 Sa 203/21, RN 61.

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

Inhaltlich werden die Anforderungen der Meldepflicht dahingehend ausgestaltet, dass der Steuerberater die Art der Verletzung, (soweit möglich mit Angabe der Kategorien und der ungefähren Anzahl der betroffenen Personen), die wahrscheinlichen Folgen und die durch ihn ergriffenen Abhilfemaßnahmen zu beschreiben hat. Darüber hinaus hat er den Datenschutzbeauftragten zu benennen. Die Aufsichtsbehörden stellen auf ihren jeweiligen Webseiten Online-Meldeformulare zur Verfügung. Diese sollten für die Meldung verwendet werden.

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. Dies kann etwa der Fall sein, wenn Bankdaten einer natürlichen Person fälschlicherweise an eine unbefugte Person übermittelt wurden.

Auch bei hohen Risiken kann die Benachrichtigungspflicht entfallen: Eine Information 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 Unternehmenswebseite.

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 ist, 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. Das Online-Meldeformular der zuständigen Aufsichtsbehörde kann hier als Muster dienen.

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).[41] Des Weiteren sind Dateien und Datenträger vor

[41] Weitergehend hierzu folgend unter Ziff. 12.3.

Weitergabe und vor Einspielung der Daten in das Kanzleinetzwerk auf Virenfreiheit zu überprüfen. Die Verwendung eines Einzelrechners (Stand-Alone-PC) zur Überprüfung auf Schadsoftware kann zusätzlichen Schutz bieten.

Es bietet sich an, die jeweils aktuellen Hinweise des BSI regelmäßig zu prüfen und die notwendigen Schutzmaßnahmen zu ergreifen[42].

Vor einer Übermittlung ist immer nochmals die Überprüfung des/der Empfänger vorzunehmen, damit die Daten nur an Berechtigte übermittelt werden.

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, bevor auf Links geklickt wird oder Anlagen geöffnet werden.

- 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 durch einen aktuellen Virenscanner auf Viren, Trojaner etc. untersucht wurden.

- Der Versand von ausführbaren Programmen (*.com, *.exe) und Skriptsprachen (*.vbs, *.bat) ist zu vermeiden und – falls trotzdem nötig – 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, Handelsrecht und Steuerrecht zu beachten.

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

Zur elektronischen Kommunikation mit verschlüsselten bzw. unverschlüsselten E-Mails gelten die Ausführungen im Abschnitt 5.4.

---

[42] abrufbar unter www.bsi-fuer-buerger.de

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 ein Mandatsverhältnis und auf den Inhalt einer verschlüsselten Mail gezogen werden. Auch in diesem Kontext ist eine besondere Vorsicht bei Daten der Lohnbuchhaltung geboten, sofern sich aus der Betreffzeile sensible Informationen entnehmen lassen.

12.3 Verschlüsselung

12.3.1. Übersicht über Verschlüsselung

Verschlüsselung bezieht sich auf den Prozess der Umwandlung von lesbarem Klartext in unleserliche Zeichen oder Code, um die darin enthaltenen Informationen vor unbefugter Kenntnisnahme zu schützen.

Es gibt verschiedene Arten von Verschlüsselung. Bei der symmetrischen Verschlüsselung wird der gleiche Schlüssel zum Verschlüsseln und Entschlüsseln der Daten verwendet. Bei der asymmetrischen Verschlüsselung werden zwei unterschiedliche Schlüssel verwendet - einer zum Verschlüsseln der Daten und der andere zum Entschlüsseln der Daten. Dies bietet einen höheren Grad an Sicherheit, da nur derjenige, der im Besitz des Entschlüsselungsschlüssels ist, in der Lage ist, die Daten zu entschlüsseln.

Eine Verschlüsselung richtet sich nach dem Schutzbedarf der zu schützenden personenbezogenen Daten. Berufsgeheimnisträger sollten daher darauf achten, dass alle Mitarbeiter über den sicheren Umgang mit personenbezogenen Daten informiert sind und entsprechende Methoden zur Verschlüsselung nutzen.

12.3.2. Verschlüsselung bei der Datenübermittlung

Grundsätzlich muss zwischen einer Verschlüsselung personenbezogener Daten bei der Datenübermittlung und der verschlüsselten Ablage (Speicherung) von personenbezogenen Daten unterschieden werden. Die Aufgabe einer Transportverschlüsselung ist es zu verhindern, dass personenbezogene Daten bei der Übermittlung „abgehorcht“ werden können.

