Datenschutz in der Steuerberatungskanzlei

Stand: 10/2019

Inhaltsverzeichnis

1. Vorbemerkung

Seit dem **25.05.2018 ist die EU-Datenschutz-Grundverordnung (DSGVO)** in allen Mitgliedstaaten der EU verbindlich anzuwenden. In Deutschland wird die DSGVO durch das Bundesdatenschutzgesetz ergänzt.

Die DSGVO und das Bundesdatenschutzgesetz legen einer Steuer--kanzlei umfangreiche Pflichten im Bereich Datenschutz auf. Es gilt, das **„Grundrecht auf informationelle Selbstbestimmung“** sicherzustellen und die **Daten der Betroffenen** (Mandanten, Mitarbeiter, Geschäftspartner etc.)**vor Missbrauch zu schützen.** Kanzleien mit 20 und mehr Mitarbeitern, die ständig personenbezogene Daten verarbeiteten, haben die Pflicht, einen Datenschutzbeauftragten (DSB) zu bestellen (Näheres zur aktuellen Gesetzeslage in den folgenden Ausführungen). Dies trifft in einer Steuerkanzlei im Grunde auf jeden Mitarbeiter zu. Verarbeiten in einer Kanzlei weniger als 20 Mitarbeiter regelmäßig personenbezogene Daten, liegt die Umsetzung sämtlicher datenschutzrelevanter Themen in den Händen der Kanzleileitung, es sei denn, dass freiwillig ein DSB bestellt worden ist.

Aus Gründen der besseren Lesbarkeit wird im folgenden Text i. d. R. von der „Kanzlei“ oder vom „Verantwortlichen“ gesprochen. Dieses Merkblatt soll kleine und mittlere Kanzleien informieren, damit diese ihre Organisation und Prozesse an die geltende Rechtslage anpassen können.

2. Datenschutzrelevante Themen

Die Themen im Datenschutzmanagement der Kanzlei reichen vom datenschutzkonformen Internetauftritt über die Kontrolle der Dienstleister, die Beschreibung und Bewertung sämtlicher datenschutzrelevanter Prozesse in der Kanzlei bis hin zur Sensibilisierung der Mitarbeiter. Es gab und gibt viel zu tun für den DSB, denn Datenschutz wird oft vernachlässigt. Das Gefährdungspotenzial steigt jedoch durch die moderne Technik stetig an (jederzeitige Verfügbarkeit von Daten, leichtes Erstellen von Profilen und Querverbindungen, Apps zum mobilen Zugriff auf Berufsgeheimnisdaten etc.).

3. Die DSGVO und das Bundesdatenschutzgesetz (BDSG)

Die DSGVO hat weitreichende Auswirkungen auf nahezu alle Kanzleien in Deutschland. Alle Entscheidungsträger sollten sich der Auswirkungen der DSGVO bewusst sein und wissen, was -diese für den Alltag in ihrer Kanzlei bedeutet. Seit dem 25.05.2018 sind in Deutschland sowohl die Vorgaben der DSGVO als auch die Vorgaben des BDSG zu beachten. Mit dem „Zweiten Datenschutz-Anpassungs- und Umsetzungsgesetz EU“ (2. DSAnpUG-EU) wurden weitere Anpassungen im bundesdeutschen Datenschutzrecht vorgenommen.1 Eine der wichtigsten Neuerungen ist die Pflicht zur Bestellung eines Datenschutzbeauftragten: Bisher mussten das Unternehmen tun, die mindestens zehn Personen beschäftigten, die ständig personenbezogene Daten verarbeiteten. Diese Grenze wurde auf mind. 20 Personen angehoben, ohne den Unternehmer von seinen übrigen datenschutzrechtlichen Pflichten zu befreien.

Betrachten wir zunächst die Vorgaben aus Europa.

Die DSGVO

- regelt das Recht auf **Schutz personenbezogener Daten** als **Grundrecht** innerhalb der EU,
- vereinheitlicht weitgehend die derzeit bestehenden 28 nationalen Gesetze zum Datenschutz innerhalb der EU,
- **erhöht die Sanktionen** drastisch (bis zu 10/20 Mio. € bzw. 2/4 % des weltweiten Jahresumsatzes),
- wird durch die Aufsichtsbehörden teilweise wesentlich -**strenger sank-tioniert,** als es bisher der Fall war,
- beinhaltet eine **Meldepflicht** für sog. Datenpanneninnerhalb von **72 Stunden** und eine **Beweislastumkehr**,
- setzt wesentlich mehr an Dokumentation voraus als das BDSG-alt,
- bringt neue Aspekte wie **Privacy by Design & Default, Rechenschaftspflicht, Risikobewertung,**
- **ist seit 25.05.2018 EU-weit verbindlich anzuwenden!**

Das BDSG regelt die Punkte, die die DSGVO im Rahmen sog. Öffnungsklauseln den Mitgliedsstaaten überlässt, u. a. die **Be-stellung eines DSB,** wenn in der Kanzlei i. d. R. **mindestens 20 Personen ständig personenbezogene Daten verarbeiten**. Im Zweifel gehen stets die Regelungen der DSGVO denen des BDSG vor.

Im Einklang mit der DSGVO gilt es noch zahlreiche Aspekte zu beachten. So muss die Kanzlei bei jeder Erhebung personenbezogener Daten dem Betroffenen nun umfangreiche Informationen zur Verfügung stellen. Dies reicht von den Prozessen, in denen personenbezogene Daten verarbeitet werden, über Informationen zur Kanzleileitung und zum DSB bis hin zum Widerspruchsrecht und zur Datenschutzaufsichtsbehörde, bei der sich der Betroffene beschweren könnte, wenn er einen rechtswidrigen Umgang mit seinen Daten befürchtet.

Bei sog. Datenpannen, z. B. bei unberechtigter Weitergabe von personenbezogenen Daten an Dritte oder dem Verlust eines USB-Sticks mit Kundendaten, gilt die Meldepflicht an die Aufsichtsbehörde, wobei die Meldefrist innerhalb 72 Stunden ab Kenntnis der Datenpanne besteht.

Das „Verzeichnis der Verarbeitungstätigkeiten“, in dem jeder einzelne personenbezogene datenverarbeitende Prozess in der Kanzlei beschrieben wird, ist um eine Risikobewertung zu ergänzen. Ggf. ist bei hohem Restrisiko zudem noch eine sog. „Datenschutz-Folgenabschätzung“ erforderlich.

Die Schulung und Sensibilisierung der Mitarbeiter sind unerlässlich.

Der DSB hat mit der DSGVO nunmehr eine verstärkte Über-wachungspflicht hinsichtlich der Einhaltung der Regelungen aus der DSGVO und dem BDSG.

Die Kanzlei trifft nach der DSGVO eine verstärkte „Rechenschaftspflicht“ und muss im Falle einer Datenschutz- oder -Datensicherheitspanne sowie einer Kontrolle durch die Aufsichtsbehörde nachweisen können, welche Maßnahmen implementiert wurden, um Pannen zu verhindern. Hierdurch bestehen erweiterte Anforderungen bzgl. der Dokumentation der IT-Infrastruktur und der IT-Sicherheitsmaßnahmen durch die Kanzlei. Sollte dennoch etwas passieren, sieht die DSGVO empfindliche Bußgelder bis zu 20 Mio. € oder 4 % des weltweiten Jahresumsatzes vor.

