www.nwb.de

Christian Solmecke

DSGVO: Die zehn wichtigsten To-dos für Steuerkanzleien

Pflichten, die jeder Steuerberater kennen muss

nwb

DSGVO: Die zehn wichtigsten To-dos für Steuerkanzleien

Pflichten, die jeder Steuerberater kennen muss

Von
Christian Solmecke

Christian Solmecke hat sich als Rechtsanwalt und Partner der Kölner Medienrechtskanzlei WILDE BEUGER SOLMECKE auf die Beratung der Internet und IT-Branche spezialisiert. So hat er in den vergangenen Jahren den Bereich Internetrecht/E-Commerce der Kanzlei stetig ausgebaut und betreut zahlreiche Medienschaffende, Web 2.0-Plattformen und App-Entwickler.

Anregungen und Kritik zu diesem Werk senden Sie bitte an:
service@nwb.de
Autoren und Verlag freuen sich auf Ihre Rückmeldung.

Sonderausgabe für NWB Verlag GmbH & Co. KG, Herne 2018
mit freundlicher Genehmigung

Satz: Helmut Rohde, Euskirchen

Inhalt

Alles aus einer Hand!

Die Software-Lösung für Steuerberater.

Stotax Kanzlei

Ihr Startpaket
ab € 39,00 monatlich zzgl. USt
GoBD- und GKV-zertifiziert

Computer Bild
TRUSTED SOLUTIONS
★★★★★ 2018
ANWENDER- UND EXPERTENBEFRAGUNG
Ausgabe 4/2018
STOLLFUß MEDIEN
IN DER KATEGORIE STEUERSOFTWARE

Für alle wesentlichen Aufgaben der Steuerberatung.

Intuitive Benutzerführung und ein optimal aufeinander abgestimmtes Zusammenspiel aller Module:

- Finanzbuchhaltung
- Anlagenverwaltung
- Jahresabschluss
- Lohnabrechnung mit kostenfreiem DEÜV-Modul
- Steuern
- DMS-System

Cloud-Software für Ihre Mandanten

Stotax Select

Gratistest und mehr Informationen unter:
Telefon: 0800 5225575 (gebührenfrei)
www.stotax-kanzlei-software.de

stotax
Stollfuß Medien

1. Die wichtigsten Grundlagen

Der Datenschutz sichert das Grundrecht auf „informationelle Selbstbestimmung“ (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 Grundgesetz, BVerfGE 65, 1 – Volkszählung). Geschützt sind danach sog. „personenbezogene Daten“. Das sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (Betroffene) beziehen. Beispiele sind: Name, Telefonnummer, E-Mail-Adresse, IP-Adresse, IBAN. In allen Steuerberaterkanzleien werden ständig eine Vielzahl von personenbezogenen – teils besonders sensiblen – Daten verarbeitet. Neben der Verschwiegenheitspflicht aus § 203 StGB sowie den §§ 57, 62 StBerG müssen Sie als Steuerberater daher auch geltendes Datenschutzrecht beachten, um die Daten Ihrer Mandanten, Dienstleister, Partner und Mitarbeiter zu schützen.

Ab dem 25. Mai 2018 gilt auch in Deutschland die Datenschutzgrundverordnung (DSGVO) der Europäischen Union. Durch das neue EU-Recht werden unmittelbar das bisherige Bundesdatenschutzgesetz (BDSG a. F.) und die EU-Datenschutzrichtlinie (Richtlinie 95/46/EG), auf der das BDSG basiert, abgelöst. Zeitgleich tritt ein dazu gehöriges neues Bundesdatenschutzgesetz (BDSG n. F.) in Kraft, das die DSGVO zum Teil modifiziert und konkretisiert. Die DSGVO soll außerdem wohl 2019 ergänzt werden durch die noch in Abstimmung befindliche EU-e-Privacy-Verordnung, die Internet- und Telemediendienste betreffen wird.

Ziel der DSGVO ist zunächst ein weitestgehend einheitliches Datenschutzrecht innerhalb der EU. Darin sollen vor allem die Rechte und Kontrollmöglichkeiten derjenigen gestärkt werden, deren personenbezogene Daten verarbeitet werden (Betroffene). Die DSGVO schafft neue Rechtsgrundlagen für die Datenverarbeitung und intensiviert die Pflichten der betroffenen Unternehmen (Verantwortliche). Sie müssen als Steuerberater im Hinblick auf ihre eigene rechtliche, betriebliche und technisch-organisatorische Struktur eine Vielzahl von Vorgaben beachten, um etwa Transparenz, Kontrolle und Sicherheit der gesammelten Nutzerdaten vor unbefugten Zugriffen Dritter zu gewährleisten.

Anders als noch das BDSG a. F. wird die DSGVO mehr Einfluss auf den Alltag in der Steuerberatungskanzlei haben. Daher ist es für Sie sehr wichtig, sich jetzt (wenn nicht schon geschehen) um die Umsetzung der neuen Regelungen zu kümmern und neue datenschutzrechtliche Prozesse zu etablieren. Gerade, wenn Sie noch nicht gehandelt haben, sollten Sie **dringend die Maßnahmen in Ihrer Kanzlei umsetzen**, die wir Ihnen in dieser eBroschüre vorstellen. Zusätzlich sollten Sie auf Ihren Berufszweig zugeschnittene, praxistaugliche Literatur hinzuziehen, um die zentralen Fragen des neuen Datenschutzrechts für Ihre Kanzleiorganisation beantworten zu können.

2. Kosten der Umstellung vs. Risiken

Kommt auf Ihre Kanzlei ein „Mehr“ an Aufwand und Kosten zu?

Ja. Steuerkanzleien müssen einige ihrer Prozesse anpassen – und dadurch werden ihnen auch Mehrkosten entstehen, nicht nur am Anfang der Umstellung, sondern auch im laufenden Kanzleialltag. Denn Steuerberaterkanzleien verarbeiten systematisch auch sensible personenbezogene Daten (Art. 9 DSGVO), für welche die DSGVO ein hohes Schutzniveau vorschreibt.

Mehraufwendungen am Anfang fallen zunächst an für die Erstellung eines DSGVO-konformen Verzeichnisses der Verarbeitungstätigkeiten, das kleinteilig all Ihre Prozesse, in denen Daten verarbeitet werden, auflistet. Allein der Überblick über die eigenen Prozesse, bei denen personenbezogene Daten verarbeitet werden, nimmt sicherlich einige Zeit in Anspruch. Kanzleileitungen sind darüber hinaus dafür verantwortlich, die Einhaltung der Datenschutzgrundsätze gegenüber der Aufsichtsbehörde nachzuweisen (**Rechenschaftspflicht**, Art. 5 Abs. 2 DSGVO). Das führt dazu, dass Kanzleien nun all ihre Datenverarbeitungstätigkeiten sowie die Maßnahmen dokumentieren müssen, die sie sonst zur Einhaltung der Anforderungen der DSGVO getroffen haben. Zudem müssen Ihre Verträge mit all Ihren externen Dienstleistern überprüft werden. Darunter fallen z. B. Cloud-Anbieter, externe Rechenzentren oder sonstige Dienstleister außerhalb Ihrer Kanzlei, die für Sie personenbezogene Daten Dritter verarbeiten (Auftragsverarbeiter, Art. 28 DSGVO). Auch müssen Sie ein speziell auf Ihre Kanzlei abgestimmtes Datenschutzkonzept erstellen, z. B. im Hinblick auf Ihre Informationspflichten, Betroffenenrechte und die Sicherheit Ihrer IT-Systeme. Des Weiteren werden Sie

Ihre Mitarbeiter im Umgang mit der DSGVO schulen müssen. Sollten Sie einen Datenschutzbeauftragten benötigen, müssen Sie entweder die Ausbildung eines kanzleiinternen Mitarbeiters oder einen externen Beauftragten bezahlen. Auch in Ihren laufenden Prozessen werden die Kosten für den Datenschutz in Ihrer Steuerkanzlei sicherlich steigen. Denn die Anforderungen an Datensicherheit, Dokumentation und Transparenz werden durch die DSGVO angehoben, teilweise werden auch gänzlich neue Pflichten etabliert.

