5.2.4 Hinweise[*] der Bundessteuerberaterkammer zum Datenschutz und zur Datensicherheit in der Steuerberaterpraxis

Beschlossen vom Präsidium der Bundessteuerberaterkammer am 25. April 2012

Gliederung

I. Grundsätzliche Bemerkungen

1. Verschwiegenheit und Datenschutz - Wesensmerkmale des Berufs Steuerberater

Bei der Beurteilung dieser Merkmale lassen sich folgende vier Fallgruppen differenzieren

- Die Verschwiegenheitspflicht des Steuerberaters, unabhängig davon, ob er angestellt oder selbstständig tätig ist, ergibt sich aus § 57 Abs. 1 StBerG, § 5 BOStB und § 203 Abs. 1 Nr. 3 StGB. Sie stellt eine der Grundvoraussetzungen für die steuerberatende Tätigkeit dar. Die Verschwiegenheitspflicht erstreckt sich auf alles, was dem Steuerberater in Ausübung des Berufs oder bei Gelegenheit seiner Berufstätigkeit anvertraut oder be-

[**] Die Hinweise werden derzeit überarbeitet und bilden nicht den aktuellen Rechtsstand ab.

kannt geworden ist. Hierzu gehört u. a. auch die bestehende Mandatsbeziehung selbst. Geschützt werden auch solche Tatsachen, die anlässlich einer sog. „vereinbaren“ Tätigkeit zur Kenntnis gelangt sind sowie solche Tatsachen, die keine unmittelbare Verbindung zur Berufstätigkeit haben, wie z. B. die privaten Verhältnisse des Mandanten. Wegen der zentralen Bedeutung der Verschwiegenheit ist bereits jeder Anschein einer Verletzung zu vermeiden. Die Verschwiegenheitspflicht besteht auch nach Beendigung des Auftragsverhältnisses zeitlich unbeschränkt fort.

- **Mitarbeiter i. S. d. § 62 StBerG** sind vom Praxisinhaber bzw. Arbeitgeber zur Verschwiegenheit zu verpflichten. Dies gilt unabhängig davon, ob sie angestellt tätig oder freie Mitarbeiter i. S. v. § 17 BOStB sind. Hierzu zählen neben Steuerfachangestellten und Steuerfachwirten z. B. auch Auszubildende, Aushilfskräfte oder gelegentlich helfende Familienmitglieder. Die Verpflichtung ist schriftlich vorzunehmen und hat sich auf alle einschlägigen Vorschriften zu erstrecken. Entsprechende Vordrucke sind in den berufsständischen Verlagen erhältlich. Durch die Verpflichtung zur Verschwiegenheit werden die Gehilfen des Steuerberaters diesem in Bezug auf das berufliche Auskunfts- und Zeugnisverweigerungsrecht gleichgestellt (s. u. a. § 102 Abs. 2 AO, § 53a StPO). Eine Verletzung der Verschwiegenheitspflicht ist auch für sie strafbewehrt (§ 203 Abs. 3 Satz 2 StGB).

- **Sonstige Beschäftigte des Steuerberaters, die nicht Mitarbeiter im Sinne des § 62 StBerG** sind, die aber Zugang zu den Praxisräumen und den geschützten Personendaten haben, z. B. Reinigungspersonal, sind nicht nach dem Steuerberatungsgesetz, sondern bei Aufnahme ihrer Tätigkeit gemäß § 5 Satz 2 BDSG auf das Datengeheimnis zu verpflichten. Unabhängig von der Verpflichtung auf das Bundesdatenschutzgesetz dürfen diese Personen keinen Zugang zu berufsrechtlich geschützten Daten oder Akten haben.

- Rechtsnachfolger der Berufsangehöriger und weitere Personen i. S. d. § 203 Abs. 3 Satz 3 StGB sind ebenfalls auf das Berufsgeheimnis verpflichtet und dem Steuerberater in Bezug auf das berufliche Auskunfts- und Zeugnisverweigerungsrecht gleichgestellt.

- Dem Datenschutzbeauftragten des Berufsträgers steht wie diesem ein Zeugnisverweigerungsrecht zu (§ 4f Abs. 4a BDSG und § 203 Abs. 2a StGB). Über die Ausübung dieses Rechts entscheidet der Berufsträger.

- **Beschäftigte eines Fremdunternehmens**, wie z. B. von DV-Wartungsfirmen, Aktenvernichtungs-, oder Reparaturdiensten, kann der Steuerberater nicht auf die Wahrung des Datengeheimnisses verpflichten. Hier gilt vielmehr über § 11 Abs. 5 BDSG die Pflicht, den Auftragnehmer sorgfältig auszuwählen und einen schriftlichen Auftrag zu erteilen . In diesem Rahmen muss der Steuerberater mit dem Fremdunternehmen vereinbaren, dass dieses seine bei ihm tätigen Personen auf das Datengeheimnis des BDSG verpflichtet.

2. Verhältnis Berufsrecht und Datenschutzrecht

Die berufliche Pflicht zur Verschwiegenheit und das Datenschutzrecht sind zwei Regelungskreise, die sich partiell überschneiden. Sowohl die berufliche Pflicht zur Verschwiegenheit als auch das Datenschutzrecht zielen auf einen sorgsamen Umgang mit personenbezogenen Daten und dienen der Abwehr unbefugter Zugriffe durch Dritte einschließlich des Staates.

Die berufsrechtliche Verschwiegenheitspflicht dient dem Schutz aller durch das Mandat bekannt gewordenen Informationen und damit dem Vertrauen des Mandanten in die Integrität der von ihm zur Verfügung gestellten Daten. Darüber hinaus schützen die Regelungen zur berufsrechtlichen Verschwiegenheit (vgl. § 203 StGB, § 57 Abs. 1 StBerG) auch das allgemeine Vertrauen in die Verschwiegenheit des Berufsstands, da die Verschwiegenheit nicht nur auf die personenbezogenen Daten beschränkt, sondern auch Geschäfts- und Betriebsgeheimnisse umfasst. Das öffentliche Interesse an diesen Schutzgütern zeigt sich in der strafrechtlichen Sanktionierung (§ 203 Abs. 1 Nr. 3, Abs. 3 Satz 2 StGB).

Schutzzweck des Datenschutzrechts ist dagegen das Recht auf informelle Selbstbestimmung. Das Bundesdatenschutzgesetz bzw. die Landesdatenschutzgesetze sind jedoch nur nachrangig anzuwenden. Sie kommen dann zur Anwendung, wenn Spezialgesetze keine bereichsspezifischen Regelungen treffen. Der Grundsatz der Subsidiarität des BDSG ist in § 1 Abs. 3 Satz 1 BDSG formuliert. Darin heißt es: „Soweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor“. Im Steuerberatungsgesetz sind dies die §§ 57, 62, die die Verschwiegenheitspflicht des Steuerberaters und seiner Gehilfen regeln. Soweit der Anwendungsbereich dieser beiden Vorschriften reicht, kommen die datenschutzrechtlichen Vorschriften des Bundes und der Länder nicht zur Anwendung. Weitere Voraussetzung für die Anwendung des BDSG bei nicht-öffentlichen Stellen[†] ist, dass sie Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben (§ 1 Abs. 2 Nr. 3, 1. Alt. BDSG) bzw. ein manueller Datenumgang einen Dateibezug aufweist (§ 1 Abs. 2 Nr. 3, 2. Alt. BDSG) und keine Verwendung ausschließlich für persönliche oder familiäre Tätigkeiten vorliegt. Das bedeutet, dass z. B. manuell geführte Mandantenkarteien oder elektronisch geführte Akten und Listen genauso unter das BDSG fallen wie die auf einem elektronischen Terminkalender gespeicherten dienstlichen Notizen. In Papierform vorliegende Akten und Aktensammlungen fallen in der Regel nicht unter das BDSG. Insoweit gilt allerdings die berufsrechtliche Pflicht zur Verschwiegenheit.

[†] Das sind natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts.

In einer Steuerberaterpraxis zählen zu den personenbezogenen Daten i. S. d. BDSG vor allem die im Rahmen der steuerberatenden Tätigkeit verwendeten Mandantendaten. Aber auch die Daten über Angestellte und Dienstleister der Praxis stellen Daten im vorgenannten Sinne dar.

3. Bestellung eines Datenschutzbeauftragten

Die Bestellung eines Datenschutzbeauftragten ist erforderlich, wenn in der Steuerberaterpraxis in der Regel mehr als neun Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten befasst sind (§ 4 f Abs. 1 Satz 4 BDSG). Aus datenschutzrechtlicher Sicht ist allein die Anzahl der Personen entscheidend, die sich im Rahmen ihrer Aufgabenerfüllung mit der automatisierten Verarbeitung personenbezogener Daten befassen. Auszubildende oder freie Mitarbeiter sind mitzuzählen. Durch die Formulierung „in der Regel“ wird klargestellt, dass Personen, die nicht regelmäßig mit der automatisierten Verarbeitung personenbezogener Daten befasst sind, unberücksichtigt bleiben können.

Die Auffassung, dass der Steuerberater unabhängig von der Anzahl der bei ihnen tätigen Personen nach § 4 f Abs. 1 Satz 6 BDSG zur Bestellung eines Datenschutzbeauftragten verpflichtet seien, ist unzutreffend. Zwar haben Steuerberater im Rahmen ihrer beruflichen Tätigkeit u. a. auch besondere Arten personenbezogener Daten i. S. d. § 3 Abs. 9 BDSG, wie z. B. den Konfessionsstand, zu erheben und zu verarbeiten. Allerdings liegt hierzu regelmäßig entweder die Einwilligung des Betroffenen vor und/oder die Erhebung, Verarbeitung oder Nutzung dient der Zweckbestimmung des Vertragsverhältnisses, was eine Vorabkontrolle und damit die Bestellung eines Datenschutzbeauftragten – allein wegen der Verarbeitung dieser Daten – entbehrlich macht (§ 4 d Abs. 5 Satz 2, 2. Halbsatz BDSG).

Datenschutzbeauftragter kann sowohl ein Mitarbeiter der Steuerberaterpraxis als auch eine externe Person sein. § 4 f Abs. 2 Satz 3 BDSG ermöglicht es Berufsgeheimnisträgern, also auch Steuerberatern, eine Person außerhalb der Praxis zum Beauftragten für Datenschutz zu bestellen.

Der Datenschutzbeauftragte hat ein Zeugnisverweigerungsrecht im Hinblick auf die Daten, die der beruflichen Geheimhaltungspflicht des Praxisinhabers/Steuerberaters unterliegen. Allerdings entscheidet der Steuerberater, ob und in welchem Umfang der Datenschutzbeauftragte von diesem Recht Gebrauch machen darf. Um dem Datenschutzbeauftragten diese Konstellation ausreichend deutlich zu machen, empfiehlt sich die Aufnahme einer klarstellenden Regelung im Bestellungsvertrag. In gleichem Umfang besteht ein Beschlagnahme-

verbot für die Akten und Schriftstücke des Datenschutzbeauftragten (vgl. § 4 f Abs. 4 a BDSG).

Kanzleiinhaber, die nicht verpflichtet sind, einen Datenschutzbeauftragten zu bestellen, haben in anderer Weise sicherzustellen, dass die Erfüllung der Aufgaben des Datenschutzbeauftragten (vgl. § 4 g Abs. 1 und 2 BDSG) gewährleistet ist (§ 4 g Abs. 2 a BDSG). Dieser Verpflichtung wird insbesondere durch die Erstellung des gemäß § 4 e BDSG erforderlichen Verfahrensverzeichnisses und dessen Meldung an die Datenschutzaufsichtsbehörde gemäß § 4d Abs. 1 BDSG sowie eine (dokumentierte) turnusmäßige Belehrung der Mitarbeiter in Bezug auf die datenschutzrechtlichen Vorschriften einschließlich der Überwachung der Einhaltung dieser Vorschriften nachgekommen.

4. Auftragsdatenverarbeitung

Wird eine andere Stelle mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beauftragt, ist der Aufraggeber für die Einhaltung der Vorschriften des BDSG verantwortlich (§ 11 Abs. 1 BDSG). Der Auftraggeber ist verpflichtet, den Auftragnehmer sorgfältig auszuwählen und in der schriftlichen Beauftragung bestimmte Inhalte zu vereinbaren, wie z. B. den Umfang, die Art und den Zweck der vorgesehenen Verarbeitung oder die Art der Daten und den Kreis der Betroffenen (§ 11 Abs. 2 BDSG). Darüber hinaus muss der Auftraggeber sich überzeugen, dass die beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen eingehalten werden (§ 11 Abs. 1 Satz 4 BDSG). Eine persönliche Augenscheinnahme ist nicht erforderlich, sofern die Überzeugung auf andere Weise gebildet werden kann, z. B. durch Vorlage von Auditierungs-Testate des Auftragnehmers.

Sowohl die nicht ordnungsgemäße Beauftragung zur Auftragsdatenverarbeitung als auch die unterbliebene Kontrolle sind bußgeldbewehrt (§ 43 Abs.1 Nr. 2b BDSG).

Eine Auftragsdatenverarbeitung liegt auch vor, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann (§ 11 Abs. 5 BDSG).