Fasst man die Grundsätze der DSGVO zusammen, so handelt es sich um:

- Rechtmäßigkeit der Datenverarbeitung,
- Verarbeitung nach Treu und Glauben und Transparenz,
- Zweckbindung,
- Datensparsamkeit und Speicherbegrenzung,
- Richtigkeit und Aktualität,
- Integrität und Vertraulichkeit sowie
- unabhängige Kontrolle.

Auf die Punkte Rechtmäßigkeit der Verarbeitung und individuelle Datenschutzrechte wird im Folgenden besonders eingegangen.

4. Grundsätze der DSGVO und des BDSG

4.1 Rechtmäßigkeit der Verarbeitung

4.1.1 Einwilligung

Die DSGVO rückt die **Einwilligung der Betroffenen** stark in den Fokus. Immer dann, wenn keine Rechtsgrundlage vorhanden ist, muss der Betroffene seine Einwilligung ausdrücklich erklären. Er muss stets in der Lage sein, seine Einwilligung zu verweigern oder zu widerrufen, ohne dabei Nachteile hinnehmen zu müssen. Auf Betreiben des Europäischen Parlaments wurde zusätzlich ein sog. **„Kopplungsverbot“** mit in die DSGVO aufgenommen. Dies soll verhindern, dass Betroffene Angebote im Internet nur dann nutzen können, wenn sie hierbei Daten von sich preisgeben, die für die Nutzung des entsprechenden Dienstes nicht erforderlich sind. Die Wirksamkeit einer Einwilligung hängt zudem davon ab, dass der Betroffene sie **„informiert“** erteilt. Aus diesem Grund muss im Zuge der Einwilligung darüber informiert werden, wer der **Verantwortliche** ist und zu welchem **Zweck** die Einwilligung erfolgt. Werden im Zuge einer solchen Einwilligung erstmals personenbezogene Daten von Betroffenen erhoben, so gilt es, noch weitere Angaben zu machen, auf die unter 4.2.1 (Information) eingegangen wird. Die Einwilligung selbst muss in **leichter und verständlicher Sprache** verfasst sein. Die Schriftform ist im Grunde nicht gefordert, der Verantwortliche muss aber im Zuge seiner Rechenschaftspflicht nachweisen können, dass eine Einwilligung vorliegt. Neben dem bereits etablierten Verfahren „Double-Opt-in“ bei Einwilligungen in den Newsletter-Bezug gibt es jedoch derzeit im Grunde keine Alternativen zur Schriftform.

Für die Einwilligung von Kindern gelten spezielle Regelungen, wobei die DSGVO hier eine Altersgrenze von 16 Jahren vorsieht. Diese Grenze kann von den Mitgliedsstaaten auf bis zu 13 Jahre herabgesenkt werden, wovon Deutschland allerdings keinen Gebrauch gemacht hat. Dies bezieht sich jedoch nicht auf Einwilligungen im beruflichen oder gewerblichen Bereich, sondern auf Einwilligungen bei einem **Angebot von Diensten der Informationsgesellschaft**, z. B. sozialen Netzwerke, Chats oder Online-Foren. Es ist zu erwarten, dass sich in der Praxis diesbezüglich noch viele Fragen stellen werden.

Bereits erteilte Einwilligungen gelten fort, wenn sie DSGVO-konform erteilt wurden.

Praxistipp Kanzleien sind gut beraten, ihre Prozesse bzgl. des Einholens von Einwilligungen zu überprüfen. Vergessen Sie nicht, die Anmeldung zum Newsletter-Bezug datenschutzkonform zu gestalten („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 i. d. R. eine E-Mail-Nachricht mit 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. Dieses Verfahren hat sich mittlerweile im E-Mail-Marketing in Deutschland durchgesetzt. Denken Sie auch an Datenerhebungen im Rahmen von Tracking der Besucher des Internetauftritts! Als Tracking bezeichnet man die Technik, mit der das Nutzerverhalten im Internet analysiert werden kann. Dafür gibt es spezielle Tracking-Tools, wie z.B. Google Analytics. I. d. R. nutzt man hierfür Cookies oder Zählpixel.

4.1.2 Weitere Verarbeitungsgrundlagen

Die DSGVO erlaubt Datenverarbeitungen, die zur **Erfüllung eines Vertrages** oder eines **vorvertraglichen Schuldverhältnisses** erfolgen. Entscheidend hierbei ist, dass die Erhebung der Daten für die Erfüllung des Vertrages erforderlich ist, was bei einem Steuerberatungsvertrag zunächst grundsätzlich der Fall ist. Entscheidend ist, dass der Mandant im Rahmen der Transparenz über die Datenverarbeitung informiert wird (vgl. 4.2.1).

Im **Beschäftigungskontext** kommen verstärkt die Regelungen des BDSG zum Tragen, da die DSGVO hier eine Öffnungsklausel vorsieht. Beim Einholen von Einwilligungen im Beschäftigungskontext (ein Klassiker ist die **Einwilligung in die Veröffentlichung eines Mitarbeiterfotos** auf der Homepage), ist besondere Sorgfalt geboten. Hier wird die Freiwilligkeit der Einwilligung aufgrund des **wirtschaftlichen Abhängigkeitsverhältnisses** oftmals in-frage gestellt. Vor diesem Hintergrund ist es wichtig, die Einwilligung datenschutzkonform und für den Mitarbeiter transparent zu gestalten und ihm ein Widerrufsrecht einzuräumen. Gerade für die Beendigung des Arbeitsverhältnisses sollten entsprechende Regelungen bzgl. der Entfernung der Bilder von der Homepage getroffen werden. Einwilligungen für die Veröffentlichung von Mitarbeiterbildern in sozialen Netzwerken sind etwas komplizierter zu gestalten, aber durch den DSB mit Sicher-heit zu regeln. Hier müssen weitergehende Vereinbarungen getroffen werden. An dieser Stelle sei auch angemerkt, dass eine **Social Media Guideline** heutzutage fast unvermeidbar ist, wenn man von den Mitarbeitern einerseits Engagement in sozialen Netzwerken in beruflichem Interesse erwartet, andererseits aber auch im Privatleben eine gewisse **„Netiquette"** einfordert.

Im Grunde muss für jede Verarbeitung personenbezogener Daten eine Rechtsgrundlage vorhanden sein. Auch die DSGVO führt somit das Prinzip des sog. **„Verbots mit Erlaubnisvorbehalt"** fort, sprich die Verarbeitung personenbezogener Daten ist grundsätzlich verboten, es sei denn, es gibt eine Rechtsgrundlage, die diese gestattet. Für eine **Weiterverarbeitung** von personenbezogenen Daten muss stets hinterfragt werden, ob die Verarbeitung noch für den ursprünglichen Zweck erfolgt.