Ist es überhaupt noch möglich, die Anpassungen rechtzeitig vorzunehmen?

Haben Sie noch nicht mit der Umstellung begonnen, kann die rechtzeitige Umsetzung zumindest der wichtigsten Grundlagen noch möglich sein. Sie müssen dann aber ab sofort alle verfügbaren Kapazitäten bündeln, externes Know-how und bestenfalls Beratung in Anspruch nehmen. Sollten Sie es nicht mehr schaffen, alle Anforderungen vollständig vor dem 25. Mai zu erfüllen, müssen Sie individuell abschätzen, welche Datenverarbeitungen bei Ihnen die größten Risiken für die Daten etwa Ihrer Mandanten bergen. Es kommt also auf die richtige Schwerpunktsetzung an. Mit diesen Prozessen sollten Sie beginnen, denn sie beeinflussen die Höhe der möglichen Geldbußen.

Welche Risiken drohen bei einer verspäteten Umsetzung der neuen Vorgaben?

Die zuständigen Aufsichtsbehörden können zunächst nach Art. 83 DSGVO **Bußgelder** verhängen. Diese können – je nach Verstoß und dessen Schwere – bis zu 20 Millionen Euro oder bis zu 4 Prozent des weltweiten Jahresumsatzes eines Unternehmens betragen. Es gilt immer der jeweils höhere Betrag. Daneben besteht auch weiterhin die Möglichkeit, wegen bestimmten Datenschutzrechtsverstößen **wettbewerbsrechtlich abgemahnt** zu werden, was – je nach Ausmaß und Zahl der Verstöße – hohe Abmahnkosten verursachen kann. Neu ist auch, dass Betroffene wegen der Verletzung des Datenschutzrechts im Rahmen ihrer **Schadensersatzansprüche** nun auch ihren immateriellen Schaden geltend machen können. Nach außen **haftet immer die Kanzleileitung**, auch für Fehlverhalten von Mitarbeitern.

Lohnt sich Hilfe von außen?

Ja, gerade im Hinblick auf das hohe Risiko sollte entsprechendes Know-how durch berufszweigsbezogene datenschutzrechtliche Literatur oder Seminare erworben werden. Im Einzelfall kann auch eine Beratung sowie Konzepterstellung durch einen auf das Datenschutzrecht spezialisierten Rechtsanwalt oder einen Datenschutzbeauftragten empfehlenswert sein. Insgesamt können sich die Investitionen in Datensicherheit und Compliance lohnen und Ihnen später weitere Kosten ersparen. Ziehen Sie solche Literatur heran, welche die datenschutzrechtlichen Themen auf Ihren Berufsalltag als Steuerberater begrenzt und gleichzeitig Praxistipps und Umsetzungsmuster an die Hand gibt. Zu umfassendes Know-how mit der falschen Schwerpunktsetzung kann mehr verwirren, als dass es hilft.

3. Verzeichnis der Verarbeitungstätigkeiten erstellen

Art. 30 DSGVO schreibt vor, dass Unternehmen ein „Verzeichnis der Verarbeitungstätigkeiten“ führen sowie dieses auf Anfrage der Aufsichtsbehörde zur Verfügung stellen müssen. Dabei handelt es sich um eine Dokumentation und Übersicht aller Verfahren, bei denen personenbezogene Daten verarbeitet werden. Zwar können Unternehmen mit weniger als 250 Beschäftigten von dieser Pflicht ausgenommen sein (Art. 30 Abs. 5 DSGVO). Diese Ausnahme wird jedoch aufgrund der intensiven Verarbeitung besonders sensibler Daten nicht für Steuerkanzleien anwendbar sein. Schließlich verarbeiten Steuerberater Informationen über die Gesundheitsaufwendungen oder Religionszugehörigkeit Ihrer Mandanten. Ein solches Verzeichnis ist auch im Hinblick auf die gesamte Umstellung sehr sinnvoll. Denn so können Sie sich einen Überblick über alle Prozesse in Ihrer Kanzlei verschaffen und besser planen, was noch zu tun ist.

Beginnen sollten Sie, indem Sie alle Geschäftsprozesse z. B. in einer Excel-Tabelle oder in einem anderen, speziell geeigneten Software-Tool auflisten, in denen personenbezogene Daten verarbeitet werden. „Verarbeitung“ bezeichnet kurzgefasst jeden Vorgang im Zusammenhang mit personenbezogenen Daten wie *das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung,*

das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung, Art. 4 Nr. 2 DSGVO. Dabei ist nicht von Bedeutung, ob die Daten auf Papier oder elektronisch gespeichert werden. Soweit Ihnen eine feingliedrige Darstellung Ihrer Geschäftsprozesse möglich ist, empfehlen wir diese. Bei einem zu großzügigen Clustern der Geschäftsprozesse ist zu erwarten, dass dies nicht den Anforderungen der Datenschutzbehörden genügt. Bei der Auswahl dieser Prozesse sollten Sie sich immer in die Lage eines Kontrolleurs der Datenschutzbehörde versetzen. Diesem muss es möglich sein, anhand des Verarbeitungsverzeichnisses einen vollständigen Einblick in die Prozesse Ihres Unternehmens zu erhalten. Neben offensichtlichen Prozessen wie etwa „Neue Mandanten elektronisch erfassen" und „Steuererklärung übermitteln" können dies etwa sein: Daten der Mitarbeiter und Bewerber speichern, Jahresgespräche, Reisekostenabrechnung, Besucherverwaltung, E-Mail-Marketing, Papier- und Aktenvernichtung, Telefonsupport, Videoüberwachung etc. Letztlich werden in fast allen internen wie externen Prozessen Daten verarbeitet. Daher empfehlen wir, Ihr Geschäft möglichst umfangreich abzubilden.