Das Verhältnis zwischen Mandant und Steuerberater stellt nach der herrschenden Meinung keine Auftragsdatenverarbeitung dar. Hierbei handelt es sich regelmäßig um eine Funktionsübertragung. Die Begründung hierfür liegt darin, dass dem Steuerberater die zugrundeliegende Aufgabe übertragen wird und dafür eine Dienstleistung erbracht wird, die über eine

weisungsabhängige, technische Dienstleistung hinausgeht. Das bedeutet, dass der Steuerberater kein Auftragnehmer i. S. d. § 11 BDSG ist und (Steuerberatungs-) Verträge nicht angepasst werden müssen.

Bei der Beauftragung von Dienstleistern, die den Steuerberater unterstützen und dabei mit personenbezogenen Daten zu tun haben können, liegt hingegen eine Auftragsdatenverarbeitung vor. Dies gilt z. B bei der Einschaltung eines Rechenzentrums, eines Wartungspartners des EDV-Systems oder von Entsorgungstätigkeiten von Datenträgern. Hierbei ist dann der Steuerberater als Auftraggeber in der Verantwortung, dass eine BDSG-konforme Beauftragung abgeschlossen wird.

5. Informationspflichten nach § 42a BDSG

Bei der unrechtmäßigen Kenntniserlangung von bestimmten personenbezogenen Daten durch Dritte, sind die Betroffenen und die datenschutzrechtliche Aufsichtsbehörde (Kontaktdaten der Datenschutzaufsichtsbehörden der Länder s. Homepage des Bundesdatenschutzbeauftragten: www.bfdi.bund.de). unverzüglich zu informieren, wenn für die Betroffenen schwerwiegende Beeinträchtigungen für ihre Rechte oder ihre schutzwürdigen Interessen drohen (§ 42a BDSG). Zu diesen Daten gehören nach § 42a Abs. 1 Nr. 2 BDSG auch personenbezogene Daten, die einem Berufsgeheimnis unterliegen. Für das Merkmal der schwerwiegenden Beeinträchtigung der Rechte oder der schutzwürdigen Interessen müssen weitere Hinweise hinzukommen, die über eine bloße Kenntnisnahme hinausgehen. Die Datenschutzaufsichtsbehörde ist in jedem Fall unverzüglich zu informieren. Gegenüber den Betroffenen kann im Einzelfall noch die Beseitigung der Ursache abgewartet werden, sofern durch die Information über den Vorfall ein weiterer Schaden eintreten könnte.

Die Benachrichtigung der Betroffenen muss eine Darlegung der Art der unrechtmäßigen Kenntniserlangung und Empfehlungen für Maßnahmen zur Minderung möglicher nachteiliger Folgen enthalten. Die Benachrichtigung der zuständigen Aufsichtsbehörde muss zusätzlich eine Darlegung möglicher nachteiliger Folgen der unrechtmäßigen Kenntniserlangung und der daraufhin ergriffenen Maßnahmen umfassen. Die Unterlassung der Informationspflicht ist nach § 42 Abs. 2 Nr. 7 BDSG bußgeldbewehrt.

6. Durchsuchung und Beschlagnahme

Mit der Stellung des Steuerberaters und dem gesetzlichen Schutz des Vertrauensverhältnisses zu seinen Mandanten ist es nicht vereinbar, dass der Steuerberater zum „Beweisbe-

schaffer“ im Ermittlungsverfahren wird. Daher ist der Steuerberater verpflichtet, sich sowohl auf das Zeugnisverweigerungsrecht nach § 53 Abs. 1 Nr. 3 StPO als auch auf die Beschlagnahmefreiheit aus § 97 Abs. 1 StPO zu berufen.

Auch die Mitarbeiter müssen entsprechend aufgeklärt werden. Des Weiteren sind bei der Anlegung von Akten und Datenbeständen zwischen beschlagnahmefreien und –fähigen Unterlagen, Daten und Handakten zu unterscheiden und diese – deutlich gekennzeichnet – getrennt aufzubewahren bzw. (ggf. verschlüsselt) abzuspeichern. Näheres zum richtigen Verhalten im Falle von Durchsuchung und Beschlagnahme enthalten die „Hinweise der Bundessteuerberaterkammer zur Durchsuchung und Beschlagnahme von Unterlagen beim Steuerberater“, Berufsrechtliches Handbuch, Berufsfachlicher Teil, Abschnitt 5.2.6, der sowohl die Befugnisse der Strafverfolgungsbehörden und die Rechtsstellung des Beraters erläutert als auch praktische Hinweise für das Verhalten vor, während und nach der Maßnahme gibt.

II. Anhang:

Anlage 1: Glossar mit Anwendungshinweisen

Die Autoren haben sich bemüht, nachfolgend die Schlagworte zusammenzutragen und zu erläutern, die im Zusammenhang mit dem Datenschutz und der Datensicherheit in Steuerberaterpraxen ggf. klärungsbedürftig sind. Die Begriffssammlung erhebt keinen Anspruch auf Vollständigkeit. Anregungen in Bezug auf weiter aufzunehmende Begriffe werden unter berufsrecht@bstbk.de gern entgegen genommen. Gerade der IT-Bereich unterliegt einer ständigen Weiterentwicklung, weshalb nicht ausgeschlossen werden kann, dass bestimmte Ausführungen kurzfristig überholt sind. Hierfür wird um Verständnis gebeten.

Begriff	**Erläuterung**
Administration/ Administrator	Der Administrator betreut Computersysteme und -netzwerke. Er ist Inhaber umfassender Nutzungsrechte, plant, installiert, konfiguriert und pflegt die IT-Infrastruktur einer Praxis bzw. eines Unternehmens. Hierzu gehören neben Servern und Arbeitsplatzrechnern auch die zugrunde liegenden Speichersysteme, Netzwerke und Telekommunikationssysteme. In Betracht kommt nur eine Person, der absolute Vertraulichkeit entgegengebracht werden kann und die über die erforderlichen Sachkenntnisse verfügt. Der Datenschutzbeauftragte und der Administrator sind grundsätzlich personenverschieden.
Akkreditierter Zertifizierungsdiensteanbieter	Zertifizierungsdiensteanbieter können bei der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (BNetzA) einen Antrag auf Akkreditierung stellen. Die Akkreditierung ist ein Gütezeichen, das die BNetzA dem Zertifizierungsdiensteanbieter ausstellt, wenn eine umfassende Prüfung der verwendeten technischen Komponenten und des Sicher-

	heitskonzepts zu einem positiven Ergebnis geführt hat. Die auf einem qualifizierten Zertifikat beruhende qualifizierte elektronische Signatur, ausgestellt durch einen Zertifizierungsdiensteanbieter mit Anbieterakkreditierung, wird auch qualifizierte elektronische Signatur mit Anbieterakkreditierung genannt und entspricht der höchsten Sicherheitsstufe bei den elektronischen Signaturen.
Akte	Akte im Sinne des BDSG ist jede sonstige, amtlichen oder dienstlichen Zwecken dienende Unterlage, die nicht unter den Dateibegriff des § 46 Abs. 1 BDSG fällt. Dazu zählen auch Bild- und Tonträger, nicht aber Vorentwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen (§ 46 Abs. 2 BDSG).
Aktive bzw. ausführbare Inhalte/ Programme	Da die Möglichkeiten, mit normalen HTML-Seiten ein dynamisches und benutzerorientiertes Internetangebot zu schaffen, begrenzt sind, werden Internetangebote zunehmend von ausführbaren Programmcodes unterstützt, die eine nahezu unbegrenzte Funktionsvielfalt bieten. Derartige Internetangebote sind ohne das Herunterladen und Ausführen von Programmen auf dem lokalen Rechner gar nicht oder nur mit Einschränkungen nutzbar. Durch aktive bzw. ausführbare Inhalte auf Web-Seiten (z. B. Java, ActiveX) kommen Programme auf dem Rechner des Benutzers zur Ausführung, von denen dieser nicht unbedingt vorher weiß, was sie tun. Häufig ist beim Anklicken eines Links nicht klar ersichtlich, dass damit ein Programm gestartet wird. Durch aktive Inhalte können im eigenen DV-System Daten zerstört, übermittelt oder verändert werden. So können z. B. vertrauliche Daten des Steuerberaters ausgespäht und über bestehende Internetverbindungen direkt übertragen oder bei nicht bestehender Internetverbindung an einem geheimen Ort gespeichert und zu einem späteren Zeitpunkt übermittelt werden. Datenveränderungen durch ausführbare Inhalte können z. B. in der Infektion von Programmen mit einem Computervirus oder in der Veränderung von Datenbankeinträgen bestehen. Auch kann der Rechner des Steuerberaters zu Angriffen auf weitere Rechner genutzt werden.
Aktenvernichtung	⇒ Datenlöschung, ⇒ Schredder
Anhänge	⇒ E-Mail-Attachments
Anonymisieren	Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können (§ 3 Abs. 6 BDSG).
Arbeitsspeicher	Der Arbeitsspeicher oder Hauptspeicher ist in der Informationstechnik der Speicher eines Computers, in dem Datenobjekte, also Programme und die von diesen in Mikroprozessoren zu verarbeitenden Nutzdaten, abgelegt und zu einem späteren Zeitpunkt (unverändert) abgerufen werden können, solange der Computer angeschaltet ist. Die Informationspsychologie verwendet den Ausdruck „Arbeitsspeicher“ als ein Synonym für den menschlichen „Kurzspeicher“ oder „Kurzzeitspeicher“.
Archiv	Die Archivierung von Daten und Unterlagen ist von der reinen Aufbewahrung zu unterscheiden. Aufbewahrung (⇒ Aufbewahrungspflicht) bedeutet im weitesten Sinne die Speicherung auf einem Medium (Plattenspeicher, Magnetband etc.) bzw. in einem System (Dokumentenverwaltungssystem), wobei das Originaldokument stets im Vordergrund steht. Die Archivierung hingegen ist an weitere Regeln gebunden wie Unveränderbarkeit, langfristige Wiederauffindbarkeit und Wiedergabefähigkeit. Die Lebensdauer der Information im Fall der Archivierung ist nicht konstant oder unendlich. Die Aufbewahrungsfrist (Retention time) ist zum Archivierungszeitpunkt festzulegen bzw. ist durch gesetzliche Regelungen vorgegeben. Sie beinhaltet eine mögliche

	bzw. notwendige Vernichtung der Information zur gegebenen Zeit.
ASP (neuere Bezeichnung ist SaaS für Software as a Service)	Der Application Service Provider (deutsch: „Anwendungsdienstleister“) ist ein Dienstleister, der eine Anwendung zum Informationsaustausch über ein öffentliches (z. B. Internet) oder ein privates Datennetz anbietet. ASP-Leistungen sind ein Teil von ⇒ Cloud Computing. Der ASP kümmert sich um die gesamte Administration, wie Datensicherung, das Einspielen von Patches usw. Teil der ASP-Dienstleistung ist regelmäßig auch ein Service (z. B. Benutzerbetreuung) rund um die Anwendung. Dabei wird die benötigte Software nicht gekauft, sondern im Bedarfsfall über das Datennetz für die Nutzung angemietet. Mit Hilfe von ASP-Dienstleistungen können ganze Verwaltungsbereiche oder Prozessschritte ausgelagert werden. Aus der Pflicht zur gewissenhaften Berufsausübung folgt, dass der ASP-Dienstleister sorgfältig auszuwählen ist und sichergestellt werden muss, dass dieser die Anforderungen an die Datensicherheit und die Einhaltung der beruflichen Verschwiegenheitspflicht erfüllt. Hierzu gehört auch, dass er durch den Steuerberater vertraglich zur Verschwiegenheit verpflichtet wird. Darüber hinaus ist eine Vereinbarung zur Auftragsdatenverarbeitung gemäß § 11 BDSG zu schließen. Die betroffenen Verkehrskreise müssen heutzutage davon ausgehen, dass Dienstleister, auch solche, die einer besonderen Verschwiegenheitspflicht unterliegen, ASP-Dienste nutzen, sodass eine entsprechende Unterrichtung der Mandanten entbehrlich ist.
Attributzertifikat	Ein qualifiziertes Zertifikat kann auf Verlangen des Antragstellers Angaben über seine Vertretungsmacht für eine dritte Person, z. B. Geschäftsführer der Steuerberatungsgesellschaft XY, sowie berufsbezogene, z. B. Steuerberater, oder sonstige Angaben zu seiner Person enthalten (§ 5 Abs. 2 S. 1 SigG). Diese zusätzlichen Angaben (Attributzertifikat) werden bei geschäftlichen Vorgängen mit gesendet. Bei privater Nutzung kann das Attributzertifikat unterdrückt werden. Voraussetzung für die Aufnahme der o. g. Attribute in das Zertifikat ist, dass diese Angaben von der zuständigen Stelle gegenüber dem Zertifizierungsdiensteanbieter bestätigt werden.
Aufbewahrungspflicht	Unter der Aufbewahrungspflicht wird die Pflicht verstanden, Daten und Belege über bestimmte Zeiträume aufzubewahren. Vorschriften zur Aufbewahrung sind insbesondere in § 257 HGB, § 147 AO, § 66 StBerG und § 14 b UStG enthalten. Der DWS-Verlag gibt das Merkblatt „Aufbewahrungsfristen sowie Recht auf Datenzugriff“ heraus. Bestimmte Belege, z. B. Bilanzen, vollstreckbare Urkunden, müssen in Papierform aufbewahrt werden. Originär elektronisch entstandene Daten und Dokumente müssen aus steuerlichen Gründen in auswertbarer elektronischer Form vorgehalten werden (§ 147 Abs. 6 AO).
Aufsichtsbehörden für den Datenschutz	Aufsichtsbehörden für den Datenschutz sind staatliche Aufsichts- und Ordnungsbehörden, die die Beachtung datenschutzrechtlicher Regelungen überwachen. Für Berufsträger sind in der Regel die „Aufsichtsbehörden für den nicht-öffentlichen Bereich“ (Landesbeauftragte für den Datenschutz) zuständig.
Auftragsdatenverarbeitung	⇒ Grundsätzliche Bemerkungen (Ziffer 4.)
Auskunft/ Auskunftsrecht	⇒ Betroffener
Auskunftsverhalten	Grundsätzlich hat nur der Mandant einen Auskunftsanspruch gegen seinen Steuerberater. Für eine umfassendere Auskunftsberechtigung gegenüber Dritten, z. B. Auskunft an Familienmitglieder, bedarf es der vorherigen Entbindung des Steuerberaters von der Verschwiegenheitspflicht.