Praxistipp Überprüfen Sie alle Prozesse, in denen personenbezogene Daten verarbeitet werden, auf die jeweilige Rechtsgrundlage. Sind weitere Einwilligungen erforderlich? Brauchen Sie eine Social Media Guideline?

4.1.3 Sensible Daten

Die DSGVO sieht für bestimmte Daten besondere Regelungen vor. Betrachten wir zunächst die „besonderen Kategorien personenbezogener Daten". Hierzu gehören im BDSG rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

Auch die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten unterliegen besonderen Auflagen. Gerade die „besonderen Kategorien personenbezogener Daten“ kommen im Grunde in jeder Steuerkanzlei vor, auch wenn diese mit Ausnahme der Mitarbeiterdaten durch das Berufsgeheimnis zusätzlichen und vorrangigen Schutz genießen.

Praxistipp Prozesse, in denen solche Datenbestände vorhanden sind, sind im Verzeichnis der Verarbeitungstätigkeiten eindeutig zu kennzeichnen. Diese Prozesse müssen einem besonderen Schutz unterliegen. Ggf. muss für diese Prozesse eine Datenschutz-Folgenabschätzung durchgeführt werden.

4.1.4 Risikobewertung und Datenschutz-Folgenabschätzung

Jeder Prozess in der Kanzlei, in dem personenbezogene Daten verarbeitet werden, ist hinsichtlich des damit verbundenen Risikos für den Betroffenen zu bewerten. Das Risiko für die Kanzlei (Bußgeld oder Kosten für IT-Experten nach Befall mit Schadsoftware) spielt dabei keine Rolle. Es geht einzig und alleine darum, welche Konsequenzen für den Betroffenen zu befürchten sind, wenn seine Daten offenbart werden. Potenzielle Schäden können physischer, materieller oder immaterieller Art sein. Die DSGVO benennt hier z. B. Diskriminierung, Identitätsdiebstahl, finanzielle Verluste, Rufschädigung, Verlust der Vertraulichkeit oder einen Verstoß gegen das Berufsgeheimnis. Die Risiko-bewertung betrachtet hierbei die Eintrittswahrscheinlichkeit sowie die Schwere des Risikos. Die ermittelten Risiken müssen dann durch -geeignete Abhilfemaßnahmen (insb. durch technisch-organisatorische Maßnahmen) eingedämmt werden. Führt eine Datenver-arbeitung dennoch weiter zu einem hohen Risiko für den Betroffenen, so hat die Kanzlei eine sog. Datenschutz--Folgenabschätzung vorzunehmen. Hierbei ist stets der Rat des DSB einzuholen, sofern ein solcher benannt wurde.

Eine solche Bewertung wird in den meisten Fällen weder die Kanzleileitung noch der DSB allein bewerkstelligen können, sondern es werden je nach Prozess weitere Mitarbeiter (EDV-Beauftragter, ggf. auch Vertreter von Dienstleistern) zu beteiligen sein. Die Verantwortung für diese Bewertung liegt jedoch bei der Kanzleileitung. Die DSGVO sieht vor, dass die Datenschutzaufsichtsbehörden eine Liste der Verarbeitungsvorgänge veröffentlichen, bei denen eine solche Datenschutz-Folgenabschätzung erforderlich ist.

Praxistipp Verschaffen Sie sich möglichst schnell und umfassend einen Überblick über alle Prozesse in der Kanzlei, in denen personenbezogene Daten verarbeitet werden! Stellen Sie für jeden Prozess die Schutzmaßnahmen dar. Mehr dazu beim Verzeichnis der Verarbeitungstätigkeiten (vgl. 9.).

4.2 Individuelle Datenschutzrechte

4.2.1 Information

Der Verantwortliche hat den Betroffenen bei jeder Datenverarbeitung von sich aus aktiv zu informieren. Der Betroffene muss auch wissen, was passiert, wenn er seine Daten nicht preisgibt. Zu den erforderlichen Informationen gehören der Zweck der Datenverarbeitung, die Kontaktdaten des Verantwortlichen, die Kontaktdaten des DSB (sofern vorhanden), ggf. die berechtigten Interessen, auf deren Grundlage die Datenverarbeitung erfolgt, die Empfänger oder Kategorien von Empfängern und (falls geplant) eine Übermittlung in Drittstaaten (außerhalb der EU/des EWR). Hinzu kommt die Dauer der Datenspeicherung, das Recht auf Auskunft und Widerruf sowie das Bestehen eines Beschwerderechts bei der Aufsichtsbehörde. Falls im Zuge der Datenverarbeitung eine automatisierte Entscheidungsfindung stattfindet, ist der Betroffene auch über die involvierte Logik und die Tragweite bzw. die Auswirkungen dieser Entscheidung zu informieren. Bei Aufnahme eines Mandats hat die Kanzlei den Mandanten diese Informationen zur Verfügung zu stellen. Darüber hinaus ist ein solcher Datenschutzhinweis auch im Beschäftigungsverhältnis und im Rahmen des Internetauftritts erforderlich.

Praxistipp Prüfen Sie, an welchen Stellen in der Kanzlei personenbezogene Daten erhoben werden — Personalfrage-bogen bei Einstellung, Mandantendaten bei Verträgen, Gewinnspiele bei Messen, Aufnahme von Interessenten oder Tracking im Rahmen des Internetauftritts usw. Tragen Sie die erforderlichen Informationen zusammen, um Ihre Datenschutz-erklärungen nach den Vorgaben der DSGVO zu gestalten!

4.2.2 Auskunft

Ein Betroffener kann jederzeit Auskunft darüber verlangen, ob eine Kanzlei Daten zu seiner Person verarbeitet. Ist dies der Fall, so hat er ein Recht zu erfahren, welche Kategorien von Daten zu welchem Zweck verarbeitet werden, an wen diese weitergeleitet werden und wie lange sie gespeichert werden. Er ist darüber in Kenntnis zu setzen, dass er ein Recht auf Berichtigung und Löschung bzw. Einschränkung der Verarbeitung dieser Daten hat. Des Weiteren ist er darauf hinzuweisen, dass er ein Recht zur Beschwerde bei einer Aufsichtsbehörde hat. Falls die Daten nicht beim Betroffenen selbst erhoben wurden, ist ihm Auskunft über deren Herkunft zu geben. Ebenfalls hat er wie bei der Information (vgl. 4.2.1) das Recht, über evtl. automatisierte Entscheidungsfindungen informiert zu werden. Werden durch den Verantwortlichen Daten des Betroffenen in ein Drittland oder an internationale Organisationen übermittelt, so ist er über die in diesem Zusammenhang bestehenden Garantien bei der Übermittlung zu informieren. Dem Betroffenen ist auf Verlangen auch eine kostenfreie Kopie dieser Daten auszuhändigen. Die Auskunft ist dem Betroffenen unverzüglich zu erteilen, spätestens jedoch innerhalb eines Monats.