Beispiel E-Mail (TLS - Transport Layer Security)

Ein Mindeststandard der E-Mail-Verschlüsselung ist die Verwendung des TLS-Protokolls. Der Anwender bemerkt den Einsatz des TLS-Protokolls nicht, da eine etwaige Verschlüsselung zwischen dem sendenden und dem empfangenden E-Mail-Server aufgebaut wird. Die Aufgabe der Kanzlei beim Einsatz des TLS-Protokolls ist es, sicherzustellen, dass die verwendete Version des TLS-Protokolls dem Stand der Technik entspricht und dass das TLS-Protokoll korrekt konfiguriert ist.

Das TLS-Protokoll wird permanent weiterentwickelt. Informationen zu einer Implementierung nach dem Stand der Technik können auf der Seite des BSI abgerufen werden (Technische Richtlinie TR-02102-2, Teil 2 – Verwendung von Transport Layer Security).

Beispiel VPN (Virtual Private Network)

Eine weitere Möglichkeit zur Verschlüsselung bei der Datenübermittlung ist die Nutzung eines VPNs (Virtual Private Network). Beispiel für den Einsatz eines VPNs ist der Zugriff eines Mitarbeiters von einem mobilen Arbeitsplatz auf das Kanzleinetzwerk.

Beispiel Dokumentenaustausch

Auch beim Dokumentenaustausch kann Verschlüsselung zum Einsatz kommen. Beispielsweise können Dateien mit einem Passwort versehen oder mit einer speziellen Software verschlüsselt werden, bevor sie per E-Mail oder Cloud-Dienst versendet werden.

12.3.3. Verschlüsselung bei der Speicherung

Während bei der Transportverschlüsselung personenbezogene Daten nur vor einem Abhorchen geschützt werden sollen, ist ein anderer Anwendungsfall die längerfristige Verschlüsselung von gespeicherten Daten vor unbefugtem Zugriff.

Beispiele für die Verschlüsselung von gespeicherten personenbezogenen Daten

Datenträger wie Festplatten oder USB-Sticks können mit Hilfe einer entsprechenden Software verschlüsselt werden. Hierbei wird das gesamte Laufwerk verschlüsselt und kann erst nach Eingabe eines Passworts oder auch nach dem Einsatz eines anderen Faktors wieder freigeschaltet werden. Durch eine solche Verschlüsselung kann garantiert werden, dass auch bei Verlust des Datenträgers nur autorisierte Personen Zugriff auf den Datenträger haben.

Das Verschlüsseln von **Verzeichnissen oder Dateien** ist eine weitere Option. Hierbei werden nur bestimmte Ordner auf dem Datenträger verschlüsselt. Im Ergebnis sind nicht alle Daten geschützt. Diese Methode wird verwendet, wenn in einem Kanzleinetzwerk nur bestimmte personenbezogene Daten vor unbefugtem Zugriff geschützt werden sollen.

Eine weitere Möglichkeit besteht darin, **Cloudspeicher** mit einer Verschlüsselung zu nutzen. Hierbei werden die Dateien bereits vor dem Hochladen verschlüsselt und somit sind sie sowohl auf dem lokalen Gerät als auch in der Cloud geschützt.

12.4 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.

12.5 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 sowie der für die 2-Faktor-Authentifizierung notwendigen Hardware[43] 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 weiterzugeben bzw. nicht ungeschützt im Computer zu hinterlegen.

12.6 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 (SSL) verfügen.

Auch bei Logins zu geschlossenen Benutzerbereichen oder Filesharing-Plattformen[44] 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

---

[43] Vgl. EU-Zahlungsdiensterichtlinie - PSD2

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

Zunächst ergeben sich Aufbewahrungspflichten aus dem Steuer- und Handelsrecht. Dabei ist zu beachten, dass Aufbewahrungspflichten des Mandanten häufig im Rahmen des Auftrages vom Steuerberater übernommen werden, da eine ordnungsgemäße Buchführung auch die Sicherstellung der gesetzlichen Aufbewahrungsfristen umfasst.[45]

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

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 5 Jahren (vgl. § 169 Abs. 2 AO) vorzunehmen.