Authentifizierung/Authentisierung	Authentifizierung ist der Vorgang der Überprüfung einer behaupteten Identität, beispielsweise einer Person oder eines Objekts. Authentisierung dagegen ist der Vorgang des Nachweises der eigenen Identität. Die Authentifizierung von Objekten, Dokumenten oder Daten meint die Feststellung, dass diese authentisch sind – es sich somit um ein unverändertes, nicht kopiertes Original handelt. Eine überprüfte Identität, also nach der erfolgreichen Authentifizierung, wird Authentizität genannt. In Computer-Netzwerken wie dem Internet wird Authentifizierung eingesetzt, um die Authentizität von Informationen sicherzustellen.
Automatisierte Verarbeitung	⇒ Datenverarbeitung, automatisierte
Automatisiertes Abrufverfahren	Automatisierte Abrufverfahren ermöglichen die Übermittlung personenbezogener Daten durch Abruf (§ 3 Abs. 2 BDSG). Die Einrichtung eines automatisierten Verfahrens zur Übermittlung personenbezogener Daten durch Abruf ist zulässig, soweit es unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen und der Aufgaben oder Geschäftszwecke der beteiligten Stellen angemessen ist (§ 10 Abs. 1 BDSG).
Backup	Unter Backup versteht man das teilweise oder gesamte Kopieren der in einem Computersystem vorhandenen Daten auf ein anderes Speichermedium, um einen Datenverlust bei Systemausfällen zu begrenzen. Zur wiederherstellbaren, vollständigen Datensicherung ist die Fixierung aller Werte bzw. Daten notwendig. Die auf dem Speichermedium gesicherten Daten werden als Sicherungskopie, oft auch als Backup bezeichnet. Es empfiehlt sich, eine turnusmäßige, in der Regel tägliche Sicherung durchzuführen. Zudem sollte mindestens ein wöchentliches Backup an einem anderen sicheren Ort außerhalb des Gebäudes aufbewahrt werden. Gleichzeitig ist organisatorisch sicherzustellen, dass die Datenwiederherstellung nur beim berechtigten Dateninhaber erfolgt und möglich ist.
Benutzerkennung	Die Benutzerkennung dient der Identifikation eines Anwenders (Login) und besteht in der Regel aus Buchstaben, Zahlen, Sonderzeichen oder biometrischen Merkmalen. Eine komplexe Zusammensetzung der Benutzerkennung aus verschiedenen Zahlen und Zeichen erhöht in Verbindung mit einem sicheren Passwort die Systemsicherheit.
Berufsgeheimnis	Unter dem Berufsgeheimnis wird die Verpflichtung bestimmter Berufsgruppen verstanden, Daten und Informationen, von denen sie im Rahmen ihrer beruflichen Tätigkeit Kenntnis erlangen, nicht an Dritte weiterzugeben. Die berufliche Schweigepflicht, der neben Steuerberatern z. B. auch Ärzte, Rechtsanwälte, Apotheker und Psychologen unterliegen, ist auch von den Mitarbeitern zu beachten. Die Missachtung des Berufsgeheimnisses stellt eine Straftat gemäß § 203 StGB dar. (⇒Vorbemerkungen - Verschwiegenheit und Datenschutz - Wesensmerkmale des freien Berufs Steuerberater)
Betrieblicher Datenschutzbeauftragter	Der betriebliche Datenschutzbeauftragte ist ein Organ der innerbetrieblichen Selbstkontrolle. Er hat die Einhaltung der Bestimmungen zum Datenschutz im Unternehmen sicherzustellen (⇒ Vorbemerkungen – Bestellung eines Datenschutzbeauftragten).Die Voraussetzungen für seine Bestellung und die Aufgaben sind in § 4f und § 4g BDSG geregelt.
Betroffener	Betroffener i. S. d. Datenschutzes ist jede bestimmte oder bestimmbare natürliche Person, über die Daten bei öffentlichen oder nicht-öffentlichen Stellen gespeichert sind (§ 3 Absatz 1 BDSG). Betroffene haben nach § 34 BDSG ein Recht auf Auskunft, ob und welche personenbezogenen Daten über sie gespeichert sind, aus welchen Quellen diese Daten stammen und zu welchem Verwendungszweck sie gespeichert werden. Hinsichtlich falscher Daten besteht ein Berichtigungsanspruch. Die Rechte auf Auskunft und Berichtigung können jedoch verweigert werden, wenn das allgemeine öffentliche Interesse, das Interesse der jeweiligen nicht-öffentlichen Stelle an

	der Wahrung des Geschäftsgeheimnisses oder das Interesse Dritter zur Geheimhaltung überwiegt. Betroffene können die Übermittlung ihrer persönlichen Daten an Dritte untersagen. Weiterhin besteht ein Anspruch auf Sperrung bzw. Löschung der Daten. Schließlich haben Betroffene ein Beschwerderecht bei der zuständigen Aufsichtsbehörde für den Datenschutz (⇒ Aufsichtsbehörden für den Datenschutz).
Bildschirmschoner	Bildschirmschoner werden zum Schutz des Bildschirms sowie aus Gründen des Datenschutzes verwendet. Mit ihrer Hilfe kann verhindert werden, dass Unbefugte Einblick in zu schützende Daten erhalten. Dazu ist der Bildschirmschoner mit einer Passworteingabe bei Reaktivierung der Arbeitsoberfläche einzurichten. Dem Sicherheitsgedanken wird ebenso Rechnung getragen, wenn eingestellt wird, dass der Bildschirm – wiederum passwortgeschützt – in der inaktiven Phase schwarz geschaltet wird oder in einen Stromsparmodus wechselt.
Browsereinstellungen	Im Internet-Browser können verschiedene Sicherheitsstufen eingestellt werden. Grundsätzlich sollte eine möglichst hohe Sicherheitsstufe gewählt werden. So kann z. B. durch die Deaktivierung von aktiven Inhalten (ActiveX, Java, Java-Script) und Skript-Sprachen (z. B. Visual Basic Script, VBS) die Ausführung von aktiven Inhalten verhindert werden. Wird der Browser auf die höchste Sicherheitsstufe eingestellt, ist jedoch eine uneingeschränkte Internetnutzung nicht mehr möglich: Bei der Deaktivierung von JavaScript können z. B. verschiedene Websites nicht bzw. nicht vollständig angezeigt werden; so wird z. B. das Home-Banking nicht mehr unterstützt. Aufgrund der Funktionseinschränkungen empfiehlt sich die Installation einer ⇒ Firewall sowie der Einsatz eines aktuellen Virenschutzprogramms anstelle der Einstellung des Browsers auf die höchste Sicherheitsstufe. Zusätzlich kann auch angedacht werden, beim Internet-Browser grundsätzlich die höchste Sicherheitsstufe einzustellen, aber die Rechner einiger, für die Gefahren des Internets besonders sensibilisierter Mitarbeiter hiervon auszunehmen. <u>Checkliste für einige wichtige Browsereinstellungen:</u> · Hohe Sicherheitsstufe auswählen · „Proxyserver verwenden“ kann eingestellt werden · „Proxyserver für lokale Adressen umgehen“ einstellen · ActiveX-Steuerelemente wegen der hohen Sicherheitsrisiken deaktivieren bzw. nur nach Eingabeaufforderung ausführen · Scripting deaktivieren bzw. für einzelne, für die Gefahren von ausführbaren Inhalten sensibilisierte Mitarbeiter aktivieren · Für den Aufruf von externen Programmen zur Darstellung von Dateien „Eingabeaufforderung“ einstellen · Automatisches Starten von herunter geladenen Programmen abstellen · Warnmeldungen wie z. B. „Bei ungültigen Zertifikaten warnen“, „Bei Wechsel zwischen sicherem und nicht sicherem Modus warnen“, „Warnen falls Formulardaten umgelenkt werden“ aktivieren
Bundesbeauftragter für den Datenschutz	Der Bundesbeauftragte für den Datenschutz überprüft als Aufsicht die Ausführungen der datenschutzrechtlichen Regelungen im öffentlichen Bereich, vornehmlich der Bundesbehörden. Er wird auf Vorschlag der Bundesregierung vom Deutschen Bundestag für eine Amtszeit von fünf Jahren gewählt. Er ist fachlich unabhängig und nur dem Gesetz unterworfen. Die Dienststelle ist beim Innenministerium angesiedelt. Neben der Aufsichtsfunktion trägt er zur Sicherung und Weiterentwicklung des Datenschutzes sowie der Informationsfreiheit auf nationaler und europäischer Ebene bei. Der Bundesbeauftragte für Datenschutz ist Ansprechpartner und kann kontaktiert werden, wenn öffentliche und nicht öffentliche Stellen Persönlichkeitsrechte im Da-

	tenschutz nicht beachten.
Bundesdatenschutzgesetz (BDSG)	Das Bundesdatenschutzgesetz soll den Einzelnen davor schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird (§ 1 Abs. 1 BDSG; ⇒ Datenschutzrecht).
Bit	Ein Bit ist eine Maßeinheit für Datenmenge. Dabei bezeichnet 1 Bit die kleinste darstellbare Datenmenge die beispielsweise durch eine Binärziffer dargestellt werden kann. Moderne Computer und Speichermedien verfügen über Speicherkapazitäten von Milliarden von Bits. Speichergrößen werden daher in anderen Einheiten angegeben. Vielfache von Bit sind z. B. Kilobit (10^3 bit), Megabit (10^6 bit) oder Gigabit (10^9 bit).
Cloud Computing	Beim Cloud Computing werden Daten und Anwendungen nicht mehr auf lokalen Rechnern gespeichert, sondern ausgelagert und über ein fremdes Netzwerk zur Verfügung gestellt. Dabei können nicht nur die Anwendungen, sondern auch die daraus erzeugten Daten in einem externen Rechenzentrum gespeichert und verarbeitet werden. Cloud Computing ermöglicht eine flexible und ortsungebundene Nutzung von IT-Leistungen, die - im Vergleich zu Inhouselösungen - mit Kostenersparnissen verbunden sein kann. In jedem Fall ist dabei die Einhaltung deutscher Steuer-, Datenschutz- und Berufsrechtsbestimmungen zu gewährleisten. Zudem muss hinsichtlich bestimmter Daten jederzeit nachgewiesen werden können, wo sich diese befinden und wer sie einsehen kann. In der Regel ist Cloud Computing auch ⇒ Auftragsdatenverarbeitung, wenn personenbezogene Daten betroffen sind. Weitere Informationen zur Thematik z. B. auf www.bitkom.org.
Chiffrat	Ein Chiffrat (auch Kryptogramm, Kryptotext oder Schlüsseltext) ist eine verschlüsselte Nachricht. Ohne den zur Entschlüsselung notwendigen Schlüssel können aus dem Chiffrat keine Informationen gewonnen, also kein Klartext erstellt werden.
Cookie	Als Cookie bezeichnet man einen kurzen Eintrag in einer meist kleinen Datenbank bzw. in einem speziellen Dateiverzeichnis auf einem Computer, der dem Austausch von Informationen zwischen Computerprogrammen oder der zeitlich beschränkten Archivierung von Informationen dient. Ein Cookie besteht aus mindestens zwei Bestandteilen, seinem Namen und dem Inhalt oder Wert des Cookies. Zusätzlich können Angaben über den zweckmäßigen Gebrauch vorhanden sein. Die Datenbank kann oft vom Benutzer des Computers ohne besondere Hilfsmittel nicht eingesehen oder verändert werden. Viele Webseiten hinterlegen ein solches Cookie, um die Nutzer beim erneuten Einloggen wiedererkennen zu können (und z. B. dann andere Werbung einzublenden). Ein häufiges Beispiel für notwendige Cookies sind Foren. Dort findet sich oft die Möglichkeit, „eingeloggt zu bleiben“. Dabei wird ein Cookie abgelegt, das bei erneutem Besuch der Seite ausgelesen und ausgewertet wird. Auch Shops basieren häufig auf Cookies, die den Warenkorb steuern. Die meisten Browser (⇒ Browsereinstellungen) erlauben Einschränkungen für das Ablegen von Cookies auf der Festplatte. Trotz der damit verbundenen Einschränkungen in der Benutzerfreundlichkeit sollten Cookies und andere temporäre Internetdateien in regelmäßigen Abständen gelöscht werden.
Datei	Aus technischer Sicht betrachtet enthält eine Datei Daten in strukturierter Form. Gleichartige Daten werden zu jeweils einer Datei, z. B. Textdatei, Programmdatei, Zeichnungsdatei oder zu einer Datenbankdatei wie Materialdatei, Preisdatei, Kreditorendatei, Debitorendatei zusammengefasst. Sie können auf beliebigen Speichermedien abgelegt bzw. gespeichert werden. In der EDV ist die Datei eine Aneinanderreihung von ⇒ Bits. Erst ein Anwendungsprogramm oder das Betriebssystem interpretieren die Datei als Text, Programm oder Bild.