Praxistipp Überprüfen Sie, ob Sie in der Lage sind, in den datenverarbeitenden Prozessen in Ihrer Kanzlei die Daten einer Person schnell und umfassend zu ermitteln. Legen Sie fest, wer in der Kanzlei für Auskunftsanfragen von Betroffenen zuständig ist und informieren Sie Ihre Mitarbeiter über diese Vorgaben, sodass diese bei Anfragen professionell reagieren können.

4.2.3 Berichtigung und Löschung („Recht auf -Vergessenwerden“)

Ein Betroffener hat das Recht, die Berichtigung oder Vervollständigung seiner Daten zu verlangen, wenn diese unrichtig oder unvollständig in der Kanzlei gespeichert wurden.

Wenn die Daten eines Betroffenen in der Kanzlei nicht mehr erforderlich sind und es keine weitere Rechtsgrundlage für die Speicherung mehr gibt (was z. B. bei steuerrelevanten Daten i. d. R. für mindestens zehn Jahre der Fall ist), so sind diese zu löschen. Dies ist auch beim Widerruf einer Einwilligung der Fall oder wenn Daten unrechtmäßig verarbeitet wurden.

Dieses Recht kann mitunter in der Umsetzung komplex sein, so etwa, wenn bereits weitere Stellen auf Veröffentlichungen des Verantwortlichen verwiesen oder diese verlinkt haben. Auch wenn Datenbestände revisionssicher archiviert wurden oder in Back-ups enthalten sind, ist eine Löschung in der Praxis nahezu ausgeschlossen bzw. die Kosten stünden in keinem Verhältnis zum Nutzen. In diesen Situationen tritt an die Stelle der Löschung in vielen Kanzleien zunächst die Einschränkung der Verarbeitung. Diese Lösung genügt jedoch nicht den Vorgaben des DSGVO.

Oftmals vernachlässigt wird das Thema „Bewerbungen“. Abgelehnte Bewerber haben ein „Recht auf Vergessenwerden“, es sei denn, die Kanzlei hat eine Einwilligung für die weitere Speicherung eingeholt. Eine Speicherung von bis zu sechs Monaten erscheint vor dem Hintergrund der zweimonatigen Verjährungsfrist im Allgemeinen Gleichbehandlungsgesetz (AGG) vertretbar.

Praxistipp Überprüfen Sie regelmäßig die Rechtsgrundlagen für die Speicherung personenbezogener Daten in der Kanzlei!

4.2.4 Recht auf Datenübertragbarkeit

Ursprünglich für soziale Netzwerke gedacht, gilt das Recht auf Datenübertragbarkeit nunmehr für alle Daten, die ein Verantwortlicher gespeichert hat. Der Betroffene hat das Recht, seine Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten. Diese Daten können dann wiederum einem anderen Verantwortlichen zur Verfügung gestellt werden. Der Betroffene hat auch das Recht darauf, dass diese Übertragung unmittelbar zwischen zwei Verantwortlichen erfolgt. Fraglich ist, inwieweit dies mit den bislang marktüblichen Systemen realisierbar ist.

Praxistipp Fragen Sie beim Hersteller Ihrer Softwarelösungen an, ob bereits Möglichkeiten vorhanden sind, um die Personenstammdaten und ggf. weitere Daten der Betroffenen in einem maschinenlesbaren Format zu exportieren.

4.2.5 Widerspruch

Ein Betroffener hat das Recht, der Speicherung seiner Daten zu widersprechen. Dies gilt jedoch nur, wenn keine anderen -Gründe, wie z. B. gesetzliche Aufbewahrungsfristen oder Interessen -Dritter, der Löschung widersprechen. Gerade im Bereich Marketing (Newsletter, Mandanten-Infobriefe etc.) gibt es hierzu bereits zahlreiche Regelungen, die es zu beachten gilt. So macht z. B. auch das Gesetz gegen den unlauteren Wettbewerb (UWG) Auflagen hinsichtlich der werblichen Ansprache. Daraus resultiert u. a. die unter 4.1.1 bereits angesprochene Forderung, bei der Anmeldung zum Newsletter-Bezug das „Double-Opt-in“-Verfahren zu nutzen.

Praxistipp Überprüfen Sie die Notwendigkeit der in Ihrem Internetauftritt eingebundenen Tracking-Funktionen. Werden diese Auswertungen in der Kanzlei genutzt? Sind diese Anwendungen in der Lage, ein „Do Not Track“-Signal des -Nutzers umzusetzen?

5. Pflichten des Verantwortlichen

Viele der Pflichten eines Verantwortlichen ergeben sich aus den oben dargestellten individuellen Rechten. Hinzu kommen jedoch noch weitere Aspekte, u. a. die Bestellung eines DSB. Diesem Thema ist jedoch ein eigenes Kapitel (vgl. 6.) gewidmet.

5.1 Privacy by Design und Privacy by Default

Mit der DSGVO haben zwei neue Schlagworte Einzug gehalten: „Privacy by Design“ (Datenschutz durch Technikgestaltung) und „Privacy by Default“ (datenschutzfreundliche Voreinstellungen). Die eingesetzten Lösungen müssen u. a. grundsätzlich dazu geeignet sein, mit ihnen datenschutzkonform zu arbeiten.

Für Kanzleiinhaber heißt das, dass sie bei Investitionen in Lösungen und Technik, mit denen personenbezogene Daten verarbeitet werden, vom Hersteller eine Aussage dazu einfordern müssen, wie in diesen Lösungen mit personenbezogenen Daten umgegangen wird — im Grunde ein neues Kriterium als Entscheidungsgrundlage.

Online-Angebote etwa dürfen keine überflüssigen Datenfelder enthalten. Voreinstellungen müssen so getroffen werden, dass z. B. Profile nicht automatisch veröffentlicht werden oder eine Anwendung nicht automatisch Daten überträgt. Der Betroffene muss aktiv über die Nutzung der Daten bestimmen und nicht erst im Nachhinein reagieren können.

„Privacy by Design“ und „Privacy by Default“ waren im Grunde auch schon im BDSG-alt verankert. Die DSGVO verleiht dieser Forderung jedoch eine neue Qualität.

Praxistipp Überprüfen Sie Ihre Anwendungen und Unter-lagen auf die Einhaltung dieser neuen Anforderungen!

Einige Beispiele: Werden Log-ins nach mehreren Fehleingaben gesperrt? Wird die Komplexität der Passwörter technisch erzwungen? Gibt es bei Online-Zugriffen auf sensible Daten eine Mehrfachauthentifizierung? Beinhalten Ihre Formulare unnötige Datenfelder?

5.2 Rechenschaftspflicht

Seit dem 25.05.2018 ist der Verantwortliche in der Nachweispflicht; die DSGVO spricht hier von einer „Rechenschaftspflicht". Es gilt zu dokumentieren, welche Maßnahmen unternommen wurden, um den Anforderungen der DSGVO gerecht zu werden. Erleidet ein Betroffener einen Schaden, so ist es Sache der Kanzlei nachzuweisen, dass sie alle (wirtschaftlich vertretbaren) Anstrengungen unternommen hat, um diesen Schaden zu verhindern. Im Zusammenhang mit der durch die DSGVO vorgegebenen Beweislastumkehr führt dies in der Kanzlei zu einem erhöhten Dokumentationsaufwand.