Nach diesem Zeitraum von 15 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.
- Gefahr der Notwendigkeit einer strafbefreienden Selbstanzeige des Mandanten

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

[45] Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) vom 28. November 2019, https://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Weitere_Steuerthemen/Abgabenordnung/2019-11-28-GoBD.html

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

Personenbezogene Daten dürfen nur solange in einer Form gespeichert werden, die die Identifizierung ermöglicht, wie es für die Zwecke für die sie verarbeitet werden, erforderlich ist.[46]

Daneben kann auch ein Löschungsanspruch der betroffenen Person gem. Art. 17 DSGVO bestehen, wenn

(a) die betroffene Person die Einwilligung der Verarbeitung widerruft und keine anderweitige Rechtsgrundlage besteht;

(b) die betroffene Person der Verarbeitung widerspricht (gem. Art. 21 Abs. 1 DSGVO) und keine vorrangig berechtigten Gründe für diese Datenverarbeitung bestehen oder bei Widerspruch gegen Direktwerbung (Art. 21 Abs. 2 DSGVO);

(c) personenbezogene Daten zu Unrecht (unrechtmäßig) verarbeitet wurden;

(d) die Löschung gesetzlich für den Verantwortlichen verpflichtend vorgeschrieben ist;

(e) die Daten zur Erbringung eines Dienstes der Informationsgesellschaft verarbeitet werden und es sich um die personenbezogenen Daten eines Kindes handelt (Art. 8 Abs. 1).

Die DSGVO berücksichtigt aber auch, dass eine Löschpflicht nicht besteht, wenn die Verarbeitung (wie „Speicherung“) zur Erfüllung einer rechtlichen Verpflichtung erfolgt[47]. Dies ist beispielsweise durch gesetzliche Aufbewahrungsfristen gegeben. Endet beispielsweise eine Gewährleistungs- oder Garantiefrist, entfällt der eigentliche Zweck der Aufbewahrung aus Nachweispflichten und die entsprechenden Daten mit Personenbezug unterfallen der Löschpflicht, weil der ursprüngliche Zweck einer Nachweisführung entfallen ist. Es greifen dann aber die Aufbewahrungspflichten nach § 257 HGB und § 147 AO, z. B. für Handels- und Geschäftsbriefe bzw. Buchungsbelege oder Jahresabschlüsse. Diese Regelungen stellen dann eine gesetzliche Grundlage für die Verarbeitung („Speichern“) von personenbezogenen Daten im Sinne von Art. 6 Abs. 1 lit. c DSGVO dar.

Die Aufbewahrung selbst hat dann so zu erfolgen, dass dies den rechtlichen Anforderungen in Bezug auf Ordnungsmäßigkeit, Vollständigkeit, Sicherheit, Verfügbarkeit, Nachvollziehbarkeit, Unveränderlichkeit und Zugriffsschutz genügt.

Gesetzliche Aufbewahrungsvorgaben schließen die datenschutzrechtlichen Anforderungen an Datenminimierung (vgl. Art. 5 Abs. 1 lit. c DSGVO) nicht aus. Die Daten und Informationen zu einem Vorgang innerhalb einer Kanzlei oder eines Unternehmens können daher unterschiedlichen

[46] Art. 5 Abs. 1 lit. e, 1. Halbsatz DSGVO.
[47] Art. 17 Abs. 3 DSGVO.

Aufbewahrungszeiträumen und damit unterschiedlichen Löschzeitpunkten unterliegen. Um dies zu berücksichtigen, sollten diese Daten entsprechend klassifiziert werden.

Dies schließt zudem nicht per se aus, dass einzelne Datensätze oder Dokumente nicht zwischenzeitlich auf Initiative der betroffenen Person berichtigt (vgl. Art. 16 DSGVO) oder gelöscht werden können bzw. müssen. Diese Vorgänge müssen jeweils nur nachvollziehbar dokumentiert werden.

Unterlagen und Dateien, die nicht der Aufbewahrungspflicht spezieller rechtlicher Vorgaben unterliegen, sind daher grundsätzlich zu löschen, wenn der Zweck der Verarbeitung entfallen ist. Archivierungssysteme müssen dies umsetzen können, um die Anforderungen aus Art. 25 DSGVO (Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen) zu erfüllen.

Es empfiehlt sich daher, die Daten und Dokumente so zu kennzeichnen, dass eine anforderungskonforme, datenschutzrechtliche Behandlung möglich ist und unterschiedliche Löschzeitpunkte berücksichtigt werden können.

So könnten beispielsweise Anlagen zu Bewerbungsunterlagen eher gelöscht werden, als ein Kostenerstattungsbeleg für Bewerbungsgespräche oder der Arbeitsvertrag selbst.

Auch Anforderungen an die Revisionssicherheit widersprechen dem nicht, da diese nur im Rahmen der gesetzlichen Aufbewahrungsfristen zu erfüllen sind.

Zu den Aufbewahrungsfristen, die einer Löschpflicht entgegenstehen können, können noch „Karenzzeiten“, die organisatorisch oder technisch bedingt sind, hinzugerechnet werden. Diese jeweiligen Zeiträume sind jedoch auch zu dokumentieren und ihre Erforderlichkeit ist regelmäßig zu prüfen und zu dokumentieren.