Anschließend müssen die in Art. 30 DSGVO genannten Angaben in das Verzeichnis aufgenommen werden. Sollten Sie bereits über eine nach dem BDSG a. F. erforderliche Verfahrensübersicht verfügen, können Sie diese als Grundlage heranziehen und aktualisieren. So müssen Sie etwa identifizieren, woher die Daten in den jeweiligen Prozessen stammen, zu welchem Zweck sie verarbeitet werden, wer Zugriff hat und an wen sie weitergegeben werden. Zudem müssen Sie hier auch Name und Kontaktdaten des Verantwortlichen sowie eines ggf. bestellten Datenschutzbeauftragten, Löschfristen der gespeicherten Daten, die technisch-organisatorischen Maßnahmen, die Sie ergreifen, sowie eine etwaige Risikobewertung eintragen. Außerdem sollten Sie hier für alle Verarbeitungen der Daten Ihrer Mandanten, Mitarbeiter, Lieferanten etc. die rechtlichen Erlaubnisnormen dokumentieren.

Hierbei bietet es sich an, Literatur heranzuziehen, die praxistaugliche Darstellungen und Muster speziell für Steuerberater enthält. Bei allen anderen Aspekten, die in diesem Verzeichnis aufgelistet sind, können Sie sich auch Unterstützung durch einen Datenschutzbeauftragten oder eine Datenschutzkanzlei einholen. Eine Beratung ist in diesem Fall insbesondere sinnvoll, um die korrekten Rechtsgrundlagen einzutragen – und, um die weiteren, darauf aufbauenden Schritte bei der Umstellung zu begleiten.

4. Auftragsverarbeiter überprüfen und Verträge anpassen

Die DSGVO schreibt in Art. 28 weitere Pflichten für beide Seiten der sog. „Auftragsverarbeitung" vor. Unter Auftragsverarbeitung versteht man die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten durch einen **Auftragsverarbeiter (externer Dienstleister)** gemäß den Weisungen des **für die Verarbeitung Verantwortlichen (Ihre Kanzlei)** auf Grundlage eines schriftlichen Vertrags. Wichtiges Kriterium ist also die Weisungsabhängigkeit, Art. 29 DSGVO. So sind Sie als Steuerberater nicht etwa Auftragsverarbeiter Ihrer Mandanten, weil Sie in eigener Verantwortung arbeiten. Gleiches gilt für die Lohn- und Gehaltsabrechnung des Steuerberaters. Unter Auftragsverarbeitung fallen aber z. B. Ihre Kanzleisoftware, externe Rechenzentren, Cloud-Anbieter wie Google Drive oder die Dropbox, ein externes Lohnbuchhaltungsbüro, sonstige EDV-, Telekommunikations- oder IT-Dienstleister mit Fernzugriff auf Ihre Daten, E-Mail-Provider und gewisse Apps. Schließlich ist sogar Ihr Abfallentsorger als Auftragsverarbeiter anzusehen, wenn das Unternehmen Zugriff auf entsorgte Papiere hat, die personenbezogene Daten enthalten.

Im nächsten Schritt prüfen Sie daher, wer für Sie personenbezogene Daten Dritter verarbeitet und erstellen hierzu eine weitere Liste. Zudem ist es sinnvoll, hier zu vermerken, welche Daten jeweils verarbeitet werden – dazu können Sie einen Auszug aus dem Verarbeitungsverzeichnis verwenden. Da mit der neuen Rechtslage auch der Auftragsverarbeiter ein Verzeichnis der Verarbeitungstätigkeiten führen muss, sollten Sie Ihr Verzeichnis mit dem Ihres Dienstleisters abstimmen. Anschließend müssen Sie prüfen, ob die Rahmenbedingungen für die Auftragsverarbeitung schon auf dem Stand der DSGVO sind oder ob Sie Anpassungen vornehmen müssen. Hierbei müssen Sie gemäß Art. 28 DSGVO vor allem auf drei Dinge achten: die Auswahl, die vertragliche Ausgestaltung und die anschließende Kontrolle Ihrer externen Dienstleister.

Im Hinblick auf die Auswahl eines externen Dienstleisters muss dieser *„hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet,“* Art. 28 Abs. 1 DSGVO. Hier sollten Sie als Kanzlei zunächst prüfen, ob ausreichender Datenschutz gewährleistet ist. Wenn Sie hier Fehler machen, haften Sie etwa bei Datenpannen neben dem Auftragsverarbeiter als Gesamtschuldner auf Schadensersatz (Art. 82 Abs. 1 DSGVO).

Haben Sie als Kanzlei noch keine Verträge mit externen Dienstleistern geschlossen, so sollten Sie dies nun dringend nachholen. Ansonsten sollten Sie Ihre bestehenden **Verträge überprüfen**, um Ihr Haftungsrisiko zu reduzieren. Darin sollte nach Art. 28 Abs. 3 DSGVO insbes. Folgendes geregelt sein:

- Weisungsabhängigkeit
- Vertraulichkeitsvereinbarung sowie Verpflichtung auf die Verschwiegenheit nach § 203 StGB und § 62a StBerG (vgl. zu einer Musterformulierung Wickert/Potthoff, Das neue Datenschutzrecht in der Steuerberaterkanzlei: Praxisleitfaden zur Umsetzung der DS-GVO, S. 39)
- Zusicherung eines dauerhaften hinreichenden Datenschutzes i. S. d. Art. 32 DSGVO
- Offenlegung der Subunternehmer, Zusicherung, dass keine Subunternehmer ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung eingesetzt werden; im Fall einer allgemeinen Genehmigung Informationspflicht bei Wechsel
- Unterstützung bei der Erfüllung der Rechte, Information und Benachrichtigung Betroffener bei einer etwaigen Datenschutzfolgenabschätzung sowie bei Überprüfungen und Datenschutzpannen
- Umschreibung von Inhalt, Beginn und Ende eines Auftrags inkl. Zusicherung der Datenlöschung

Im weiteren Verlauf müssen Sie die datenrelevanten Tätigkeiten Ihres Auftragsverarbeiters **regelmäßig überwachen**. Gerade bei Berufsgeheimnisträgern wird eine jährliche Kontrolle empfohlen. Hier helfen zunächst die Informationen, die Ihr Auftragsverarbeiter Ihnen als Selbstauskunft nachweisen muss. Eine weitere Grundlage für die Kontrolle kann z. B. eine Zertifizierung (Art. 42 DSGVO) bzw. die Einhaltung einer genehmigten Verhaltensregel (Art. 40 DSGVO) sein. Auch ein Datenschutzaudit vor Ort ist möglich.

5. Datenschutzbeauftragten benennen?

Als nächstes müssen Sie prüfen, ob Sie verpflichtet sind, einen Datenschutzbeauftragten zu benennen. Hauptaufgaben des Datenschutzbeauftragten sind es, sowohl die Kanzleileitung (Verantwortliche) als auch die Mitarbeiter zu unterrichten und zu beraten, die Einhaltung der rechtlichen Regelungen sowie der Strategien des Verantwortlichen zu überwachen und Schulungen durchzuführen. Ggf. arbeitet er auch mit der Aufsichtsbehörde zusammen.