	Rechtlich versteht man unter einer Datei eine Sammlung personenbezogener Daten, die durch automatisierte Verfahren nach bestimmten Merkmalen ausgewertet werden kann (vgl. § 3 Abs. 2 BDSG, ⇒ automatisierte Verarbeitung), oder eine sonstige Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen geordnet, umgeordnet und ausgewertet werden kann. Ausdrücklich hiervon ausgeschlossen sind Akten und Aktensammlungen, es sei denn, dass sie durch automatisierte Verfahren umgeordnet und ausgewertet werden können.
Datenfernübertragung (DFÜ)	Als DFÜ bezeichnet man die Übermittlung von Daten zwischen Computern über ein Medium, bei der ein zusätzliches Protokoll verwendet wird. Am weitesten verbreitet ist DFÜ über Festnetz. Üblich sind auch andere Übertragungsmedien wie Funk (GPRS, UMTS, Bluetooth, WLAN ...). In Bezug auf notwendige Sicherheitsmaßnahmen wird auf die Ausführungen in den Vorbemerkungen („Verschwiegenheit und Datenschutz - Wesensmerkmale des freien Berufs Steuerberater“) verwiesen.
Datengeheimnis	Das Datengeheimnis untersagt es den bei der Datenverarbeitung Beschäftigten, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Es besteht auch nach Beendigung der Beschäftigung weiter (§ 5 BDSG). ⇒ auch Berufsgeheimnis
Datenklassifikation	Als Datenklassifikation bezeichnet man die Einteilung aller Daten und Informationen eines Unternehmens in Vertraulichkeitsklassen. Für den Umgang mit den Daten verschiedener Vertraulichkeitsstufen sind intern jeweils spezielle Verhaltensregeln festzulegen.
Datenlöschung	Löschen i. S. d. BDSG bezeichnet das Unkenntlichmachen gespeicherter personenbezogener Daten (§ 3 Abs. 4 Nr. 5 BDSG). Personenbezogene Daten können grundsätzlich jederzeit gelöscht werden (Ausnahmen s. § 35 Abs. 3 Nr. 1 und 2 BDSG). Auch um dem Grundsatz der ⇒ Datensparsamkeit (§ 3 a BDSG) zu entsprechen, empfiehlt es sich, nicht mehr benötigte Daten zu löschen. Dagegen sind Daten zu löschen, wenn ihre Speicherung unzulässig ist, die Richtigkeit sensibler Daten nicht bewiesen werden kann bzw. die Daten nicht mehr benötigt werden (§ 35 Abs. 2 BDSG). Die Datenlöschung ist abzugrenzen von der ⇒ Datensperre Generelle Hinweise zur (unwiederbringlichen) Löschung von Daten · Sicheres Löschen erfordert technisch-organisatorische Maßnahmen in allen Phasen der Verarbeitung, insbesondere bei Veräußerung, Vermietung, Aussonderung, Rückgabe, Reparatur und Wartung von Datenträgern. · Die Maßnahmen sind durch konkrete Handlungsanweisungen zu bestimmen, welche den Schutzbedarf der zu löschenden Daten ebenso berücksichtigen wie den Aufwand und die Kosten für eine mögliche Datenwiederherstellung. · Das einmalige, komplette Überschreiben mit Zufallszahlen sollte beim Löschen von Daten jeder Art praktiziert werden. Mehrmaliges Überschreiben ist beim Löschen personenbezogener Daten mittlerer und höherer Schutzstufen erforderlich. Hierbei können spezielle Softwarewerkzeuge zum Einsatz kommen.

	▪ Soll ein noch intakter Datenträger verkauft, vermietet, ausgesondert, zurückgegeben oder einer neuen Nutzung zugeführt werden, ist zuvor der gesamte Datenträger zu löschen. ▪ Das selektive Löschen einzelner Dateien durch Überschreiben ist nur dann geeignet, wenn sichergestellt ist, dass keine Kopien der in diesen Dateien enthaltenen Daten an anderen Orten abgelegt wurden. ▪ Das Löschen durch Überschreiben ist durch geeignete und geprüfte Softwarewerkzeuge vorzunehmen und stichprobenartig zu kontrollieren. ▪ Defekte Datenträger, deren Daten nicht mehr mit Softwarewerkzeugen überschrieben werden können, sind durch mechanische oder thermische Zerstörung (Disketten, CD, DVD, Festplatten) bzw. durch magnetische Durchflutung (Disketten) unbrauchbar zu machen. ▪ Müssen Datenträger ohne vorheriges Löschen der Daten aus der Hand gegeben werden (z. B. Reparatur, Rückgabe an den Hersteller in der Garantiezeit), ist in Abhängigkeit von der Sensibilität der Daten durch vertragliche Regelungen zu verhindern, dass unerwünschte Informationsflüsse stattfinden oder von Angreifern ausgenutzt werden können. Ggf. sind Schadensersatzansprüche zu vereinbaren oder es ist auf Garantieansprüche zu verzichten. ▪ Es ist zu beachten, dass sich in vielen Geräten Datenträger befinden. Somit ist nicht nur bei Personal Computern sondern auch bei Kopierern, Druckern, Faxgeräten, Handys usw. auf die richtige Löschung von Daten zu achten. ▪ Zu den Anforderungen an eine Datenträgervernichtung wird auf DIN 66399 verwiesen. ⇒ Schredder Der Begriff des Unkenntlichmachens verlangt, dass irreversibel bewirkt wird, dass eine Information nicht länger aus den gespeicherten Daten gewonnen werden kann. Unter Umständen sind hierfür mechanische, thermische, chemische oder sonstige Methoden erforderlich. <u>Löschung von Daten auf CDs bzw. DVDs</u> Neuere Aktenvernichter können neben Papier auch Kreditkarten und CDs bzw. DVDs schreddern. Dabei ist zu bedenken, dass auf einem Quadratmillimeter einer zerstörten CD noch bis zu 12 DIN A4-Seiten Informationen sichtbar gemacht werden können, auf einem Quadratmillimeter einer zerstörten DVD sind es sogar noch bis zu 80 DIN A4-Seiten. Aus diesem Grund können CDs/DVDs auch nur bedingt durch Zerkratzen gegen unbefugtes Lesen geschützt werden. Deshalb, aber auch aus Gründen des Umweltschutzes, sollten CDs/DVDs datenschutzgerecht recycelt werden. Dabei werden nicht nur die Daten zuverlässig vernichtet, sondern es entsteht auch ein hochwertiger Wertstoff für die Medizintechnik, Automobil- und Computerindustrie. <u>Löschung von Daten auf USB-Sticks, Speicherkarten und Festplatten</u>

	Die Annahme, das Löschen der Daten auf einem mobilen Speichermedium oder Festplatten sei endgültig, und Daten nicht mehr lesbar, wenn sie auf dem Speichermedium gelöscht wurden, ist falsch. Einfach gelöschte Daten sind in der Regel wieder herstellbar, weil dabei lediglich die Einträge im Dateiverzeichnis entfernt werden und selbst dies nicht vollständig geschieht. Auch zur Löschung von Festplatten ist ein bloßer Druck auf die Löschtaste oder ein einfacher Löschbefehl im Explorer nicht ausreichend. Wenn ein Computer mit einer Festplatte den Besitzer wechselt, ist es diesem in vielen Fällen ohne Weiteres möglich, den vermeintlich gelöschten früheren Inhalt zu rekonstruieren. Auch bei vielen Löschprogrammen werden die Dateninhalte nicht tatsächlich gelöscht, sondern es wird nur die Verknüpfung im „Inhaltsverzeichnis“ auf dem Datenträger (Festplatte, Disketten, Speicherkarten, USB-Stick etc.) gelöscht. Da die Daten weiterhin vorhanden sind, können sie beim Verkauf, bei einer Reparatur oder bei der Aussonderung des Geräts von Unbefugten ausgelesen werden. Dies bedeutet, dass Software-Lösungen ggf. nicht ausreichen, um die Daten endgültig zu löschen. Für die sichere Datenvernichtung empfehlen sich daher Hardware-Lösungen. Insoweit kommt die Datenträgervernichtung durch Entmagnetisieren, Ausglühen oder Schreddern in entsprechend gesicherten Vernichtungsanlagen bei einer zertifizierten Recycling-Firma in Betracht. Beim professionellen Löschen mit einem Entmagnetisierer (Degausser) wird der Datenträger mehreren Magnetfeldern von sich ändernder Polarität und allmählich abnehmender Stärke ausgesetzt. Allerdings gibt es selbst bei diesem gründlichen Verfahren immer noch die Gefahr von Restmagnetisierungen und damit der Datenrückgewinnung. Das „Ausglühen“ der Datenträger in einer Verbrennungsanlage ist eine sichere Löschmöglichkeit. Beim Ausglühen verliert die Kobalt-Nickel-Legierung, deren Schmelzpunkt bei 700°C liegt, ihre magnetischen Eigenschaften. Damit sind die Daten irreversibel gelöscht. Beim „Schreddern“ werden die Datenträger mechanisch zermalen. Dann ist eine Reproduktion der Daten nur unter erheblichen Aufwand möglich. Nach dem Verbrennen des Schredderguts ist der Datenträger endgültig gelöscht. Der ⇒ Bundesbeauftragte für den Datenschutz empfiehlt die Vernichtung von sensiblen Datenträgern unter Aufsicht des Auftraggebers durchführen zu lassen, was bei verschiedenen Recycling-Firmen angeboten werden soll. Außerdem würden bei einer professionellen Datenträgervernichtung in einem Zertifikat Typ, Hersteller, Modell und Seriennummer bei der endgültigen Vernichtung des Datenträgers dokumentiert.
Datennutzung	Datennutzung bezeichnet jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt (§ 3 Abs. 5 BDSG). Typische Fälle des Nutzens sind das Abrufen, Auswerten oder Zusammensortieren vorhandener Daten.
Datenpanne	Wird umgangssprachlich als Bezeichnung eines Vorfalls verwendet, der eine Informationspflicht nach § 42a BDSG zur Folge hat. ⇒ Grundsätzliche Bemerkungen (Ziffer 5.)
Datenschutz	Datenschutz dient dem grundgesetzlich gewährleisteten Schutz vor einer Beeinträchtigung des Persönlichkeitsrechts gemäß Art. 2 Abs. 1 GG (§ 1 Abs. 1 BDSG), aus dem sich auch das Grundrecht auf informationelle Selbstbestimmung ergibt. Danach kann grundsätzlich jeder selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten bestimmen. Einschränkungen sind nur aufgrund von Gesetzen zulässig. Zu den Geset-

	zen, die das Persönlichkeitsrecht beim Umgang mit personenbezogenen Daten schützen sollen, gehört insbesondere das ⇒ Bundesdatenschutzgesetz. ⇒ auch Datenschutzrecht
Datenschutz-audit	Zur Verbesserung des Datenschutzes und der Datensicherheit können Steuerberater ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen (vgl. § 9 a BDSG).
Datenschutzbeauftragter (DSB)	⇒ betrieblicher Datenschutzbeauftragter; ⇒ Vorbemerkungen; ⇒ §§ 4 f und 4 g BDSG; ⇒ Bundesbeauftragter für den Datenschutz; ⇒ Landesbeauftragter für den Datenschutz
Datenschutzrecht	Auf Bundesebene regelt das ⇒ Bundesdatenschutzgesetz den Datenschutz für alle öffentlichen Stellen des Bundes und der Länder sowie für alle nichtöffentlichen Stellen, die Datenverarbeitungsanlagen nutzen. Hierzu gehören auch Steuerberaterpraxen. Daneben regeln die Landesdatenschutzgesetze der Bundesländer den Datenschutz in Landes- und Kommunalbehörden. Der Datenschutz ist nach der Rechtsprechung des Bundesverfassungsgerichts ein Grundrecht (Recht auf informationelle Selbstbestimmung). Hieraus folgt, dass der ⇒ Betroffene grundsätzlich selbst darüber entscheiden kann, wem er welche persönlichen Informationen offenbart.
Datensicherheit	Datensicherheit umfasst, im Gegensatz zum Datenschutz, begrifflich alle Maßnahmen, die notwendig sind, um die Datenverarbeitung selbst (z. B. Daten, Programme, Datenverarbeitungsgeräte, Daten- und Kommunikationsnetze sowie DV-Prozesse und -Verfahren) und die sonstige Nutzung zur Gewährleistung der Datenschutzvorschriften vor unbefugtem Zutritt, Zugang und Zugriff, vor unbefugter Weitergabe, Veränderung und Verarbeitung sowie bei Missbrauch, Diebstahl, Fehlern und Störungen jeder Art in angemessener Weise zu sichern; sie bezeichnet eine technisch-organisatorische Aufgabe.
Datensicherung	Im weiteren Sinne bezeichnet die Datensicherung die Summe der technischen, organisatorischen und personellen Maßnahmen, um die Datensicherheit zu gewährleisten. Im engeren Sinne kann die Datensicherung (auch Bestandssicherung genannt) mit einem ⇒ Backup gleichgesetzt werden.
Datenspeicherung	⇒ Datenträger
Datensperre	Sperren ist - wie auch das Speichern, Verändern, Übermitteln und Löschen personenbezogener Daten - eine Form der Datenverarbeitung i. S. d. ⇒ Bundesdatenschutzgesetzes und bezeichnet das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken (§ 3 Abs. 4 Nr. 4 BDSG). Eine Sperrung personenbezogener Daten ist gemäß § 35 Abs. 3, 4 BDSG vorzunehmen, wenn ▪ einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen, ▪ Grund zur Annahme besteht, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden, ▪ eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist, bzw. ▪ die Richtigkeit personenbezogener Daten, die automatisiert verarbeitet oder in nicht automatisierten Dateien gespeichert sind, vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt.
Datenträger	Datenträger sind insbesondere Bänder, Disketten, CDs und DVDs, USB-