5.3 Meldung von Datenpannen

Alle Datenschutzpannen sind nach der DSGVO an die Aufsichtsbehörde zu melden, es sei denn, dass diese Panne voraussichtlich nicht zu einem Risiko für den Betroffenen führt. Eine Benachrichtigung der betroffenen Personen muss dagegen nur dann erfolgen, wenn ein hohes Risiko für deren Rechte und Freiheiten besteht.

Die Meldung muss innerhalb von 72 Stunden nach Bekannt-werden der Panne erfolgen!

Praxistipp Stellen Sie sicher, dass die Meldewege in Ihrer Kanzlei funktionieren! Die Kanzleileitung und der DSB müssen über Datenschutz- und Datensicherheitspannen umgehend informiert werden!

5.4 Verstöße (Bußgeld)

Verstöße gegen die Vorgaben der DSGVO sind mit Bußgeldern bis zu 10 Mio. €/20 Mio. € oder 2 % bzw. 4 % des weltweiten Jahresumsatzes bewehrt. Nahezu alle in diesem Fachbeitrag angesprochenen Vorgaben der DSGVO sind bei Verstoß bußgeldbewehrt. Eines sollte noch explizit herausgestellt werden: Nach der DSGVO ist der Verstoß gegen die Pflicht zur Ergreifung geeigneter und angemessener technischer und organisatorischer Maßnahmen zum Schutz personenbezogener Daten eine Ordnungswidrigkeit!

Diese Bußgeldtatbestände stellen zwar ein Risiko für die Kanzlei dar, spielen aber keine Rolle für die Bewertung der Prozessrisiken in der Kanzlei. Hierfür ist allein die Frage ausschlaggebend, welches Risiko bzw. welcher Schaden für den Betroffenen entstehen könnte.

6. Der Datenschutzbeauftragte (DSB)

Nach DSGVO sind Kanzleien dann zur Bestellung eines DSB verpflichtet, wenn eine Kerntätigkeit mit umfangreicher oder systematischer Überwachung von Personen oder eine Kerntätigkeit mit umfangreicher Verarbeitung besonderer Kategorien von Daten vorliegt. Das BDSG behält jedoch aufgrund einer Öffnungsklausel in der DSGVO die bisherige Regelung bei, sodass diese drei Fallgruppen in Deutschland kaum eine Rolle spielen.

Kanzleien, in denen i. d. R. 20 oder mehr Personen regelmäßig personenbezogene Daten verarbeiten, haben die Pflicht, einen DSB zu bestellen! Bei der Ermittlung der Anzahl der i. d. R. mindestens 20 Personen, die ständig personenbezogene Daten verarbeiten, sind alle „Köpfe" zu zählen: Kanzleileitung, Beschäftigte, freie Mitarbeiter, Praktikanten, Auszubildende.

Um dem Datenschutz hinreichend Rechnung zu tragen und den Anforderungen der DSGVO angemessen zu begegnen, kann die Einführung und Umsetzung eines Datenschutz-Managementsystems jedoch nur gelingen, wenn der DSB auch über die entsprechenden Fachkompetenzen verfügt. Diese machen sich immer an den Anforderungen in der Kanzlei und der Komplexität der kanzleiinternen Organisation fest. Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V. hat hierzu das „berufliche Leitbild der Datenschutzbeauftragten“ entwickelt, auf das im Folgenden kurz eingegangen wird.

6.1 Fachkompetenz

Hierzu gehört eine qualifizierte Ausbildung in zumindest einer der Kategorien Organisation und Prozesse, Informations- und Kommunikationstechnologie (IuK) oder Recht, dazu solide Grundkompetenzen in den beiden anderen Kategorien. Neben einer mindestens zweijährigen Berufserfahrung in den genannten Bereichen muss diese Person eine anerkannte Qualifikation zum DSB nachweisen.

6.2 Datenschutzrechtliche Grundkompetenzen

Im Zuge seiner Ausbildung erhält ein angehender DSB Grundkompetenzen im Datenschutzrecht. Darüber hinaus benötigt er Kenntnis der datenschutzrelevanten Vorschriften in der Steuer-beratung, was bei einer Person aus der Kanzlei gegeben sein sollte. Auch Kenntnis des Allgemeinen Persönlichkeitsrechts und der Grundrechtecharta der EU mit Datenschutzbezug gehören zu seiner Ausbildung, genau wie Grundlagen des europäischen und des deutschen Datenschutzrechts, Rechtsgrundlagen der Verarbeitung personenbezogener Daten und datenschutzrechtliche Anforderungen beim Einsatz von IuK.

6.3 IuK-Grundkompetenzen

Um den datenschutzrechtlichen Anforderungen beim Einsatz der IuK zu genügen, muss ein DSB technisches Verständnis (Sachverhalte der Informationstechnologien) mitbringen. Die Organisation der IuK, die Strukturen von IT-Systemen, IT-Applikationen und IT-Prozessen sollten ihm bekannt sein. Ebenso sollte er über Kenntnisse im Informationssicherheitsmanagement verfügen. Nur mit diesen Fähigkeiten wird er in der Lage sein, Risiken für betroffene Personen, die aus IT-Systemen, IT-Applikationen und IT-Prozessen resultieren, zu erkennen.

6.4 Weitere Kompetenzen

Ein DSB versteht die Kanzleiprozesse und Managementsysteme, kennt Methoden zur Risikoanalyse sowie zu Audit- und Prüfverfahren. Er verfügt über persönliche Integrität, Beratungskompetenz, methodische und didaktische Kompetenz und kann seinen eigenen Status durchsetzen.

6.5 Externer versus interner DSB

Die Funktion des DSB kann sowohl von kanzleiinternen als auch von externen Personen übernommen werden. Der Vorteil des internen DSB ist, dass dieser die Kanzlei kennt und in den internen Ablauf eingebunden ist. Nachteilig kann sich jedoch auswirken, dass neben der Unkündbarkeit des bestellten (zukünftig „benannten“) DSB dessen Tätigkeit nicht zeitlich begrenzt werden kann, da er weisungsfrei ist und sein Zeitaufwand zulasten seiner eigentlichen Tätigkeit geht. Ganz nebenbei besteht zudem die Gefahr der „Betriebsblindheit“. Es gilt darüber hinaus, Interessenkollisionen zu vermeiden. So darf die Funktion des DSB nicht durch den EDV-Leiter, den Personalleiter oder die Kanzleileitung wahrgenommen werden. Als zusätzlichen Kostenaufwand gilt es auch, erforderliche Schulungen, Weiterbildungen, ein eigenes Büro, einen eigenen PC etc. einzukalkulieren.

Ein externer DSB hingegen hat eine neutrale Stellung und Unabhängigkeit, wodurch Interessenkonflikte vermieden werden. Er verfügt bereits über entsprechende Fachkenntnisse. Die Nachteile, dass der externe DSB anfangs die Kanzlei nicht kennt und nicht ohne Weiteres in den internen Ablauf eingebunden ist, sind durch entsprechende Branchenkenntnisse gut zu kompensieren.