Art. 37 DSGVO nennt hier als möglicherweise einschlägigen Grund für die Benennung, dass *„(...) die Kerntätigkeit des Verantwortlichen (...) in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 (...) besteht.“* Zwar haben Steuerkanzleien regelmäßig etwa mit sensiblen Daten zu Krankheiten oder Informationen über die Religionszugehörigkeit (Daten i. S. d. Art. 9 DSGVO) zu tun – doch ist dies auch die Kerntätigkeit einer Kanzlei? Leider können wir Ihnen diese Frage nicht abschließend beantworten, weil diese Auslegungsfrage zum jetzigen Zeitpunkt noch nicht gerichtlich geklärt ist. Allerdings könnte auch bei kleineren Kanzleien eine Verpflichtung zur Datenschutz-Folgeabschätzung vorliegen, was nach dem BDSG n. F. ebenfalls zur Pflichtbenennung eines Datenschutzbeauftragten führt (s. u.). Allerdings macht das BDSG n. F. den Datenschutzbeauftragten dann zur Pflicht, wenn in Ihrer Kanzlei in der Regel **mindestens zehn Personen ständig mit der automatisierten Datenverarbeitung beschäftigt** sind (§ 38 Abs. 1 BDSG n. F.). Da in einer modernen Steuerkanzlei jeder Mitarbeiter (z. B. Kanzleileitung, Steuerberatern, Sekretariat, Buchhaltung) ständig mithilfe von PCs Daten verarbeitet, ist ein Datenschutzbeauftragter für Sie ab dieser Größe Pflicht.

Im Hinblick auf die Personalie steht es Ihnen frei, einen innerbetrieblichen Datenschutzbeauftragten zu installieren oder einen externen einzusetzen. Wenn Sie sich für einen externen Datenschutzbeauftragten entscheiden, können Sie neben den Landessteuerberaterverbänden auch bei Ihrer Kammer nachfragen, ob diese Ihnen einen speziellen Datenschutzbeauftragten vermitteln können. Übrigens: Auch wenn Sie nicht zur Benennung verpflichtet sind, können Sie sich hier externe Hilfe holen. In jedem Fall muss ein Datenschutzbeauftragter entsprechend beruflich und fachlich qualifiziert sein und sich regelmäßig fortbilden (Art. 37 Abs. 5 DSGVO). Die Benennung müssen Sie veröffentlichen und Ihrer Datenschutz-Aufsichtsbehörde melden (Art. 37 Abs. 7 DSGVO). Sollten Sie sich für eine **interne** Person entscheiden, so müssen Sie Folgendes beachten:

Nach Art. 38 DSGVO ist der Datenschutzbeauftragte frühzeitig einzubinden, fachlich weisungsfrei und berichtet unmittelbar der höchsten Managementebene. Damit keine Interessenkonflikte entstehen, darf es sich nicht um ein Mitglied der Kanzleileitung, einen IT- oder Personalverantwortlichen handeln. Ansonsten darf der Datenschutzbeauftragte aber durchaus auch andere Aufgaben im Unternehmen wahrnehmen, sofern sichergestellt ist, dass daraus keine Interessenkollisionen erwachsen (Art. 38 Abs. 6 S. 2 DSGVO).

Beachten Sie, dass die Kosten für die Aus- und Fortbildung eines internen Datenschutzbeauftragten sowie der zeitliche Aufwand mit einkalkuliert werden müssen (Art. 38 Abs. 2 DSGVO). Entsprechende Ausbildungen bieten etwa Landessteuerberaterverbände oder die DATEV an. Auch wenn Sie nicht zur Benennung verpflichtet sind, sollten Sie dennoch in die Ausbildung der intern mit dem Thema Datenschutz betrauten Person (dies kann auch die Kanzleileitung sein) investieren.

Ein interner Datenschutzbeauftragter darf nicht ohne wichtigen Grund gem. § 626 BGB abberufen oder gekündigt werden (vgl. Wickert/Potthoff, Das neue Datenschutzrecht in der Steuerberaterkanzlei: Praxisleitfaden zur Umsetzung der DS-GVO, S. 19).

6. Rechte der Betroffenen und Informationspflichten beachten

Die Rechte aller Personen (Art. 12 – 23 DSGVO), deren Daten Sie verarbeiten, bringen für Sie neue Pflichten mit sich. Für Steuerkanzleien bedeutet das: Sie müssen bereits jetzt ein **praktikables Verfahren etablieren**, um in Zukunft zeitnah und DSGVO-konform insbesondere auf folgende wichtige Ansprüche der Betroffenen reagieren zu können:

Die Betroffenen einer Datenverarbeitung haben gem. Art. 15 DSGVO ein **umfassendes Auskunftsrecht**, welches die Übermittlung der von ihnen gespeicherten Daten umfasst. Sie müssen eine Bestätigung darüber erteilen, ob Sie personenbezogene Daten verarbeiten. Wenn ja, müssen Sie dem Betroffenen weitergehend Auskunft im Hinblick auf die in Art. 15 Abs. 1 lit. a) – h) DSGVO genannten Informationen erteilen, z. B. über die Verarbeitungszwecke, die Kategorien personenbezogener Daten, die verarbeitet werden und über die Herkunft der Daten. Die Kanzlei muss die in Art. 15 DSGVO genannten Informationen „unverzüglich" zur Verfügung stellen – dies ist i. d. R. spätestens einen Monat nach der Anfrage. Je nach Art und Weise der gespeicherten Daten kann die Übermittlung in elektronischer Form oder etwa als (Akten)Kopie geschehen (Art. 15 Abs. 3 DSGVO). Gerade im Hinblick auf Ihre Verschwiegenheitspflicht als Steuerberater müssen Sie aber darauf achten, keine Daten Dritter weiterzugeben und entsprechende Stellen, wenn möglich, schwärzen.

Art. 17 DSGVO gibt Betroffenen erstmals qua Gesetz ein „Recht auf Vergessenwerden", also ein **Recht auf Löschung der eigenen Daten**, wenn die Speicherung der Daten nicht mehr notwendig ist, der Betroffene seine Einwilligung zur Datenverarbeitung widerrufen hat, die Daten unrechtmäßig verarbeitet wurden oder eine Rechtspflicht zum Löschen nach EU- oder nationalem Recht besteht. Nach Art. 17 Abs. 3 DSGVO gilt dies aber nicht in den genannten Ausnahmefällen. Darunter fällt etwa eine Speicherung zur Erfüllung einer rechtlichen Verpflichtung, wie etwa Archivierungspflichten, die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt, oder die Notwendigkeit zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Art. 13 und Art. 14 DSGVO sehen auch für Steuerberaterkanzleien im Regelfall eine Vielzahl an Informationen vor, die Sie Betroffenen zum Zeitpunkt der Erhebung von personenbezogenen Daten, aber auch bei jeder Berichtigung, Löschung oder Einschränkung der Datenverarbeitung am besten schriftlich mitteilen müssen. Dabei ist auf eine präzise, transparente, verständliche und leicht zugängliche Form sowie eine klare und einfache Sprache zu achten (Art. 12 Abs. 1 DSGVO). Die **Informationspflichten** bestehen sowohl online (z. B. in der Datenschutzerklärung, dazu später mehr) als auch offline, etwa für Besucher vor Ort. Für den letzteren Fall müssen Sie entsprechende Informationsblätter vorbereiten. Art. 13 DSGVO sieht für die Erhebung beim Betroffenen zum Bespiel folgende Informationen zwingend vor:

- Name und Kontaktdaten des Verantwortlichen (ggf. auch Vertreter)
- Zweck und Rechtsgrundlage der Verarbeitung
- Falls Rechtsgrundlage der Art. 6 Abs. 1 f.) DSGVO ist: Angabe der berechtigten Interessen des Verantwortlichen oder Dritten
- Aufklärung über Rechte des Betroffenen (neben Auskunft und Löschung auch **die weiteren: Berichtigung, Einschränkung, Widerspruch, Datenübertragung**)
- Hinweis auf Beschwerderecht bei einer Aufsichtsbehörde
- Speicherdauer der Daten (jedenfalls die Kriterien für die Festlegung dieser Dauer)

Die Informationspflichten sind auf den jeweiligen Einzelfall und die jeweilige Verarbeitung gesondert anzupassen (vgl. zu den Informationspflichten und der Datenschutzerklärung einer Steuerberaterkanzlei Wickert/Potthoff, Das neue Datenschutzrecht in der Steuerberaterkanzlei: Praxisleitfaden zur Umsetzung der DS-GVO, S. 29 f.).