	Sticks, Speicherkarten und Festplatten. Auch in anderen Geräten wie Netzwerkdruckern, Digicams, Faxgeräten, Diktiergeräten, Mobiltelefonen und Kopierern befinden sich Datenträger, woran im Fall der Weitergabe an Dritte zu denken ist, um dem Datenschutz Rechnung zu tragen. ⇒ Datenlöschung
Datenverarbeitung, automatisierte	Automatisierte Datenverarbeitung ist die Erhebung, Verarbeitung oder Nutzung => personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen. Erheben ist das Beschaffen von Daten über den Betroffenen. Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten (§ 3 Abs. 4 BDSG).
Datenvermeidung und Datensparsamkeit	Datenvermeidung und Datensparsamkeit beschreiben datenschutzrechtliche Grundsätze, nach denen sich die Gestaltung und Auswahl von Datenverarbeitungssystemen an dem Ziel auszurichten haben, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere soll von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch gemacht werden, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht (§ 3 a BDSG). Das Prinzip der Datenvermeidung und Datensparsamkeit steht in engem Zusammenhang mit dem traditionellen datenschutzrechtlichen Grundsatz, dass nur diejenigen personenbezogenen Daten verarbeitet werden dürfen, die für die Erfüllung der jeweiligen Aufgabe benötigt werden. ⇒ auch Zweckbindung der Daten
Direkterhebung	Der Grundsatz der Direkterhebung verlangt, personenbezogene Daten unmittelbar beim Betroffenen zu erheben (§ 4 Abs. 2 Satz 1 BDSG).
Download	Als Download wird das Herunterladen und die Übertragung von Daten von einer Gegenstelle (z. B. Netzrechner, Internet) auf den eigenen Rechner bezeichnet. Herunterladen ist somit das Gegenstück zum Hochladen bzw. „Upload". Fehlende Integrität durch gefälschte oder veränderte bzw. virenbehaftete Software stellt ein Sicherheitsrisiko dar. Die Vertraulichkeit lässt sich unter anderem durch Verschlüsselungsverfahren erreichen. <u>Hinweise für Downloads aus dem Internet</u> 1. Um nicht versehentlich ein Programm mit Schadensfunktion zu starten, sollten Fenster im Internet nie mit einem möglicherweise dort vorhandenen Button „Schließen“ geschlossen werden, da hier ein Programm mit Schadensfunktion hinterlegt sein könnte. Stattdessen sollte das im oberen rechten Eck vorhandene Kreuzchen des Softwareherstellers für das Schließen eines Fensters verwendet werden. 2. Programme sollten nur von vertrauenswürdigen Seiten, z. B. Originalseite des Herstellers, geladen werden. 3. Nach dem Download sollte die Angabe der Größe der Datei und - soweit angegeben - auch der Prüfsumme mit der vorgegebenen Größe und Prüfsumme verglichen werden. Werden dabei Abweichungen festgestellt, kann davon ausgegangen werden, dass unzulässige Veränderungen, meist durch Viren, vorgenommen worden sind. Die Datei sollte daher sofort gelöscht werden. 4. Die herunter geladenen Dateien sollten vor der Installation stets mit einem aktuellen Virenschutzprogramm überprüft werden. 5. Gepackte (komprimierte) Dateien sollten erst entpackt und auf Viren überprüft werden. 6. Installierte Entpackungsprogramme sollten so eingestellt werden, dass die zu entpackenden Dateien nicht automatisch gestartet werden.

Dritter	Dritter ist jede Person oder Stelle außerhalb der verantwortlichen Stelle. Dritte sind nicht der Betroffene sowie Personen und Stellen, die im Inland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen. (§ 3 Abs. 8 S. 2 BDSG).
Electronic Banking	Prinzipiell gibt es fünf Arten von Electronic Banking: ▪ Electronic Banking per Datenträgeraustausch (DTA oder DTAUS) ▪ Onlinebanking (auch E-Banking, Homebanking oder Telebanking) ▪ Telefonbanking ▪ SB-Banking ▪ Kartengestütztes Bezahlen (auch POS). Die einzelnen Varianten sind für bestimmte Zielgruppen entwickelt worden. So wird z. B. der klassische Datenträgeraustausch bevorzugt von größeren Geschäftskunden genutzt, während das in der Nutzung sehr einfache Telefonbanking eher den Privatkunden anspricht. In der Praxis findet jedoch oft eine Vermischung statt. Es ist zwischen der Sicherheit der eigentlichen Datenübertragung zur oder von der Bank und der Abwicklung am Arbeitsplatz zu unterscheiden. Bei allen Browser- oder Client-basierten Electronic Banking-Systemen ist eine Verschlüsselung der Datenübertragung seitens der Banken gewährleistet. Diese ist nur unter erheblichem Zeit- und Ressourcenaufwand – manipulierbar. Erste Angriffsfläche für einen eventuellen Betrüger ist neben dem bedienenden Menschen vor Allem der heimische PC. So sollten Computer immer durch einen aktuellen Virenscanner und eine Firewall gesichert werden, um die Verbreitung von Schadprogrammen wie z. B. Virus Keyloggern und Trojanern zu unterbinden. Mit solchen Schadprogrammen wäre z. B. die Fernsteuerung des Computers möglich. Durch Phishing und Pharming wird versucht, direkt an die zur Auftragsunterzeichnung notwendigen Daten (z. B. PIN/TAN) zu gelangen. Jeder Bankkunde kann sich bereits dadurch schützen, wenn die von den Banken zur Verfügung gestellten Zugangsberechtigungen nicht weitergegeben bzw. im Computer hinterlegt werden. Soweit der Steuerberater Zahlungen für seine Mandanten auf elektronischem Weg erledigt, sind dem Vertrauensverhältnis entsprechend besondere Sicherheitsmechanismen einzurichten. Diese können aus der Einschaltung eines sicheren Serviceproviders oder der Nutzung von E-Bankingprogrammen und der zusätzlich gesicherten Aufbewahrung der Zugangs- und Transaktionscodes bestehen.
Elektronische Signatur	Elektronische Signaturen sind Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen (§ 2 Nr. 1 SigG). Die (einfache) elektronische Signatur gem. § 2 Nr. 1 SigG unterliegt keinen besonderen Regulierungen. Sie kann z. B. mit Hilfe des weit verbreiteten „Pretty Good Privacy“-Verfahrens (PGP) erzeugt werden. Es handelt sich hierbei um eine Software, die der Nutzer im Internet herunterladen und mit deren Hilfe er ein Schlüsselpaar generieren kann. Mit dem privaten, geheim zu haltenden Schlüssel signiert der Nutzer ein Dokument. Den öffentlichen Schlüssel gibt der Nutzer z. B. auf seiner Homepage bekannt oder hängt ihn an eine E-Mail an. Mit Hilfe des öffentlichen Schlüssels kann der Empfänger prüfen, ob die übermittelten Daten vollständig und unverfälscht sind. Nicht festgestellt werden kann jedoch, ob die Signatur von dem angegebenen Absender oder von einer fiktiven Person, die unter dem Namen des Absenders auftritt, stammt. Sofern sich zwei Personen kennen, kann dieses Problem

	ausgeräumt werden, indem sie sich ihre öffentlichen Schlüssel gegenseitig übergeben. Die fortgeschrittene elektronische Signatur (§ 2 Nr. 2 SigG) ist eine elektronische Signatur, die · ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sind, · die Identifizierung des Signaturschlüssel-Inhabers ermöglichen, · mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann, und · mit den Daten, auf die sie sich beziehen, so verknüpft sind, dass eine nachträgliche Veränderung der Daten erkannt werden kann. Die qualifizierte elektronische Signatur (§ 2 Nr. 3 SigG) ist eine fortgeschrittene elektronische Signatur, die · auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen und · mit einer sicheren Signaturerstellungseinheit erzeugt werden.
E-Mail	Eine E-Mail ist eine elektronische, briefartige Nachricht. Die meisten E-Mails werden im Klartext (⇒ Chiffrat) verschickt, können also prinzipiell auf jedem Rechner, den die Nachricht auf ihrem Weg vom Absender zum Empfänger passiert, gelesen werden. Zieht man eine Analogie zur Briefpost, ist eine E-Mail daher eher mit einer Postkarte vergleichbar als mit einem durch einen Umschlag vor neugierigen Blicken geschützten Brief. Ebenfalls ähnlich wie bei einem Brief oder einer Postkarte und genauso einfach lassen sich E-Mails mit einer falschen Absenderadresse verschicken, was zum Beispiel bei Spam oft zu beobachten ist. Empfänger-, Kopie- und Blindkopie-Adressen (mit *TO*, *CC* beziehungsweise *BCC* im E-Mail-Kopf gekennzeichnet) lassen sich gleichermaßen fälschen (Mail-Spoofing). Die Lösung für diese beiden Probleme ist ⇒ Verschlüsselung und Absenderauthentifizierung (⇒ Authentifizierung). Hierzu existieren bspw. die Verfahren Pretty Good Privacy und dessen freie Variante GNU Privacy Guard, sowie S/MIME (vorwiegend im Business-to-Business-Bereich), die jedoch nicht weit verbreitet sind. Selbst solche Verschlüsselungsverfahren decken lediglich den Inhalt der E-Mail ab, nicht die Betreff-Zeile oder das E-Mail-Datum. Dadurch können unter Umständen Rückschlüsse auf den Inhalt einer verschlüsselten Mail gezogen werden. Gemäß BDSG (Anlage zu § 9 Satz 1) sind je nach Art der Daten geeignete Schutzmaßnahmen zu treffen. Dabei wird auf die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren hingewiesen, (=> E-Mail-Verschlüsselung) Der Umgang mit E-Mails könnte z. B. wie folgt geregelt werden: 1. Offensichtlich unsinnige E-Mails bzw. solche von unbekannten Absendern sind ungeöffnet zu löschen. 2. Auch bei E-Mails von vermeintlich bekannten bzw. vertrauenswürdigen Absendern ist stets zu prüfen, ob die Nachricht inhaltlich und sprachlich zum Absender passt (z. B. englischsprachige Nachricht von deutschem Mandanten, fehlender Bezug zur Geschäftsbeziehung) und ob die Anlage (⇒ Attachment) auch erwartet wurde. 3. Beim Eintreffen mehrerer E-Mails mit gleichlautendem Betreff ist besondere Achtsamkeit geboten.