Egal jedoch, ob sich ein interner oder externer DSB — oder in kleinen Kanzleien die Kanzleileitung selbst um das Thema kümmert, ist es dringend geboten, den Anforderungen der DSGVO vollumfänglich und gewissenhaft zu begegnen.

6.6 Rolle des Datenschutzbeauftragten (DSB)

Der DSB ist bei der Erfüllung seiner Aufgaben weisungsfrei, er darf deswegen weder abberufen noch benachteiligt werden. Er berichtet unmittelbar der Kanzleileitung. Den Betroffenen gegenüber ist er allerdings zur Geheimhaltung verpflichtet.

Der DSB hat folgende Aufgaben:

- Unterrichtung und Beratung des Verantwortlichen und der Beschäftigten,
- Überwachung der Einhaltung der Datenschutzvorschriften und Überwachung der Sensibilisierung und Schulung der Mitarbeiter und der diesbezüglichen Überprüfungen,
- Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung,
- Zusammenarbeit mit der Aufsichtsbehörde;
- Anlaufstelle für die Aufsichtsbehörde.

Hinzu kommt noch die Beratung der betroffenen Personen zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte gem. DSGVO im Zusammenhang stehenden Fragen.

So ausgeprägt die Überwachungsfunktion des DSB jedoch auch sein mag, die Umsetzung der Anforderungen des DSGVO und des BDSG liegt in der Verantwortung der Kanzleileitung. Datenschutz ist und bleibt Chefsache!

Im Vergleich zum alten Recht haben sich hier die Zuständigkeiten in Richtung Kanzleileitung verschoben — Datenschutz ist Chefsache! Dem DSB kommt nunmehr eine verstärkte Überwachungsfunktion und eine Beratungsfunktion zu.

Praxistipp Überprüfen Sie, ob Ihr DSB über die erforderlichen Fachkompetenzen verfügt! Sollte noch kein DSB bestellt sein, überprüfen Sie die Notwendigkeit einer Bestellung! Bewerten Sie Vor- und Nachteile einer externen und einer internen Lösung!

Bei der Ermittlung der Anzahl der i. d. R. mindestens 20 Personen, die ständig personenbezogene Daten verarbeiten, sind alle „Köpfe“ mitzuzählen: Geschäftsleitung, Beschäftigte, freie Mitarbeiter, Praktikanten, Auszubildende.

6.7 Meldung an die Aufsichtsbehörde

Seit dem 25.05.2018 ist jede Kanzlei verpflichtet, die Kontaktdaten ihres DSB an die für sie zuständige Datenschutzaufsichtsbehörde zu melden. Viele Aufsichtsbehörden haben hierzu Online-Meldeverfahren eingerichtet. Aufgrund der föderalen Struktur der Datenschutzaufsicht in Deutschland ist die hierfür zuständige Behörde im nichtöffentlichen Bereich der jeweilige Landesbeauftragte für den Datenschutz, d. h. in Bayern das Bayerische Landesamt für Datenschutzaufsicht.

7. Auftragsverarbeitung

Von Auftragsverarbeitung spricht man, wenn sich die Kanzlei einer Stelle bedient, die für sie im Auftrag und weisungsabhängig personenbezogene Daten erhebt, verarbeitet oder nutzt (z. B. ein Rechenzentrum, IT-Dienstleister oder Aktenvernichtungsunternehmen). Die Verantwortung und die Haftung für den Umgang mit den personenbezogenen Daten bleiben weiterhin beim Auftraggeber, sprich bei der Kanzlei.

Das vor der DSGVO geltende alte Recht sah vor, dass im -Falle einer Auftragsdatenverarbeitung (§ 11 BDSGalte Fassung) der Auftragnehmer sorgfältig auszuwählen und der Auftrag schriftlich zu erteilen war. Hierbei galt es im Einzelnen schriftlich festzulegen:

- den Gegenstand und die Dauer des Auftrags,
- den Umfang, die Art und den Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und den Kreis der Betroffenen,
- die nach § 9 BDSG alte Fassung zu treffenden technischen und organisatorischen Maßnahmen,
- die Berichtigung, Löschung und Sperrung von Daten,
- die Pflichten des Auftragnehmers, insb. die von ihm vorzunehmenden Kontrollen,
- die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,
- die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,
- mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,
- den Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,
- die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

Zur sorgfältigen Auswahl gehörte u. a. die Überprüfung der technisch-organisatorischen Maßnahmen beim Auftragnehmer. Dies konnte durch ein Vor-Ort-Audit, durch Vorlage von Auditberichten/Zertifizierungen oder durch Selbstauskunft erfolgen.

Mit der DSGVO änderten sich die Begrifflichkeiten, man spricht seit dem 25.05.2018 von Auftragsverarbeitung und Auftragsverarbeitern. Die oben genannten Rechte und Pflichten von Auftraggeber und Auftragnehmer sind im Grunde genommen gleichgeblieben.

Neu ist zudem, dass der Auftragsverarbeiter bei Vertragsschluss die beauftragten Subunternehmer explizit benennen muss. -Gerade im Online-Bereich und bei Service- und Wartungsarbeiten geben viele Dienstleister Aufträge an Subdienstleister weiter. Hier ist bis zum letzten Glied der Kette eine vertragliche Regelung erforderlich. Der Wechsel eines Subunternehmers ist durch den Auftraggeber schriftlich zu genehmigen. In der Praxis werden sich vermutlich Lösungen etablieren, bei denen der Auftragsverarbeiter einen Wechsel schriftlich anzeigt und dem Auftraggeber ein Sonderkündigungsrecht einräumt.

Aufgrund der jüngsten Änderung des § 203 Strafgesetzbuch ist es nunmehr möglich, auch Auftragsverarbeiter und deren Sub-unternehmen als Mitwirkende auf die berufliche Verschwiegenheit zu verpflichten. Sofern im Zusammenhang mit der Beauftragung also personenbezogene Daten verarbeitet werden, die der beruflichen Verschwiegenheit unterliegen, ist eine Ergänzung bzgl. der Verpflichtung des Auftragsverarbeiters und dessen Subunternehmer um § 203 Strafgesetzbuch erforderlich.

Für den Abschluss des Vertrages sowie eventueller Änderungen/Ergänzungen kommt neben der Schriftform auch die elektronische Form in Frage. Die elektronische Form muss aber dokumentiert werden.

Das alte Bundesdatenschutzgesetz sah auch die Fernwartung von EDV-Systemen als Auftragsverarbeitung. Hierzu lässt sich die DSGVO nicht explizit aus. Es ist aber davon auszugehen, dass dieser Umstand im Falle der Fernwartung von EDV-Systemen, in denen personenbezogene Daten verarbeitet werden, auch weiterhin als Auftragsverarbeitung angesehen wird.

Haftete nach altem Recht allein der Auftraggeber für Verstöße des Auftragsverarbeiters, so weitet die DSGVO die Haftung in bestimmten Situationen auch auf den Auftragsverarbeiter aus.