7. Datenschutzerklärung Ihrer Webseite muss geändert werden

Die Datenschutzerklärung Ihrer Webseite muss Antworten auf folgende Fragen geben:

- Welche personenbezogenen Daten werden erhoben? (z. B. die IP-Adresse eines Besuchers)
- Was passiert mit den erhobenen Daten?
- Warum werden überhaupt Daten erhoben?
- Werden die erhobenen Daten an Dritte weitergegeben?
- Findet ein grenzüberschreitender Datenverkehr statt?
- Welche Maßnahmen werden zur Gewährleistung der Sicherheit der Daten ergriffen?

Haben Sie bereits eine **Erklärung**, müssen Sie diese **dringend an die DSGVO anpassen**, die insbesondere folgende Neuerungen mit sich bringt:

- Alle in Art. 13 und 14 DSGVO genannten Pflichtinformationen müssen enthalten sein (siehe Punkt 6)
- Erläuterung des Datenerhebungs- bzw. -verarbeitungsvorgangs und des dahinterstehenden Zwecks
- Angabe der konkret anwendbaren Rechtsgrundlage
- Nicht mehr zwingend notwendig, aber empfehlenswert: Information über Art und Umfang der Verarbeitung in der Datenschutzerklärung belassen
- Hinweis auf ein (eingeschränktes) Widerspruchsrecht, wenn die Verarbeitung personenbezogener Daten auf Art. 6 Abs. 1 e) oder f.) DSGVO beruht
- Hinweis auf ein Widerspruchsrecht gegen zulässige Direktwerbung und – in besonders schutzwürdigen Fällen – auch gegen sonstige zulässige Datenverarbeitungen. Da die Information hierüber laut Gesetz separat zu erfolgen hat, ist noch unklar, ob dies überhaupt Teil der Datenschutzerklärung sein soll

Neben den bereits unter Punkt 6 (Informationspflichten) genannten, zwingend erforderlichen Informationen müssen Sie im Einzelfall weitere Informationen vorhalten:

- Hinweis auf Widerrufsrecht, wenn die Verarbeitung personenbezogener Daten auf einer Einwilligung der betroffenen Person beruht (Art. 7 DSGVO)
- Sofern vorhanden: Kontaktdaten des Datenschutzbeauftragten
- Bei gesetzlicher oder vertraglicher Pflicht zur Datenerhebung: Aufklärung des Betroffenen über diese Pflicht und die möglichen Folgen einer Nichtbereitstellung
- Beim Einsatz automatisierter Entscheidungsfindungen (einschl. Profiling): Aufklärung hierüber, insbesondere die zugrundeliegende Logik, die Tragweite und die angestrebten Auswirkungen für den Betroffenen
- Bei einer Weitergabe an Dritte: Angabe der Empfänger/Kategorie von Empfängern
- Angabe der Absicht zur Datenübermittlung ins Ausland (dann auch Angabe des von der Kommission festgelegten Datenschutzniveaus des jeweiligen Drittlandes)
- Im Falle von Übermittlungen nach Art. 46, 47 oder 49 DSGVO: Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind

Hierzu können Sie in einem ersten Schritt auch unseren individualisierbaren Online-Datenschutzerklärungs-Generator nutzen, den wir von der Kanzlei WILDE BEUGER SOLMECKE gemeinsam mit der Deutschen Gesellschaft für Datenschutz (DGD) entwickelt haben: https://www.wbs-law.de/it-recht/datenschutzrecht/datenschutzerklaerung-generator/.

Allerdings müssen wir darauf hinweisen, dass wir keine 100-prozentige Rechtssicherheit garantieren können.

8. Datenverarbeitung und Einwilligungen überprüfen

Steuerberatungskanzleien müssen des Weiteren prüfen, ob sie alle Daten, die sie bereits bei sich gespeichert haben, weiterhin verarbeiten dürfen und wie dies auch in Zukunft rechtssicher möglich ist. Die Datenverarbeitung ist auch nach der DSGVO weiterhin nur zulässig, wenn es die Verordnung oder ein anderes Gesetz ausdrücklich erlaubt (Verbot mit Erlaubnisvorbehalt). Die praktisch relevantesten Erlaubnistatbestände nach Art. 6 DSGVO sind:

- Einwilligung des Betroffenen, die den Anforderungen der Art. 7, 8 DSGVO entspricht;
- für die Erfüllung eines Vertrags/zur Durchführung vorvertraglicher Maßnahmen erforderlich;
- zur Erfüllung einer rechtlichen Verpflichtung erforderlich;
- zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, wenn keine schutzwürdigen Interessen des Betroffenen überwiegen.

Im Hinblick auf die **Daten von Mandanten oder anderen Vertragspartnern** ist die Verarbeitung nicht selten bereits **zur Erfüllung eines Vertrags** erforderlich und damit gesetzlich erlaubt (Art. 6 Abs. 1 S. 1 b) DSGVO). Achten Sie jedoch in beiden Fällen auf den **Grundsatz der Datenminimierung (Art. 5 Abs. 1 c) DSGVO).** Speichern Sie also nur Daten, die wirklich notwendig sind.

Es kann jedoch auch Fälle geben, in denen es auf die **Einwilligung der Betroffenen,** also z. B. Interessenten oder Mandanten, ankommt. Nämlich immer dann, wenn Sie mehr Daten erheben wollen, als für den Standardvertrag erforderlich, oder einfach, weil Sie Rechtssicherheit haben möchten. Ein wichtiger Fall ist das Kanzleimarketing, etwa die Versendung eines Newsletters. Für die Einwilligung gelten folgende Voraussetzungen: Die Einwilligung muss sich auf einen bestimmten Fall und auf einen bestimmten Verarbeitungszweck beziehen. Der Betroffene muss ausreichend über die Reichweite der Einwilligung informiert gewesen sein, insbesondere auch über die Zwecke der Datenverarbeitung. Die Einwilligung muss freiwillig erteilt werden: Der Einwilligende muss also in der Lage sein, die Einwilligung zu verweigern,

ohne Nachteile zu erleiden. Außerdem müssen Sie hier das neue sog. „Kopplungsverbot“ beachten, Art. 7 Abs. 4 DSGVO: Hier ist zwar juristisch sehr umstritten, wie weit es wirklich greift. Doch um sicher zu gehen, empfehlen wir Ihnen, zukünftig eine Vertragserfüllung, z. B. eine Gratis-Leistung, nicht mehr von einer Einwilligung in die werbliche Datenverarbeitung abhängig zu machen. Der Verantwortliche muss schließlich das Vorliegen einer Einwilligungserklärung nachweisen können. Der Einwilligungstext muss klar formuliert und gut zugänglich sein. Für die Online-Anmeldung zu einem Newsletter sollten Sie hier das Double-Opt-in-Verfahren nutzen, bei dem Nutzer aktiv ein Häkchen betätigen und die Einwilligung anschließend per Mail bestätigen müssen. Zusätzlich müssen Sie deutlich auf die Widerrufsmöglichkeit hingewiesen haben. **Bestehende Einwilligungen müssen Sie i. d. R. nicht neu einholen,** sofern diese den Anforderungen der neuen DSGVO gerecht werden.