	4. E-Mails von unbekannten Absendern, die zwar nicht offenkundig sinnlos, aber auch nicht mit einer (qualifizierten) elektronischen Signatur versehen sind, sind mit Vorsicht zu behandeln. 5. Automatische Empfangsbestätigungen sind zu unterlassen, sofern sie nicht verlangt oder im Einzelfall mit dem Mandanten vereinbart wurden. 6. E-Mail-Attachments sind nur dann zu öffnen, wenn sie von einem vertrauenswürdigen Absender stammen und vorher auf Viren, Trojaner etc. untersucht wurden. 7. Vertrauliche Nachrichten und Anlagen sind nur verschlüsselt per E-Mail zu versenden. 8. Anlagen sind in allgemein üblichen, möglichst kompatiblen, sicheren und sparsamen Formaten zu versenden. 9. Der Versand von ausführbaren Programmen (*.com, *.exe), Skriptsprachen (*vbs, *.bat), Office-Dateien (*.doc, *.xls, *.ppt) oder Bildschirmschonern (*.scr) ist zu vermeiden und vorher mit dem Empfänger abzustimmen. 10. Wegen der Gefahr von aktiven Inhalten mit Schadensfunktion sind E-Mails grundsätzlich nicht im HTML-Format zu verschicken. 11. Aufforderungen zur Weiterleitung einer E-Mail mit Viruswarnung, Anhängen etc. an Geschäftspartner, Freunde, Bekannte oder Kollegen sind auf gar keinen Fall zu befolgen. 12. Sofern eine elektronische Signatur vom Empfänger (z. B. § 77 a FGO oder individuelle Vereinbarungen mit den Mandanten) gefordert oder durch das Berufsrecht (z. B. § 9 Abs. 1 StBGebV, siehe auch § 14 Abs. 4 UStG) vorgeschrieben ist, ist die E-Mail mit dem jeweils verlangten Typ von elektronischer Signatur zu unterzeichnen. Ist eine elektronische Signatur nicht vorgeschrieben, ist das Erfordernis einer elektronischen Signatur sowie die Auswahl des geeigneten Typs der Signatur im Einzelfall zu prüfen. 13. Es ist regelmäßig zu prüfen, ob im Postausgangskorb E-Mails liegen, die nicht vom Nutzer verfasst oder dort eingestellt wurden. 14. Auch bei E-Mails sind die Aufbewahrungspflichten gemäß Berufsrecht und GdPdU zu beachten.
E-Mail-Attachment	Ein Attachment ist eine Datei, die einer anderen Datei, einer ⇒ E-Mail, angehängt wird. Attachments können Viren enthalten, weshalb das sofortige Öffnen ein Sicherheitsrisiko darstellt und vor dem Öffnen auf Computerviren, Trojanische Pferde etc. untersucht werden sollten. Die Einstellungen des E-Mail-Programms sollten so gewählt werden, dass die Anlagen von E-Mails nicht automatisch geöffnet werden. Wird z. B. das E-Mail-Programm Outlook verwendet, kann durch die Auswahl eines hohen Sicherheitsgrades (unter Extras → Optionen → Sicherheit → Anlagensicherheit) das automatische Starten einer Anwendung verhindert werden.
E-Mail-Verschlüsselung	Grundsätzlich gilt: Eine Pflicht, nur verschlüsselte E-Mails zu versenden, besteht nicht, wenn der Mandant einem ungeschützten E-Mail-Verkehr zugestimmt hat. Hierfür reicht grundsätzlich die allgemeine Zustimmung des Mandanten aus. Einschlägige Fachverlage bieten entsprechende Musterformulierungen an. Etwas anderes gilt, wenn es sich um sensible Daten bzw. Dokumente handelt (z. B. Jahresabschluss, Steuererklärung, betriebswirtschaftliche Auswertungen). In diesen Fällen muss der Mandant einer unverschlüsselten Übermittlung ausdrücklich zustimmen. Es empfiehlt sich, - bestenfalls bereits bei Abschluss des Steuerberatungsvertrags - zu vereinbaren, hinsichtlich welcher Daten bzw. Dokumente ein

	verschlüsselter bzw. ein unverschlüsselter E-Mail-Verkehr zu erfolgen hat.
Empfänger	Vor einem Versand ist immer nochmals die Prüfung des/der Empfänger vorzunehmen und auch in den Adressstammdaten sicherzustellen, dass in Unternehmensadressen die richtige Person bezeichnet wird. Überdies sollte, soweit möglich, auch bei den verschiedenen Formen der elektronischen Post das Vier-Augen-Prinzip gewahrt werden.
Erhebung	Die Erhebung beschreibt gemäß § 3 Abs. 3 BDSG das Beschaffen von Daten über den Betroffenen.
Explorer	Die Bezeichnung Explorer (lat.: „explorator" = „Erkunder", „Entdecker") wird für Hilfsmittel zur internen und externen Datenverwaltung und -suche verwendet. Über eine entsprechende Einstellung kann die Nutzung des Explorers für einzelne Anwender oder Gruppen eingeschränkt werden, was im Sinne des Datenschutzes erfolgen sollte. Der Internet-Explorer ist ein Browserprogramm für das Internet. ⇒ Browsereinstellungen.
Fernwartung von ITK-Systemen	Mit Fernwartung/Fernbetreuung kann bei Problemen im ITK-System schnelle Hilfe geleistet werden, da der Zugriff mittels spezieller Programme über die Leitung erfolgt. Insbesondere im Zusammenhang mit der berufsständischen Verschwiegenheitspflicht wird die Frage diskutiert, ob die Fernwartung bei den Angehörigen des steuerberatenden Berufes durch Dritte zulässig ist. Mitarbeiter von Serviceunternehmen können mittels Fernwartung in der Regel zwangsläufig auch auf Mandantendaten zugreifen. Bei der Möglichkeit zur Kenntnisnahme von personenbezogenen Daten durch den Dienstleister liegt auch bei Fernwartung => Auftragsdatenverarbeitung vor. Voraussetzung ist ein Vertrag über die Auftragsdatenverarbeitung (§ 11 BDSG) mit dem Fernwartungsdienstleister. Ein Rechtsverstoß, u. a. gegen § 203 StGB liegt vor, wenn die Fernwartung von Personen wahrgenommen wird, die nicht auf die berufliche Verschwiegenheit des Steuerberaters verpflichtet sind. Der Verstoß kann vermieden werden, indem von jedem einzelnen betroffenen Mandanten die Zustimmung erteilt wurde. Neben den strafrechtlichen Auswirkungen kann auch eine zivilrechtliche Haftung in Betracht kommen.
Festplatte	Festplatten sind interne und externe Speichermedien für große Datenmengen beliebiger Datenart. Sowohl Dateien des Betriebssystems als auch andere, etwa durch Anwendungsprogramme erzeugte persönliche Daten können (relativ) dauerhaft gespeichert werden. Die Archivierung digitaler Informationen über längere Zeiträume (10 bis mehrere hundert Jahre) wirft jedoch Probleme auf, da nicht nur die Informationen evtl. verloren gehen können, sondern weil auch die Computer, Betriebssysteme und Programme zum Bereitstellen dieser Informationen u. U. nicht mehr verfügbar sind. Daher sollten die Daten in sich ständig wiederholenden Zyklen neu archiviert werden (⇒ Backup). <u>Ausfallrisiken:</u> Die Anfälligkeit von Festplatten ist besonders bei sehr schnell drehenden Systemen vorwiegend auf thermische Probleme zurückzuführen. Beim mechanischen Aufsetzen des Schreib-Lesekopfes kann die Festplatte beschädigt werden (Head-Crash). (Der Kopf schwebt im Betrieb über der Platte und

	wird nur durch ein Luftpolster am Aufsetzen gehindert, das durch die von der drehenden Scheibe mitgerissene Luft entsteht.) Im laufenden Betrieb sollte die Festplatte daher möglichst nicht bewegt werden und keinen Erschütterungen ausgesetzt sein. Weiterhin können äußere Magnetfelder die Sektorierung der Festplatte irreversibel zerstören. Fehler in der Steuerelektronik oder Verschleiß der Mechanik führen ebenfalls zu Ausfällen. Umgekehrt kann auch längerer Stillstand dazu führen, dass die Mechanik stecken bleibt und die Platte gar nicht erst anläuft. Sollen Festplatten ausgetauscht (auch bei Garantiefällen) oder repariert werden, ist zu beachten, dass alle schutzwürdigen Daten zuvor gelöscht werden und nicht mehr lesbar sind. Dies gilt auch, wenn ein komplettes PC-System zur Reparatur außer Haus gegeben wird.
File-Viren	File-Viren hängen sich an eine Programmdatei an und werden beim Start des betroffenen Programms ausgeführt. Viele Anti-Viren-Produkte können File-Viren entfernen; bei einigen File-Viren gelingt die Beseitigung jedoch nicht. Das Löschen der betroffenen Programmdatei muss zwingend durch „Überschreiben“ erfolgen, da bei einer Verschiebung in den sog. Papierkorb eine Wiederherstellung möglich ist. Einige Anti-Viren-Produkte verfügen über eine „Löschfunktion“, die die befallene Programmdatei durch Überschreiben löscht. Weiter empfiehlt es sich, das gesamte betroffene Programm zu löschen und neu zu installieren.
Firewall	Eine Firewall schützt das DV-System vor Angriffen. Es ist kein Virenschutzprogramm, sondern entscheidet darüber, welche Daten oder Dateien von außen nach innen bzw. von innen nach außen gelangen dürfen. So kann z. B. mittels einer Firewall festgelegt werden, dass ⇒ E-Mails mit Attachments (⇒ E-Mail-Attachments), die ausführbare Programme (*.exe) enthalten, entweder gar nicht oder nur in Verbindung mit einer Warnung in das Netz der Steuerberaterpraxis gelangen. Durch aktive Inhalte können jedoch Angriffe auch von innen gestartet werden, indem z. B. bei der Nutzung des Internets versehentlich ein Programm gestartet wird. Um diese Gefahr zu vermindern sind bestimmte ⇒ Browsereinstellungen und eine Sensibilisierung der Benutzer notwendig.
Funktionsübertragung	⇒ Vorbemerkung Ziff. 4: Auftragsdatenverarbeitung
GDPdU	GDPdU steht für „Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen“. Danach kann der Betriebsprüfer, wenn eine Betriebsprüfung den Zugriff auf Daten, die beim Steuerpflichtigen gespeichert sind, gemäß § 147 Abs. 5, 6 AO zwischen folgenden drei Arten des Datenzugriffs wählen: ▪ unmittelbarer Lesezugriff (Z1), ▪ mittelbarer Zugriff über Auswertungen (Z2) und ▪ Datenträgerüberlassung in verschiedenen Formaten (Z3). Das Recht, eigene Software auf die Systeme des Steuerpflichtigen aufzuspielen, hat der Betriebsprüfer dabei nicht. Für die Datenträgerüberlassung sind verschiedene Formate zugelassen, wozu es auch eine Empfehlung des Bundesfinanzministeriums für einen entsprechenden Beschreibungsstandard gibt. Die Daten lassen sich dann vom Betriebsprüfer in eine Prüfersoftware einlesen. Bei einem Zugriff ist zu beachten, dass nur prüfungsrelevante Daten eingesehen werden können. Die Zugriffsberechtigung ist entsprechend einzurichten (nur Lesezugriff, eingegrenzte Daten, Auswertungen und Zeiträume). Durch § 147 Abs. 6 AO ist der Umfang der steuerlichen Außenprüfung nicht

	erweitert worden.
Gebäude- und Raumabsicherung	Gebäude und Räume können durch geeignete Maßnahmen gegen Feuer, Einbruch, Diebstahl, Vandalismus, Wassereinbruch oder Stromausfall geschützt werden. Damit können Schäden weitgehend abgewendet bzw. minimiert werden. Zum einen wird damit ungewollter Datenverlust vermieden und zum anderen wird verhindert, dass Dritte unberechtigten Zugang zu den Daten erhalten (⇒ Zugangskontrolle, ⇒ Gefährdungspotential)
Gefährdungspotential	<u>Mitarbeiter und Dritte</u> Die Gefahr eines vorsätzlichen Datenschutzverstoßes von „innen" ist ebenso groß wie ein entsprechender Angriff von „außen". Immer wieder werden Vorfälle wie Sabotage oder Diebstahl von Mandantendaten bekannt. Ein vollständiger Schutz gegen kriminelle Energie ist nicht möglich. Umso wichtiger sind präventive Maßnahmen, die es einem potenziellen Angreifer erschweren, Schaden anzurichten. Hierzu zählen u. a. Rollenkonzepte mit individuellen und eingeschränkten Zugriffsrechten, regelmäßiger Zwang zum Passwortwechsel, Aktivierung von Logbüchern, Checkliste für neue und ausscheidende Mitarbeiter, Trennung kanzleieigener Daten von Mandantendaten etc. Inhalt und Umfang von Datenschutzschutzmaßnahmen sind von den beteiligten Personen abhängig. Bereits ein unvorsichtiger oder uneinsichtiger Mitarbeiter stellt ein Gefährdungspotenzial dar. Regelmäßige Schulungs- und Sensibilisierungsaktionen zur Förderung von Akzeptanz und Toleranz für die Datenschutzmaßnahmen sind von größter Bedeutung. Nur von der Notwendigkeit des Datenschutzes überzeugte Mitarbeiter werden die erforderlichen Schutzmaßnahmen konsequent umsetzen. Grundsätzlich gilt: · tägliche Datensicherung einrichten · Mitarbeiter zur Einhaltung von Sicherheitsregeln auffordern · Gesamtverantwortung für den Betrieb und die Sicherheit des Netzes der Steuerberaterpraxis regeln · Zugriffsrechte definieren · Internetnutzung regeln (Befugnis zum Versand/Empfang von E-Mails, zur Recherche im Internet, zum Download aus dem Netz etc.) · Konsequenzen bei Zuwiderhandlungen festlegen Außen- und auch Innentäter können aus ganz unterschiedlichen Beweggründen (Rache, Böswilligkeit, Frust) heraus versuchen, IT-Geräte, Software, Zubehör, Schriftstücke oder Ähnliches zu manipulieren oder zu zerstören. Die Manipulationen sind dabei umso wirkungsvoller, je später sie entdeckt werden, je umfassender die Kenntnisse des Täters sind und je tief greifender die Auswirkungen auf einen konkreten Arbeitsvorgang sind. Sie reichen von der unerlaubten Einsichtnahme in schützenswerte Daten bis hin zur Zerstörung von Datenträgern oder IT-Systemen, was erhebliche Ausfallzeiten nach sich ziehen kann. <u>Fremdfirmen</u> Fremdfirmen haben meist einen direkten (Kanzleizugang) oder indirekten (Remote-)Zugang zu den IT-Systemen der Kanzlei. Diesen Dienstleistern ist daher zwangsläufig in datenschutzrechtlich relevanter Weise ein Zugriff auf die zu schützenden Daten möglich. Neben einer sorgsamen Auswahl des IT-