Sofern technisch umsetzbar sollte bei Applikationen eine automatisierte Löschfrist hinterlegt werden, die einem die zur Löschung vorgesehenen Daten ermittelt.

Es empfiehlt sich, für Löschung aufgrund Wegfalls des Zwecks ein Löschkonzept zu erstellen, in dem beispielhaft folgende Punkte dokumentiert werden:

a) Verantwortlichkeiten festlegen

b) Datenarten clustern

c) Löschfristen bestimmen

d) Löschregeln erstellen

e) Löschregeln technisch umsetzen

f) Nachweisfähigkeit gewährleisten

g) regelmäßige Überprüfungen

h) Dienstleister nicht vergessen!

Ein Beispiel findet sich in der Anlage zu diesen Hinweisen.

Für die Umsetzung eines Betroffenenrechts nach Art. 17 DSGVO sind folgende Punkte durchzuführen und zu dokumentieren:

- Prüfung der Identität der betroffenen Person
- Dokumentation der Antragstellung
- ggf. Verweigerung der Löschung
- ggf. Einschränkung der Verarbeitung
- Prozess, aus dem heraus Daten gelöscht werden
- Herkunft der Daten (zentrale Ablage, individuelle Ablage, Archiv usw.)
- Betroffenengruppen
- Datenart
- einzelne Daten
- Zeitpunkt der Löschung
- Löschung bei Dienstleistern (Auftragsverarbeitung)

14. Beendigung des Mandats

Es empfiehlt sich, bereits im Steuerberatungsvertrag Regelungen zur Kündigung des Mandatsverhältnisses und dem Umgang mit vorhandenen Daten nach der Beendigung 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 Gebrauch gemacht. Der EuGH hat die Vorgaben hinsichtlich der Ausgestaltung der Regelungsbefugnis zu

Beschäftigtendatenschutz konkretisiert.[48] Eine bloße Wiederholung gesetzlicher Vorgaben entspräche nicht der Regelungsbefugnis aus Art. 88 DSGVO. Sofern dadurch beispielsweise § 26 Abs. 1 Satz 1 BDSG betroffen wäre, treten an seine Stelle die Rechtsgrundlagen aus Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung) und Art. 6 Abs.1 lit. f DSGVO (Wahrung berechtigter Interessen).

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[49] 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.[50] Zusätzlich kann eine Verarbeitung zur Wahrung berechtigter Interessen erfolgen.[51] Hier ist zu beachten, dass die betroffene Person ein Widerspruchsrecht hat.[52]

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[53] aufzuklären. Aus Nachweisgründen sollte zumindest die Textform gewählt werden.

Freiwilligkeit im Beschäftigungsverhältnis kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte

---

48 EuGH C-34/21 https://curia.europa.eu/juris/document/document.jsf?text=&docid=272066&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1

49 Grundsätze für die Verarbeitung personenbezogener Daten.

50 § 26 Abs.1 Satz 1 BDSG bzw Art. 6 Abs. 1 lit. b DSGVO.

51 Art. 6 Abs. 1 lit. f) DSGVO.

52 Art. 21 Abs. 1 DSGVO.

53 Art. 7 Abs. 3 DSGVO.

Person gleichgelagerte Interessen verfolgen. Dies ist z. B. denkbar bei der Einwilligung zur notwendigen Protokollierung der privaten Internetnutzung.

Eine Auswertung personenbezogener Daten von Beschäftigten zur Aufdeckung von Straftaten und schwerwiegenden vertraglichen Pflichtverletzungen darf nur erfolgen, wenn[54]

- 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 sind 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) nach Treu und Glauben und auf rechtmäßige, sowie 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. der 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 zu Stalking gegenüber Beschäftigten oder die Veröffentlichung von E-Mail-Adressen zu einer rapiden Zunahme von Spam-Mails führen.

[54] § 26 Abs. 1 Satz 2 BDSG.

16. Kanzleiübertragung

Bezüglich der Kanzleiübertragung decken sich die datenschutzrechtlichen Regelungen mit den berufsrechtlichen Grundsätzen.[55] Es ist zu beachten, dass sich durch eine Kanzleiübertragung die Aufbewahrungs- und Löschfristen nicht automatisch verlängern.

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

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

Syndikusrechtsanwalt Rudi Kramer
Dipl.-Staatswissenschaftler Dirk Munker
StB Dipl.-Volksw. Wolf Dieter Oberhauser
Dipl.-Ök. Stephan Rehfeld
RAin Nicole Schmidt, LL.M.
RA/StB Oliver Klose

Ansprechpartner in der BStBK:
RAin Claudia Kalina-Kerschbaum, LL.M.
RA Kay Fietkau

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