Die Daten Ihrer **Mitarbeiter** dürfen Sie speichern, sofern dies **für die Begründung, Durchführung oder Beendigung des Arbeitsverhältnisses erforderlich** ist, § 26 Abs. 1 S. 1 BDSG n. F. Wann dies der Fall ist, muss aber letztlich immer anhand der Umstände des Einzelfalls bestimmt werden, wobei eine Abwägung zwischen den Arbeitgeber- und Arbeitnehmerinteressen stattzufinden hat. Dieser gesetzliche Erlaubnistatbestand bringt durchaus Rechtsunsicherheit mit sich. Doch stattdessen eine **Einwilligung** des Arbeitnehmers einzuholen, wird in den meisten Fällen vor Gericht keinen Bestand haben. Solange es nämlich um das konkrete Arbeitsverhältnis geht, besteht eine Abhängigkeit zwischen Arbeitgeber und Arbeitnehmer, sodass eine erteilte Einwilligung im Zweifel nicht als freiwillig gilt. Lediglich bei gewissen Vereinbarungen betreffend Zusatzleistungen – z. B. Nutzung eines Diensthandys oder Aufnahme in die Geburtstagsliste – dürften Einwilligungen wirksam sein. Daher gilt: Erheben Sie nur so wenige Daten Ihrer Mitarbeiter wie absolut notwendig.

9. Maßnahmen zum Datenschutz und zur Datensicherheit, Datenschutz-Folgeabschätzung

Die DSGVO stellt auch Anforderungen an die Technik und die interne Organisation eines Unternehmens. Sie müssen nach Art. 24, 25 DSGVO konkret geeignete **technische und organisatorische Maßnahmen (TOM)** treffen, um:

1. Die **Einhaltung der Datenschutzgrundsätze**, insbesondere die Datenminimierung und die Datensicherheit zu gewährleisten, den Vorgaben der DSGVO zu genügen und die Betroffenenrechte zu schützen (Datenschutz durch Technik, Art. 25 Abs. 1 DSGVO, auch „**privacy by design**“ genannt). Welche Maßnahmen konkret erforderlich sind, hängt u. a. vom Stand der Technik, der Eintrittswahrscheinlichkeit und Schwere der Risiken für die persönlichen Rechte und Freiheiten sowie den jeweiligen Implementierungskosten ab (Art. 25, 32 DSGVO). Dabei müssen die Maßnahmen in einem wirtschaftlich angemessenen Verhältnis zum Schutzbedarf der verarbeiteten personenbezogenen Daten stehen. Das Gesetz nennt als wichtige, aber nicht abschließende Vorgaben:
   - die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
   - die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
   - die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
   - ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung zu etablieren.
2. Des Weiteren müssen alle technischen Geräte und vor allem IT-Anwendungen zukünftig so voreingestellt werden, dass nur solche Daten erhoben werden, die für den Zweck der Verarbeitung notwendig sind (Datenschutz durch **datenschutzfreundliche Voreinstellungen**, Art. 25 Abs. 2 DSGVO, auch „**privacy by default**“ genannt).

Zudem müssen Sie **Meldemechanismen** etablieren, um im Fall eines **Datenlecks** sofort reagieren zu können. Im Hinblick auf die praxisrelevante Problematik von Datenlecks, deren Dokumentation und diesbezüglichen

Benachrichtigungspflichten verweisen wir auf den Praxisleitfaden *Wickert/Potthoff*, Das neue Datenschutzrecht in der Steuerberaterkanzlei: Praxisleitfaden zur Umsetzung der DS-GVO, des NWB Verlags.

Auch müssen Sie Ihre einzelnen, im Verzeichnis der Verarbeitungstätigkeiten aufgelisteten Prozesse daraufhin überprüfen, ob hier im Einzelfall voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht. Dann müssten Sie eine ein- bis dreistufige **Datenschutz-Folgeabschätzung** (DSFA, Art. 35 DSGVO) durchführen. Ist in dem Unternehmen ein Datenschutzbeauftragter bestellt, wird dieser auf Anfrage beratend in die Durchführung einer Datenschutz-Folgenabschätzung eingebunden (Art. 35 Abs. 2 und Art. 39 Abs. 1 c) DSGVO). Die erste Stufe, eine systematische Risikobewertung (Schwellwertanalyse) sollten Sie in jedem Fall vornehmen. Darin müssen Sie schriftlich begründen, ob ein solches Risiko bei Ihnen für den jeweiligen Prozess vorliegt oder nicht. Für mehrere ähnliche Verarbeitungsvorgänge mit ähnlichem Risiko reicht eine gemeinsame Abschätzung. Als Hilfestellung dienen die ersten „Leitlinien zu DSFA der Art.-29-Datenschutzgruppe“, die aber noch durch eine sog. Blacklist der deutschen Aufsichtsbehörden präzisiert werden (Art. 35 Abs. 4 DSGVO). Steuerberater verarbeiten zwar in großem Umfang besonders schützenswerte Daten (z. B. Gesundheitsdaten und Religionszugehörigkeit i. S. d. Art. 9 DSGVO) sowie sensible Daten (Steuerdaten, Verschwiegenheitspflicht). Doch das bedeutet nicht zwangsweise, dass auch ein hohes Risiko besteht – dies hängt von Ihrem Sicherheitskonzept ab. Letztlich gibt es an diesem Punkt noch keine Rechtssicherheit. Möchten Sie auf Nummer sicher gehen, so sollten Sie in der 2. Stufe eine Bewertung dahingehend vornehmen, ob Ihre geplanten Maßnahmen und Sicherheitsvorkehrungen ausreichen, um den Schutz der Daten zu gewährleisten.

10. Mitarbeiter regelmäßig schulen

Art. 39 Abs. 1 DSGVO nennt als eine der Aufgaben eines Datenschutzbeauftragten die Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter. Daraus ergibt sich, dass entsprechende Schulungen nicht nur sinnvoll, sondern auch gesetzlich vorgesehen sind. Dieses organisatorische Element ist ein wichtiger Teil eines ganzheitlichen Datenschutz-Konzepts in Ihrer Kanzlei. Wann, mit welchem Inhalt und welchen Teilnehmern diese Schulungen stattgefunden haben, sollte dokumentiert werden, damit Sie dies als Teil Ihrer Rechenschaftspflicht gegenüber der Behörde vorzeigen können.