	Partners ist zur Absicherung daher in jedem Fall eine schriftliche Verpflichtung zur strikten Geheimhaltung notwendig. Um den physischen Einsatz von Fremdmitarbeitern in den Kanzleiräumen möglichst gering zu halten, ist es ratsam, die Nutzung einer speziellen Fernwartungssoftware zuzulassen. Unbedingt abzuraten ist dabei von Softwarelösungen, die den Fremdfirmen zeitlich und technisch einen ungehinderten und unbeschränkten Zugriff auf die Kanzleirechner ermöglichen. Diese Grundsätze sind auch bei automatischen Updates zu beachten. <u>Einbruch</u> Bei Kanzleieinbrüchen kommt neben dem Vermögensschaden immer auch ein Imageschaden durch den Verlust berufsrechtlich geschützter Daten in Betracht. Dem Vorwurf einer fahrlässigen Offenbarung von geschützten Daten kann durch den Nachweis der Beachtung von Datenschutzmaßnahmen begegnet werden. Hierzu zählen in erster Linie die Umsetzung technischer (insbesondere Zutritts-, Zugangs- und Zugriffskontrolle; ⇒ Zugangskontrolle Gebäude, Zugriffsrechte) und organisatorischer Maßnahmen (z. B. Regelungen nach Verlassen der Büroräume). Diese müssen in richtiger Kombination und im Verhältnis zum Schutzzweck getroffen werden. Weitere Entlastungsmöglichkeiten ergeben sich aus der fristgerechten Bestellung eines Datenschutzbeauftragten und einer hinreichenden Dokumentation aller getroffenen Datenschutzmaßnahmen.
Geschäftsmäßigkeit	Das Merkmal der Geschäftsmäßigkeit im Sinne des BDSG erfordert grundsätzlich eine auf eine gewisse Dauer angelegte, also mit Wiederholungsabsicht, ausgeführte Tätigkeit. Eine Entgeltlichkeit oder Gewinnerzielungsabsicht ist dagegen nicht erforderlich.
Handakte	Das Berufsrecht unterscheidet zwischen den Handakten i. w. S. und den Handakten im Sinne von § 66 Abs. 2 StBerG. I. w. S. sind Handakten sämtliche Unterlagen, die der Steuerberater im Rahmen eines Auftragsverhältnisses vom Mandanten oder für diesen von Dritten erhalten oder die der Steuerberater selbst angefertigt hat. Deutlich enger gefasst ist der Handaktenbegriff i. S. d. § 66 Abs. 2 StBerG. Die Unterscheidung spielt jedoch in datenschutzrechtlicher Hinsicht keine Rolle, da die gesamten Handakten nach § 57 Abs. 1 StBerG (Pflicht zur Verschwiegenheit), § 203 Abs. 3 StBG und nach den Bestimmungen der Datenschutzgesetze, insbesondere nach § 5 BDSG, verschwiegen zu behandeln sind. Diese gesetzlichen Verpflichtungen beginnen mit der erstmaligen Einrichtung der Akten, bestehen während der Dauer des Auftragsverhältnisses sowie während der Aufbewahrungsfrist nach Beendigung des Auftragsverhältnisses fort und enden mit der Aushändigung der Akten an den Mandanten oder mit der Aktenvernichtung. Staatliche Behörden - Staatsanwaltschaft, Steuerfahndung und Polizei - haben hinsichtlich der Akten grundsätzlich ein Beschlagnahmeverbot (§ 97 StPO) zu beachten.
Heimarbeitsplatz	Die Zunahme der Netzqualität und Geschwindigkeit macht es möglich von einem außerhalb der Kanzlei über das Internet angeschlossenen PC/Laptop wie am Kanzlei-PC zu arbeiten. Die hierzu notwendigen Sicherheitsanforderungen müssen es einem Dritten unmöglich machen, in das Kanzleinetz einzudringen. Zugangs- und Verschlüsselungstechniken sind einzusetzen, um den Schutz von unbefugtem Eindringen zu gewährleisten.

Homepage	Die Homepage einer Kanzlei ist der Ort, an dem der Berufsangehörige sich, seine Praxis, seine Mitarbeiter und das berufliche Umfeld präsentiert. Sie bildet deshalb das elektronische Aushängeschild der Kanzlei. Sie ist ein Telemediendienst. Gemäß § 5 TMG ist ein Impressum mit vorgeschriebenen Inhalten erforderlich. Auch für die Homepage gelten die allgemeinen Werberegelungen (§ 9 BOStB), wenn auch die Grenzen der inhaltlichen Ausgestaltung grundsätzlich weiter zu ziehen sind als bei sonstigen Werbeträgern, da der potenzielle Mandant durch das Aufrufen der Homepage bereits ein Interesse an der Kanzlei zum Ausdruck gebracht hat. <u>Unzulässig sind daher zumindest die folgenden Inhalte bzw. Gestaltungen:</u> - Werbeanzeigen gewerblicher Unternehmer, die dem Internet-Nutzer beim Öffnen der Homepage „entgegenspringen“ (sogenannte „Pop-Ups“) - Benutzung sachfremder sogenannter „Metatags“, die mit der beruflichen Tätigkeit und dem Internetangebot in keinem Zusammenhang stehen oder die (Marken-)Rechte Dritter verletzen, indem z. B. der Name einer renommierten Großkanzlei als Metatag verwendet wird (Metatags sind u. U. versteckte HTML-Elemente mit Metadaten über das betreffende Dokument, die die Auffindbarkeit im Internet verbessern sollen) - Vorhalten eines öffentlichen Gästebuchs auf der Homepage, wenn es Aussagen Dritter enthält, die einem Steuerberater untersagt wären - Verwendung von Werbebannern gewerblicher Unternehmen auf der eigenen Kanzleihomepage
Identifikation	Bei der Identifikation gibt der Benutzer dem Zugangskontrollsystem seine Identität bekannt, indem er beispielsweise seine Benutzerkennung in das System eingibt (⇒ Authentifizierung und Authentisierung).
Integrität	Die Integrität umfasst Datensicherheit (Schutz vor Verlust) und Fälschungssicherheit (Schutz vor vorsätzlicher Veränderung). Sie ist gewahrt, wenn Daten und Programme nur bestimmungsgemäß erzeugt und verändert werden können, wenn die Daten vom angegebenen Absender stammen, vollständig und unverändert (an den Empfänger übertragen worden) sind.
Interoperabilität	Als Interoperabilität wird im IT-Bereich die Zusammenarbeit von verschiedenen Systemen bezeichnet. Beim Einsatz von verschiedenen Programmen sollte unbedingt darauf geachtet werden, dass alle Daten in einem einfachen, üblichen Dateiformat vorliegen, in einen Datenbestand ausgelesen werden können und eine Schnittstellenbeschreibung vorliegt, um sie im Bedarfsfall auf ein neues System übertragen zu können. Bei Programmänderungen sollte darauf geachtet werden, dass die volle Funktionalität auch für die Alt-Datenbestände erhalten bleibt. Bei einem Systemwechsel ohne komplette Datenübernahme besteht die Notwendigkeit, das Altsystem noch zehn Jahre betriebsbereit zu halten. Durch Datensicherungen, auch kompletter Verzeichnisse, wird dies üblicherweise nicht erreicht.
Kontrolle	⇒ Zugriffsrechte
Kryptographie	In der Kryptographie werden Verfahren (zumeist mathematische Algorithmen) entwickelt, um Informationen zu ver- und entschlüsseln, dass es Unberechtigten nur mit höchstem Aufwand möglich ist, diese Informationen zur Kenntnis zu nehmen (⇒ Chiffrat).
Landesbeauf-	Der Landesbeauftragte für Datenschutz überprüft als Aufsichtsbehörde die

tragter für den Datenschutz	Ausführungen der datenschutzrechtlichen Regelungen im öffentlichen Bereich vornehmlich der Landes- und Kommunalbehörden und auch der Berufskammern.
Landesdaten-schutzgesetz	Jedes Bundesland verfügt über ein eigenes, unter Umständen vom Bundesdatenschutzgesetz abweichendes Landesdatenschutzgesetz, das den Datenschutz in der jeweiligen unmittelbaren und mittelbaren Landesverwaltung regelt.
Laptop	Aus datenschutzrechtlichen Gründen sind besondere Vorkehrungen bzgl. der Diebstahlsgefahr und des Zugangs zu den darauf befindlichen Daten zu beachten. Dies gilt für alle portablen Datenspeicher- und Auswertungsgeräte (z. B. USB-Sticks, Tablet-PCs, Mobiltelefone).
Leserecht	⇒ Zugriffsrechte
Löschen	⇒ Datenlöschung
Makro-Viren	Makro-Viren befinden sich als Makros innerhalb von Dateien, also z. B. in Word-Dateien, und werden beim Start des entsprechenden Programms ausgeführt.
Makroviren-schutz	Sofern nicht ständig mit makrobehafteten Dateien gearbeitet werden muss, sollte der Makrovirenschutz von Anwendungsprogrammen (z. B. WinWord, Excel, PowerPoint) aktiviert und die Warnmeldungen beachtet werden. Es empfiehlt sich der Einsatz von Anti-Viren-Programmen (⇒ Makro-Viren; ⇒ Virenschutzprogramme).
Meldepflicht	§ 4d (1) BDSG: Jede verantwortliche Stelle muss ihrer Datenschutzaufsichtsbehörde die EDV-Verfahren melden, bevor sie in Betrieb genommen werden. § 4d Abs. 2 BDSG: Für verantwortlichen Stellen, die einen Datenschutzbeauftragten bestellt haben, entfällt die Meldepflicht.
Netzwerk	Ein Netzwerk ist der Zusammenschluss verschiedener Datenverarbeitungs- und Datenspeicherungsgeräte, sowohl intern als auch extern. Bei der Einrichtung von Netzwerken sollte eine Definition der ⇒ Zugriffsrechte erfolgen. „Kabelloses“ Netzwerk ⇒ WLAN
nicht-automatisierte Datei	Eine nicht automatisierte Datei ist jede sonstige Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen geordnet, umgeordnet und ausgewertet werden kann (§ 3 Abs. 2 BDSG).
Nicht-öffentliche Stellen	Nicht-öffentliche Stellen i. S. d. BDSG sind natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts. Hierunter sind auch Steuerberaterpraxen zu subsumieren.
Nutzungskon-trolle	⇒ Zugriffsrechte
Papier	⇒ Datenträger
Passwort	Das Passwort (Kennwort) ist eine beliebige, vorgegebene oder vom Nutzer selbst gewählte alphanumerische Zeichenfolge, das der Authentifizierung eines Benutzers dient. Passwörter kommen in Verbindung mit einem Benutzer- oder User-Namen zum Einsatz. Definierte Passwortregeln erhöhen das Sicherheitsniveau.
Personenbezo-gene Daten	Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (§ 3 Abs. 1 BDSG).
Phishing	Als Phishing bezeichnet den Versuch Dritter, an die Daten eines Internetnutzers zu gelangen, z. B. über gefälschte www-Adressen, per E-Mail oder SMS, um diesen zu schädigen. Merkmale von Phishing-Attacken sind bspw. namenlose Anreden („Sehr geehrter Kunde“), ungewöhnliche Aufforderungen, mangelhafte Grammatik und Orthographie, eine vermeindliche Dringlichkeit („Wenn Sie nicht innerhalb der nächsten zwei Tage eine Verifikation durchführen, wird ihr Konto / ihre Kreditkarte gesperrt“). Im Zweifel kann man