Praxistipp Überprüfen Sie, ob mit allen Dienstleistern, die personenbezogene Daten verarbeiten, entsprechende -Verträge geschlossen wurden! Passen Sie Ihre Verträge an die neue Rechtslage an!

8. Technisch-organisatorischeMaß-nahmen

Nach altem Recht waren die technisch-organisatorischen Maßnahmen in sog. „Acht Gebote“ gegliedert: -Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Ein-gabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle und Trennungskontrolle. Ergänzend waren Vorgaben zur Verschlüsselung zu beachten. Diese Gebote haben mit der DSGVO und dem neuen BDSG nicht an Gültigkeit verloren.

Die DSGVO spricht in diesem Zusammenhang von „Sicherheit der Verarbeitung“ und benennt u. a. die klassischen Schutzziele der IT-Sicherheit. Neu ist der Begriff der „Belastbarkeit“ der Dienste und Systeme. Im Vordergrund steht die Risikobewertung. Die DSGVO fordert, dass die Maßnahmen, die zum Schutz von personenbezogenen Daten getroffen werden, unter Berücksichtigung des Risikos ausgewählt werden. Hierbei ist zu beachten, dass die Betroffenen bei der Risikobewertung in den Mittelpunkt zu stellen sind.

Auch für die technisch-organisatorischen Maßnahmen besteht eine „Rechenschaftspflicht“. Der Verantwortliche muss nachweisen können, dass die Sicherheit der Verarbeitung gewährleistet ist. Damit werden interne Richtlinien und externe Zertifizierungen noch weiter an Bedeutung gewinnen. In diesem Zusammenhang gilt es, noch weitere Informationen der Aufsichtsbehörden abzuwarten, da gem. DSGVO zukünftig nur noch akkreditierte Zertifizierungsstellen externe Zertifizierungen vornehmen dürfen.

Praxistipp Etablieren Sie ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technisch-organisatorischen Maßnahmen! Legen Sie konkrete Vorgaben für die Risikobewertung Ihrer Prozesse fest!

9. Verzeichnis der Verarbeitungs-tätigkeiten

Die DSGVO fordert von Unternehmen, die mehr als 250 Mitarbeiter beschäftigen, ein Verzeichnis aller Prozesse, in denen personenbezogene Daten verarbeitet werden, zu führen, es sei denn, eine von ihnen vorgenommene Verarbeitung birgt ein Risiko für die Rechte und Freiheiten der betroffenen Personen, die Verarbeitung erfolgt nicht nur gelegentlich oder es erfolgt eine Verarbeitung besonderer Datenkategorien bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten. Das Verzeichnis ist also zu erstellen, wenn besondere Arten personenbezogener Daten verarbeitet werden. Dies ist im Grunde in einer Steuerkanzlei immer der Fall, sodass in der Praxis nahezu keine Kanzlei umhinkommen wird, dieses Verzeichnis zu erstellen.

Um das „Recht auf Vergessenwerden“ umzusetzen, muss die Kanzlei wissen, welche Daten in welchen Prozessen vorhanden sind. Auch dies wird ohne das Verzeichnis schwerlich gelingen.

Hinzu kommt die Forderung, die Risiken der Prozesse zu bewerten. Auch dies setzt die Kenntnis aller Prozesse voraus.

Im Verzeichnis der Verarbeitungstätigkeiten sind zahlreiche Angaben aufzunehmen, u. a. die Angabe des DSB.

Auftragsverarbeiter haben ebenfalls ein Verzeichnis zu führen. In diesem sind Name und Kontaktdaten des Auftragsverarbeiters und jedes Verantwortlichen, in dessen Auftrag er tätig ist, aufzuführen. Der DSB des Auftraggebers ist ebenso zu nennen wie die Kategorien von Verarbeitungen, die im Auftrag jedes Auftraggebers durchgeführt werden. Hinzu kommen ggf. Angaben zu Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation.

Praxistipp Überprüfen Sie, ob Sie alle Prozesse erfasst haben, in denen personenbezogene Daten verarbeitet werden!

10. Sonderfall Videoüberwachung

Auf den Umstand der Videoüberwachung ist mit Hinweisschildern (Logo „Videoüberwachung“ und Angaben zum Verantwortlichen: Name und Adresse) aufmerksam zu machen. Der Prozess der Videoüberwachung ist zu dokumentieren (Kameratypen, Blickwinkel, Reichweite, Speicherdauer). I. d. R. geht man bei der Speicherdauer von ein bis zwei Arbeitstagen aus, eine Frist von bis zu zehn Wochentagen kann aber noch als angemessen betrachtet werden, sofern ein sachlich zu rechtfertigender Grund vorliegt.

Für die Kanzlei ändert sich somit im Grunde nicht viel. War die Überprüfung der Videoüberwachung bislang durch den DSB vorab durchzuführen, so sollte auch weiterhin der DSB zu Rate gezogen werden. In vielen Fällen dürfte dies aufgrund der Notwendigkeit einer Datenschutz-Folgenabschätzung ohnehin erforderlich sein. Es ist davon auszugehen, dass hier noch weitere Konkretisierungen durch den EU-Datenschutz-Ausschuss erfolgen werden.

Praxistipp Überprüfen Sie den Prozess der Videoüberwachung!

Sind alle Beobachtungsbereiche ausgeschildert? Sind die Schilder zu erkennen, bevor der Beobachtungsbereich betreten wird? Ist auf den Schildern der Verantwortliche für die Videoüberwachung benannt?

11. Datenschutz-Managementsystem

Das Datenschutz-Managementsystem hat durch die Anforderungen der DSGVO eine erhebliche Bedeutung erhalten. Wir haben mehrere Themen wie Rechenschaftspflicht, Meldung von Datenpannen, Risikobewertung oder Datenschutz-Folgenabschätzung bereits oben angesprochen. Dokumentation und Versionierung spielen eine wesentliche stärkere Rolle als früher. Im Folgenden werden stichpunktartig einige Punkte und Unterlagen angeführt, die in einer Kanzlei auf jeden Fall vorhanden sein sollten:

- Bestellung eines DSB (Bestellungsurkunde, falls erforderlich),
- Datenschutzleitlinie und Datenschutzhandbuch/Datenschutzkonzept
  - Verantwortlichkeiten in der Kanzlei
  - Stellenbeschreibung DSB
  - Kategorisierung personenbezogener Daten
  - Risikobewertung und Datenschutz-Folgenabschätzung
  - Verhalten am Telefon
  - Clean Desk Policy etc.
- Richtlinie zur Nutzung der EDV, ggf. IT-Sicherheitskonzept,
- Checklisten zur Auswahl von technischen und organisatorischen Maßnahmen,

- Regelung der Privatnutzung von Internet, E-Mail und Telefon,
- Liste der Dienstleister und Verträge zur Auftragsverarbeitung,
- Verzeichnis der Verarbeitungstätigkeiten,
- Protokollierungs-, Archivierungs- und Löschkonzept,
- Datensicherungskonzept,
- Notfallplan,
- Nachweis der Schulung der Mitarbeiter,
- Dokumentation interner und externer Audits, ggf. Zertifizierungen,
- Datenschutzhinweise für sämtliche Datenerhebungen (auch Internetauftritt!),
- Dokumentation interner und externer Audits, ggf. Zertifizierungen,
- Datenschutzhinweise für sämtliche Datenerhebungen (auch Internetauftritt!).