Es ist sinnvoll, entsprechende Schulungen nicht nur zu Beginn der Tätigkeit zu organisieren, sondern später darauf aufzubauen – entweder, weil sich das Datenschutzrecht geändert hat oder weil Sie für Ihre Kanzlei ein neues Konzept entwickelt haben.

Ziel der Schulungen ist es, die Mitarbeiter bei ihren jeweiligen datenschutzrechtlich relevanten Aufgaben zu befähigen, die Datenschutzvorschriften auch in der alltäglichen Praxis einzuhalten. Nur so können auch Sie als Kanzleileitung verhindern, dass es zu Datenpannen kommt und Sie ggf. sogar mit Bußgeldern belegt werden. Denn für das Fehlverhalten Ihrer Mitarbeiter haften Sie selbst.

Zunächst geht es darum, die Mitarbeiter für die Relevanz des Datenschutzes und die damit einhergehenden Risiken zu sensibilisieren.

In einem nächsten Schritt werden die Grundlagen des Datenschutzes vermittelt. Denn bevor man etwas anwendet, muss man die entsprechenden Regelungen auch verstehen.

Basierend auf diesem Grundlagenwissen sollten in den Schulungen spezielle Inhalte vermittelt werden. Hier geht es zum einen um die spezifischen Aufgaben der einzelnen Mitarbeitergruppen (Steuerberater, Sekretariat, Personalabteilung, Buchhaltung etc.). Zum anderen wird das von Ihnen erstellte kanzleiinterne Datensicherheitskonzept erläutert.

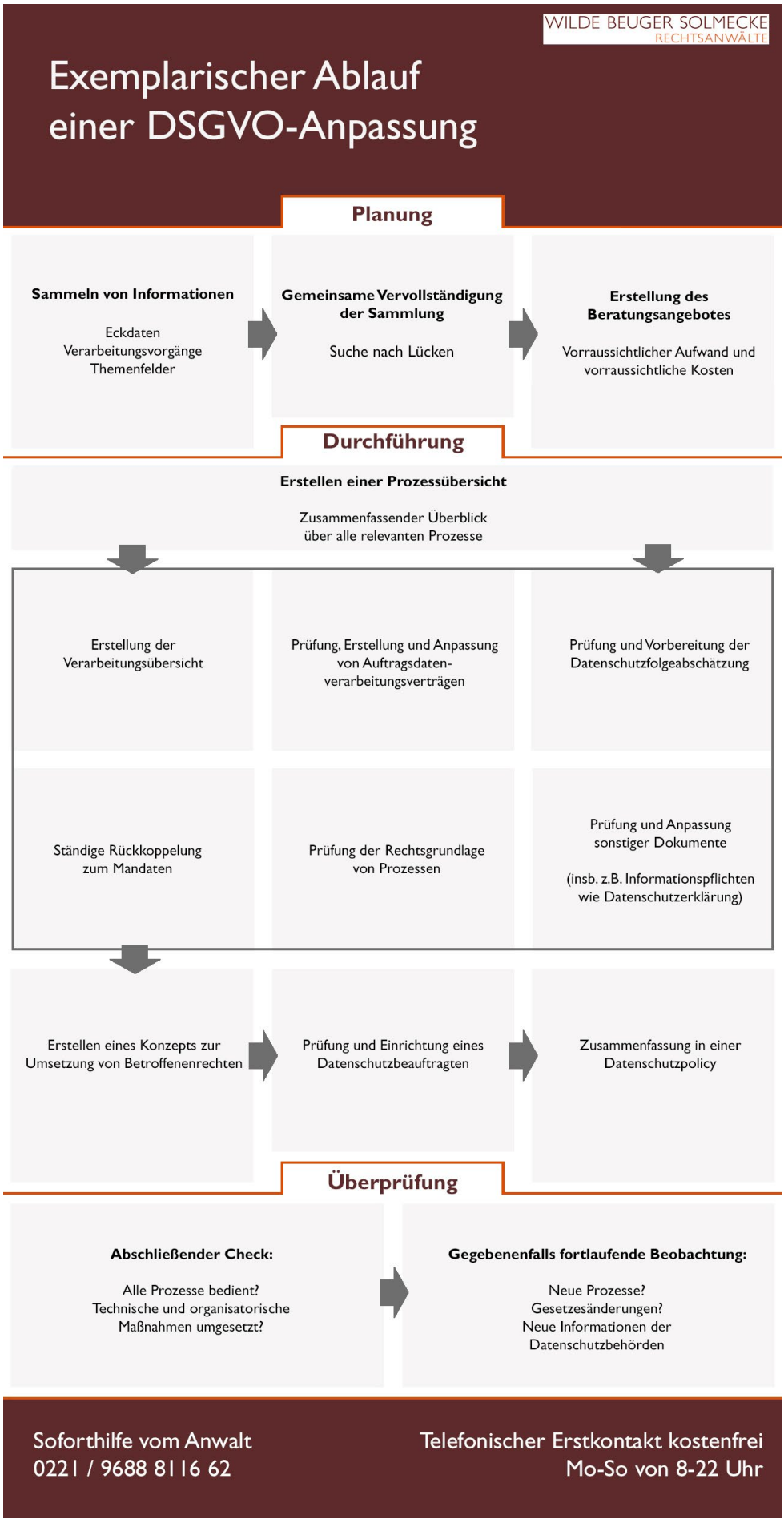
Als Beispiel kann hier z. B. der Ablauf „Auskünfte am Telefon“ gelten, der insbesondere für das Sekretariat von Bedeutung sein dürfte. Hier muss sowohl auf den Datenschutz geachtet als auch das Berufsgeheimnis gewahrt werden. Eine Abwägung mit dem Auskunftsbegehren der anrufenden Person kann im Einzelfall aber schwierig sein. So kann es bei unbekannten Personen sicherer sein, am Telefon erst einmal keine Auskunft zu erteilen und vorher Rücksprache mit der Kanzleileitung zu halten. Sollten sich Behörden melden, sollten diese auf eine schriftliche Anfrage mit Aktenzeichen verwiesen werden.

Abschließend sollte die Schulung auch durch praktische Übungen ergänzt werden.

Schließlich empfiehlt es sich, den Schulungsinhalt noch einmal schriftlich zusammenzufassen und den Mitarbeitern an die Hand zu geben.

11. Abschließende Checkliste: Welche Schritte sollten Steuerberatungskanzleien jetzt einleiten?

- ✓ Handeln Sie so **schnell** wie möglich – bis zum 25. Mai haben Sie nicht mehr viel Zeit. Für die verspätete Umsetzung der DSGVO drohen hohe Bußgelder, wettbewerbsrechtliche Abmahnungen sowie höhere Schadensersatzklagen der betroffenen Personen, deren Daten Sie speichern.
- ✓ **Sammeln Sie alle Informationen** dazu, wer wie welche Daten in Ihrer Kanzlei verarbeitet. Erstellen Sie hierzu in einer Excel-Tabelle ein DSGVO-konformes **Verzeichnis der Verarbeitungstätigkeiten.**
- ✓ Listen Sie auf, wer für Sie weisungsgebundene Daten verarbeitet (**Auftragsverarbeiter**). Prüfen Sie, ob diese Dienstleister alle gesetzlichen Anforderungen erfüllen und lassen Sie sich dies vertraglich zusichern. Überprüfen Sie Ihre zugrundeliegenden Verträge. Stimmen Sie ihre Verzeichnisse der Verarbeitungstätigkeiten aufeinander ab. Etablieren Sie ein internes System, das eine regelmäßige Überwachung Ihrer Auftragsverarbeiter gewährleistet.
- ✓ Prüfen Sie, ob Sie einen **Datenschutzbeauftragten** benennen müssen. In der Regel ist das erst der Fall, wenn in Ihrer Kanzlei mehr als neun Personen am Rechner sitzen und potenziell Zugriff auf personenbezogene Daten haben. Für kleinere Kanzleien herrscht derzeit noch Rechtsunsicherheit, ob Sie einen Datenschutzbeauftragten benötigen.
- ✓ Etablieren Sie ein System, um auf die Rechtewahrnehmung Betroffener, insbesondere auf **Auskunfts- und Löschungsbegehren**, reagieren zu können.
- ✓ Stellen Sie sicher, dass Sie bei Erhebung von personenbezogenen Daten den Betroffenen die gesetzlich vorgeschriebenen **Informationspflichten** mitteilen – etwa auf einem Infoblatt oder verständlich in einer Datenschutzerklärung. Um Ihre **Datenschutzerklärung** anzupassen, können Sie als ersten Orientierungspunkt auch den WBS-Datenschutzerklärungs-Generator nutzen.
- ✓ Prüfen Sie, ob Sie Ihre Daten rechtssicher verarbeiten. Sind die bei Ihnen gespeicherten Daten Dritter bzw. Ihrer Mitarbeiter vom Gesetz so gedeckt? Oder brauchen Sie hierfür eine **Einwilligung**? Wenn ja, erfüllt die Einwilligung auch die Bedingungen der DSGVO? Stellen Sie sicher, dass all Ihre Daten auch zukünftig rechtssicher verarbeitet werden.
- ✓ Etablieren Sie ein System, um bei Ihnen **gespeicherte Daten zu schützen** – sowohl durch interne Abläufe als auch durch Sicherheitsmaßnahmen. Wenn es doch einmal zu einem **Datenleck** kommen sollte, müssen Sie vorbereitet sein und dies schnell den Betroffenen und der Aufsichtsbehörde **melden** können. Empfehlenswert ist es, alle Maßnahmen in einer **Richtlinie für Datenschutz und Datensicherheit** festzuhalten. Prüfen Sie schriftlich, ob Sie eine **Datenschutz-Folgenabschätzung** durchführen müssen.
- ✓ **Schulen Sie Ihre Mitarbeiter** regelmäßig. Ihnen müssen sowohl die Bedeutung als auch die Grundlagen des Datenschutzes bewusst sein. Zudem müssen Sie Ihr individuelles Datenschutzkonzept kennen und anwenden können.
- ✓ Setzen Sie die **richtigen Schwerpunkte** für eine praxistaugliche Umsetzung und verschaffen Sie sich als Kanzleiinhaber eine eigene datenschutzrechtliche Kompetenz. Denn letztlich ist die Einhaltung der neuen datenschutzrechtlichen Regelungen Ihre Pflicht. Nutzen Sie hierzu Wissen, dass sich speziell an Ihre Berufsgruppe richtet.


WILDE BEUGER SOLMECKE
RECHTSANWÄLTE
Exemplarischer Ablauf einer DSGVO-Anpassung
Planung
Sammeln von Informationen
Eckdaten
Verarbeitungsvorgänge
Themenfelder
Gemeinsame Vervollständigung der Sammlung
Suche nach Lücken
Erstellung des Beratungsangebotes
Vorraussichtlicher Aufwand und vorraussichtliche Kosten
Durchführung
Erstellen einer Prozessübersicht
Zusammenfassender Überblick über alle relevanten Prozesse
Erstellung der Verarbeitungsübersicht
Prüfung, Erstellung und Anpassung von Auftragsdaten-verarbeitungsverträgen
Prüfung und Vorbereitung der Datenschutzfolgeabschätzung
Ständige Rückkoppelung zum Mandaten
Prüfung der Rechtsgrundlage von Prozessen
Prüfung und Anpassung sonstiger Dokumente
(insb. z.B. Informationspflichten wie Datenschutzerklärung)
Erstellen eines Konzepts zur Umsetzung von Betroffenenrechten
Prüfung und Einrichtung eines Datenschutzbeauftragten
Zusammenfassung in einer Datenschutzpolicy
Überprüfung
Abschließender Check:
Alle Prozesse bedient?
Technische und organisatorische Maßnahmen umgesetzt?
Gegebenenfalls fortlaufende Beobachtung:
Neue Prozesse?
Gesetzesänderungen?
Neue Informationen der Datenschutzbehörden
Soforthilfe vom Anwalt
0221 / 9688 8116 62
Telefonischer Erstkontakt kostenfrei
Mo-So von 8-22 Uhr

Der Praxisleitfaden DS-GVO für Steuerberater!

- hochaktuell unter Einbeziehung kurzfristiger Entwicklungen der letzten Wochen und Monate
- speziell für die Praxis des Steuerberaters
- aktuelle Praxistipps und Beispiele, Formulierungshilfen und Muster sowie Checklisten und Online-Verweise
- Kurzmaßnahmen, praxisgerechte Schwerpunktsetzung, Erfüllung der tatsächlichen Anforderungen der Aufsichtsbehörden

Dieser Praxisleitfaden wurde speziell für den Datenschutz und die Umsetzung der DS-GVO in Steuerberaterkanzleien entwickelt. Praxisnah beantwortet er zentrale Fragen wie z. B. welche personellen und organisatorischen Maßnahmen zu treffen sind, welche Pflichten Steuerberater haben, welche Sanktionen drohen und welche Maßnahmen bei der Umsetzung zu priorisieren sind.

Zahlreiche Praxistipps, Beispiele und Arbeitshilfen sowie vertiefende Online-Hinweise helfen Ihnen, den datenschutzrechtlichen Ist-Zustand zu analysieren, an die neuen rechtlichen Vorgaben anzupassen und sicher in die Praxis umzusetzen. So garantieren Sie den datenschutzkonformen Umgang mit den sensiblen Daten Ihrer Mandanten und schützen sich gleichzeitig vor möglichen Sanktionen.

Hochaktuell & inklusive zahlreicher Muster, Checklisten und Arbeitshilfen!

Das neue Datenschutzrecht in der Steuerberaterkanzlei: Praxisleitfaden zur Umsetzung der DS-GVO

Wickert · Potthoff
2018. XIV, 91 Seiten. € 24,90
ISBN 978-3-482-**67361**-0
Online-Version inklusive

Bestellen Sie jetzt unter **www.nwb.de/go/shop**

Bestellungen über unseren Online-Shop:
Lieferung auf Rechnung, Bücher versandkostenfrei.

NWB versendet Bücher, Zeitschriften und Briefe CO_2-neutral. Mehr über unseren Beitrag zum Umweltschutz unter **www.nwb.de/go/nachhaltigkeit**

nwb GUTE ANTWORT