MUSTER Verzeichnis der Verarbeitungstätigkeiten

Name, Firma	Kanzlei Mustermann & Partner
Vorstände, Geschäftsführer, Inhaber	Herbert Mustermann, Sabine Müller
Anschrift, Telefon, E-Mail	Hauptstraße 15, 98765 Musterhausen Tel.: 01234/56789-0 E-Mail: info@mustermann.de
Datenschutzbeauftragter	Karl Schutzheimer
Anschrift, Telefon, E-Mail	Hauptstraße 15, 98765 Musterhausen Tel.: 01234/56789-12 E-Mail: dsb@mustermann.de

Hinweis: Die nachfolgenden Angaben sind lediglich als Beispiele zu sehen und nicht allgemeingültig auf die Verfahren Ihrer Kanzlei zu -übertragen!

Auflistung:	01 Finanzbuchhaltung	02 Mandanten-Infoabend
Verfahren/Anwendungen/Programme		
Zwecke der Datenverarbeitung	Erfassung aller ein- und ausgehenden Zahlungen des Unternehmens (vgl. § 238 Abs. 1 HGB)	Führen einer Gästeliste/Einladungsliste zur Vorbereitung und Durchführung eines Mandanten-Infoabends
Kategorien betroffener Personen	Mandanten, Lieferanten, Dienstleister	Mandanten, Interessenten und Daten weiterer Gäste
Kategorien personenbezogener Daten	Mandantenstammdaten und Rechnungs-daten von Debitoren und Kreditoren	Kontaktdaten im Zuge der Anmeldung und zur Erstellung des Namensschildes
Besondere Arten personenbezogener Daten (ja/nein)	ja	nein
Kategorien von internen und externen Empfängern (einschließlich Drittland oder internationaler Organisation)	Beschäftigte, Mandanten, Finanzbehörden und ggf. weitere Behörden	Beschäftigte

Übermittlung in ein Drittland, Name des Drittlandes. Übermittlung an eine internationale Organisation, Name der internationalen Organisation	nicht vorgesehen	nicht vorgesehen
Dokumentierung geeigneter Garantien im Drittland, bzw. bei der internationalen Organisation	nicht relevant	nicht relevant
Fristen für die Löschung der Daten	zehn Jahre	nach Durchführung der Veranstaltung
Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen	vgl. gesonderte Beschreibung der technisch-organisatorischen Maßnahmen	vgl. gesonderte Beschreibung der technisch-organisatorischen Maßnahmen

12. Fazit

Der Umfang dieses Merkblatts ließ es nicht zu, auf spezielle Fragestellungen einzugehen, wie Auftragsverarbeitung außerhalb der EU, Binding Corporate Rules, Codes of Conduct und vieles mehr. Auch mussten viele Aspekte im Detail offenbleiben. Dies war jedoch auch nicht die Zielstellung. Fazit ist, dass die Anforderungen an das Datenschutz-Managementsystem einer Kanzlei bereits in den vergangenen Jahren aufgrund zunehmender technischer Komplexität und zahlreicher neuer Anforderungen gestiegen sind. Mit der DSGVO haben sich die rechtlich-organisatorischen Anforderungen verschärft und die Bußgeldsummen drastisch erhöht. Datenschutz wird aber auch mehr und mehr zum Image- und Compliance-Thema. Eine Zertifizierung nach ISO 9001/2015 ohne Umsetzung der datenschutzrechtlichen Anforderungen ist künftig kaum noch möglich.

Gehen Sie das Thema Datenschutz jetzt aktiv an!

13. Checkliste

Prüfen Sie Ihr Datenschutzmanagement auf der Grundlage der folgenden Checkliste:

Lfd.
Nr.

1. Datenschutz ist Chefsache!
   - — Gibt es eine Leitlinie zum Datenschutz?
   - — Gibt es ein Datenschutzhandbuch?
   - — Gibt es darüber hinaus Regelungen zum Umgang mit der IT und zur Privatnutzung von Internet, E-Mail und Telefon?
   - — Finden regelmäßige Schulungen/Sensibilisierungen der Mitarbeiter statt?
2. Datenschutzbeauftragte(r)
   - — Ist die Benennung eines Datenschutzbeauftragten erforderlich? (Es sind alle Köpfe zu zählen!)
   - — Falls ja, gibt es eine schriftliche Benennung, in der auch das Aufgabengebiet klar umrissen ist?
   - — Ist der zeitliche Umfang der Tätigkeit festgelegt?

3. Verzeichnis der Verarbeitungstätigkeiten
   - — Gibt es ein Verzeichnis der Verarbeitungstätigkeiten?
   - — Wurden die Risiken der Verarbeitung bewertet?
   - — Gibt es für jede Verarbeitung eine Rechtsgrundlage?
   - — Sind klare Aufbewahrungs- und Löschfristen festgelegt?
   - — Sind alle Stellen bekannt, an denen personenbezogene Daten erhoben und gespeichert werden?
   - — Ist sichergestellt, dass datenschutzrechtliche Belange bei Beginn oder Änderung eines jeden Prozesses -Berücksichtigung finden?
4. Einwilligungen
   - — Sind alle Einwilligungen DSGVO-konform?
   - — Wird insb. das Kopplungsverbot beachtet?
   - — Wird auf die Rechte in Zusammenhang mit der Einwilligung verwiesen?
5. Auftragsverarbeitung
   - — Sind alle „Verträge zur Auftragsverarbeitung“ vorhanden?
   - — Gibt es eine Übersicht über alle Dienstleister und freien Mitarbeiter?
   - — Wurden die Verträge zur Auftragsverarbeitung an die DSGVO angepasst?
6. Information
   - — Gibt es einen Datenschutzhinweis für den Internetauftritt?
   - — Gibt es Datenschutzhinweise für Kunden?
   - — Gibt es Datenschutzhinweise für Mitarbeiter?
7. Weitere Betroffenenrechte
   - — Gibt es ein Verfahren zur Beantwortung von Auskunftsersuchen?
   - — Wird das Recht auf Berichtigung und Löschung sichergestellt?
   - — Kann das Recht auf Datenübertragbarkeit sichergestellt werden?
   - — Wird das Recht auf Widerspruch sichergestellt?
8. Datenschutzverletzungen
   - — Werden Datenschutzpannen durch die Mitarbeiter erkannt?
   - — Ist sichergestellt, dass Datenschutzpannen innerhalb von 72 Stunden an die Aufsichtsbehörde gemeldet werden können?
   - — Gibt es ein Verfahren zur Benachrichtigung der betroffenen Personen?
9. Internetauftritt
   - — Wurde der Internetauftritt auf Datenschutzkonformität überprüft?

10. Videoüberwachung

— Wurde die Videoüberwachung (falls vorhanden) auf Datenschutzkonformität überprüft?