	den Quelltext der Phishing-E-Mail anzeigen und untersuchen. Meist erkennt man darin relativ schnell den eigentlichen Absender oder einen URL aus dem Ausland, der mit dem vorgetäuschten Absender nichts zu tun hat. Zum Schutz gegen Phishing-Angriffe kann man bei seinem E-Mail-Programm die HTML-Darstellung sowie Java-Script deaktivieren. Wichtig ist auch, das Antivirenprogramm stets auf aktuellem Stand zu halten. Die E-Mail-Filter einiger Antivirenprogramme können Phishing-E-Mails unter günstigen Umständen erkennen und eliminieren. Neben den technischen Schutzmöglichkeiten sind ein gesundes Misstrauen gegenüber dem unsicheren Medium E-Mail sowie das aufmerksame Lesen der Phishing-E-Mails erforderlich. Kein seriöses deutsches Unternehmen erwartet bspw. eine Reaktion innerhalb von zwei Tagen. Außerdem sollte hinterfragt werden, ob der Absender überhaupt im Besitz der Maildaten ist. Die meisten Banken und Sparkassen etwa verfügen gegenwärtig nicht über diese und schreiben ihre Kunden auf herkömmliche Weise (Postweg) an.
Proxyserver	Der Proxyserver ist eine Netzwerkkomponente, die zur Vermittlung von Internetverbindungen dient. So wird u. a. jede Website, die einmal von einem Nutzer aufgerufen wurde, im Proxyserver gespeichert. Bei nachfolgenden Aufrufen dieser Seite wird diese dann automatisch vom Proxyserver abgerufen und nicht von der ursprünglich eingegebenen Adresse. Richten sich die Kosten der Internetnutzung nach dem Datenvolumen, kann dies zu Einsparungen führen. Nachteil dieser Methode ist, dass die im Proxyserver gespeicherte Website bei einem späteren Aufruf bereits veraltet sein kann.
Prüfsummenprogramm	⇒ Virenschutzprogramm
Pseudonymisierung (BDSG)	Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren (BDSG, § 3 Abs. 6 a). Beim Pseudonymisieren werden lediglich typische Identifikationsmerkmale durch „neutrale“ Merkmale ersetzt. Die Zuordnung zu einer natürlichen Person bleibt dabei durchaus möglich, wird aber erschwert.
Pseudonymisierung (SigG)	Durch die in § 5 Abs. 3 SigG vorgesehene Möglichkeit der Pseudonymisierung des Signaturschlüsselinhabers sind beliebige organisatorische Details abbildbar: So kann z. B. die natürliche Person, Frau Müller, die in der Steuerberatungsgesellschaft XY als Sekretärin für den Steuerberater Schulz arbeitet, das Pseudonym „Steuerberatungsgesellschaft XY, Sekretariat von StB Schulz“ erhalten. Das Pseudonym ist als solches um den Kennzeichner „:PN“ zu ergänzen. D. h., im Zertifikat wird die Bezeichnung „Steuerberatungsgesellschaft XY, Sekretariat von StB Schulz:PN“ als Name des Signaturschlüsselinhabers verwendet. Die Möglichkeit der Vergabe eines Attributzertifikats wird durch den Ersatz des Namens durch ein Pseudonym nicht berührt. Darüber hinaus ermöglichen Pseudonyme beispielsweise, faktisch anonym im Internet einzukaufen und das Erstellen von Benutzerprofilen zu ver- bzw. zumindest zu behindern (⇒ Attributzertifikat).
Qualifizierte elektronische Signatur	Die qualifizierte elektronische Signatur gem. § 2 Nr. 3 SigG ersetzt im elektronischen Rechts- und Geschäftsverkehr die eigenhändige Unterschrift und ist als Beweismittel vor Gericht zugelassen. Die Signaturschlüssel werden von einem Zertifizierungsdiensteanbieter (Trustcenter; ⇒ Akkreditierter Zertifizierungsdiensteanbieter) erzeugt. Der Inhaber der elektronischen Signatur wird anhand seiner Ausweispapiere bei Beantragung der Signaturkarte identifiziert. Der geheime private Signaturschlüssel muss auf einer sicheren Hardware-Komponente (z. B. Smartcard) liegen. Dadurch wird gewährleistet, dass auch für den Inhaber der Signaturkarte der private Schlüssel nicht auslesbar ist. Mit dem privaten Schlüssel signiert der Nutzer ein Dokument. Den

	öffentlichen Schlüssel gibt der Nutzer z. B. auf seiner Homepage bekannt oder fügt ihn als Attachment einer E-Mail bei. Mit Hilfe des öffentlichen Schlüssels kann der Empfänger nun feststellen, ob das Dokument tatsächlich von dem ausgewiesenen Absender stammt und ob es unverändert ist.
Qualifizierte elektronische Signatur mit Anbieterakkreditierung	Aufgrund einer umfassenden Prüfung der verwendeten technischen Komponenten und des Sicherheitskonzepts des Zertifizierungsdiensteanbieters durch die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (BNetzA) stellt die qualifizierte elektronische Signatur mit Anbieterakkreditierung die höchste Sicherheitsstufe bei den digitalen Signaturen dar.
Raid-System	Ein Raid-System erhöht die Sicherheit von Daten durch gleichzeitige Speicherung auf eine weitere oder mehrere Festplatten.
Rechenzentrum (extern)	Im steuerberatenden Bereich versteht man unter einem Rechenzentrum in der Regel das Gebäude bzw. die Räumlichkeiten, in denen extern Rechen- und Speichertechnik (z. B. Großrechner, Server-Farmen aber auch die zum Betrieb notwendige Infrastruktur) untergebracht ist. Bei der Auswahl eines solchen IT-Dienstleisters sind besondere Sicherheitsmaßnahmen bezüglich der Kommunikationswege, der Trennung der Datenbestände und der ⇒ Zugriffsrechte zu beachten. Voraussetzung zur Nutzung eines Dienstleisters ist ein Vertrag über die ⇒ Auftragsdatenverarbeitung.
Richtlinien zur Nutzung der betrieblichen EDV	Bei der Nutzung der betrieblichen EDV sind verbindliche Richtlinien festzulegen, wie z. B.: ▪ Verpflichtung zur Verschwiegenheit (⇒ Verschwiegenheitspflicht) ▪ Verpflichtung der Mitarbeiter sowie zugriffsberechtigter Dritter zur Einhaltung der Zugriffskontrollen (d. h. z. B., keine Weitergabe von Passwörtern) ▪ Verbot von Downloads unbekannter oder unsicherer Programmanbieter ▪ Verbot der Verbindung privater Hard- und Software mit den Geräten der Praxis ▪ Bestellungen, von z. B. Büromaterial, bei Online-Shops nur für zuvor ausgewählte vertrauenswürdige Adressen ▪ Regelung hinsichtlich zulässiger privater Internetnutzung (Dauer und Art der Dienste; ⇒ Gefährdungspotential)
Rollenkonzepte	In der EDV wird als Rollenkonzept eine Benutzerverwaltung bezeichnet, in der System-Benutzern Rechte auf EDV-Systeme vergeben werden.
Schredder	Bei der Anschaffung eines Schredders sollte die DIN-Norm DIN 66399‡ beachtet werden, die die Datensicherheit eines Aktenvernichters/Reißwolfs nach drei Schutzklassen und sieben Sicherheitsstufen bewertet: **<u>Schutzklassen</u>** <u>Schutzklasse 1</u> – normaler Bedarf für interne Daten: • Begrenzte negative Auswirkungen auf das Unternehmen bei unberechtigte Offenlegung oder Weitergabe • Gewährleistung des Schutzes von personenbezogenen Daten; Ansonsten bestehe die Gefahr, dass der Betroffene in seiner Stellung und in seinen wirtschaftlichen Verhältnissen beeinträchtigt wird.

‡ Wiedergegeben mit Erlaubnis von DIN Deutsches Institut für Normung e. V. Maßgebend für das Anwenden der DIN-Norm ist deren Fassung mit dem neuesten Ausgabedatum, die bei der Beuth Verlag GmbH, Am DIN Platz, Burggrafenstraße 6, 10787 Berlin, erhältlich ist.

Schutzklasse 2 – hoher Bedarf für vertrauliche Daten:

- Informationsbeschränkung auf kleinen Personenkreis angemessen.
- Erhebliche Auswirkungen auf das Unternehmen bei unberechtigter Weitergabe und eventuell Verstoß gegen vertragliche Verpflichtungen und Gesetze.
- Hohe Anforderungen an den Schutz von personenbezogenen Daten; ansonsten bestehe die Gefahr, dass der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigt wird.

Schutzklasse 3 – sehr hoher Bedarf für besonders vertrauliche Daten:

- Informationsbeschränkung auf wenige Zugriffsberechtigte erforderlich.
- Schutz von personenbezogenen Daten muss unbedingt gewährleistet sein; ansonsten bestehe Gefahr für Leib und Leben oder für die persönliche Freiheit.
- Weitergabe hätte existenzbedrohende Auswirkungen auf das Unternehmen bzw. würde gegen Berufsgeheimnisse und Verträge verstoßen.

Sicherheitsstufen

Sicherheitsstufe 1 – Allgemeine Daten:

Reproduktion mit einfachem Aufwand
- Fläche der Materialteilchen max. 2000 mm²
- oder Breite des Streifens max. 12 mm
- Länge der Streifen nicht begrenzt
- Toleranz für 10 % des Materials: Fläche der Materialteilchen max. 3.800 mm²

Sicherheitsstufe 2 – Interne Daten:

Reproduktion mit besonderem Aufwand
- Fläche der Materialteilchen max. 800 mm²
- oder Breite des Streifens max. 6,0 mm
- Länge der Streifen nicht begrenzt
- Toleranz für 10 % des Materials: Fläche der Materialteilchen max. 2.000 mm²

Sicherheitsstufe 3 – Sensible Daten:

Reproduktion mit erheblichem Aufwand
- Fläche der Materialteilchen max. 320 mm²
- oder Breite des Streifens max. 2 mm
- Länge der Streifen nicht begrenzt
- Toleranz für 10 % des Materials: Fläche der Materialteilchen max. 800 mm²

	Sicherheitsstufe 4 – Besonders sensible Daten: Reproduktion mit außergewöhnlichem Aufwand • Fläche der Materialteilchen max. 160 mm² • und für gleichförmige Partikel: Breite des Streifens max. 6 mm • Toleranz für 10 % des Materials: Fläche der Materialteilchen max. 480 mm² Sicherheitsstufe 5 – Geheim zu haltende Daten: Reproduktion mit zweifelhaften Methoden: • Fläche der Materialteilchen max. 30 mm² • und für gleichförmige Partikel: Breite des Streifens max. 2 mm • Toleranz für 10 % des Materials: Fläche der Materialteilchen max. 90 mm² Sicherheitsstufe 6 – Geheime Hochsicherheitsdaten: Reproduktion technisch nicht möglich: • Fläche der Materialteilchen max. 10 mm² • und für gleichförmige Partikel: Breite des Streifens max. 1 mm • Toleranz für 10 % des Materials: Fläche der Materialteilchen max. 30 mm² Sicherheitsstufe 7 – Streng geheime Hochsicherheitsdaten: Reproduktion ausgeschlossen: • Fläche der Materialteilchen max. 5 mm² • und für gleichförmige Partikel: Breite des Streifens max. 1 mm oder aufgelöste Materialteilchen bis max. 5 mm² oder zerkleinerte Asche mit Fläche der Materialteilchen max. 5mm² • Toleranz für 10 % des Materials: keine Toleranz zugelassen Für eine ordnungsgemäße Aktenvernichtung wird für die Steuerberatungspraxis mindestens die Sicherheitsstufe 5 (Schutzklasse 3) empfohlen.
SaaS	⇒ ASP
Schreibrechte	⇒ Zugriffsrechte
Server	Server stellen innerhalb einer Netzwerkumgebung Daten und Programme zentral zur Verfügung. Daher sind bei ihnen sowohl physikalisch als auch administrativ besondere Sicherheitsvorkehrungen erforderlich, z. B. durch Definition von Zutritts- und ⇒ Zugriffsrechten.
Sicherheitsregeln	⇒ Richtlinien zur Nutzung der betrieblichen EDV
Signatur	⇒ Elektronische Signatur
Smartcard	Eine Smartcard ist eine spezielle Plastikkarte mit eingebautem Chip, der eine Hardware-Logik, Speicher oder auch einen Mikroprozessor enthält. Sie wird u. a. im Bereich der digitalen Signatur eingesetzt.
Social Engineering	Beim „Social Engineering“ wird versucht, durch persönliche Kontakte, z. B. Telefonate, den unberechtigten Zugang zu Informationen oder zum IT-System zu erhalten. Dabei werden vom “Social Engineer“ menschliche Eigen-

	schaften, wie z. B. Hilfsbereitschaft, Vertrauen, Angst oder Respekt, bzw. Schwächen ausgenutzt, um die Daten oder Zugänge zu erhalten. Skepsis und Zurückhaltung gegenüber Unbekannten und ihrem Auskunftsbegehren ist angebracht; gezielte Rückfragen schrecken ab.
Spyware	Spyware ist eine Software, die persönliche Daten eines PC-Benutzers ohne dessen Wissen, oder Zustimmung an Dritte sendet. Zum Schutz und den Verhaltensmaßnahmen ⇒ Viren.
Systempartner	Der Systempartner als Betreuer der EDV-Anlage hat unmittelbaren Zugang zu sensiblen Daten. Daher muss sichergestellt werden, dass über die Verschwiegenheitsverpflichtung hinaus eine klare Regelung der Zugriffszeiten und -rechte vereinbart wird und Maßnahmen zur Überwachung der Vereinbarungen getroffen werden. Dies kann im vorgeschriebenen Vertrag über die ⇒ Auftragsdatenverarbeitung geregelt werden.
Technische und organisatorische Maßnahmen	Zum Schutz der personenbezogenen Daten sind von den verantwortlichen Stellen die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften des BDSG zu gewährleisten. Insbesondere sind dazu die in der Anlage zu § 9 BDSG enthaltenen „Gebote“ einzuhalten, die folgende Kontrollziele vorgeben: Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle und Trennungsgebot (Einhaltung der Zweckbestimmung).
Trojaner	Trojaner sind selbstständige Programme, die neben ihrer eigentlichen Funktion, z. B. dem Überbringen einer Nachricht, noch weitere Funktionen ausführen, von denen der Anwender jedoch nichts weiß und deren Ausführung er im Regelfall auch nicht bemerkt. Eine solche weitere Funktion kann z. B. die Protokollierung und Versendung des Benutzernamens und Kennworts an Dritte sein. Mit Hilfe der Zugangsdaten können diese dann den Rechner unberechtigt nutzen, z. B. zum Ausspionieren vertraulicher Daten oder zur Nutzung der Telekommunikationsanbindung auf Kosten des Betroffenen. Trojaner gelangen über aus dem Internet heruntergeladene Programme oder über Dateianhänge an E-Mails (z. B. *.exe-Dateien) in das eigene DV-System. Sie können sich nicht selbstständig verbreiten. D. h., in der Regel muss der Anwender aktiv werden und ein Programm aus dem Internet herunterladen oder eine *.exe-Datei, die als E-Mail-Anhang versandt wurde, starten.
Verantwortliche Stelle	Verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt (§ 3 Abs. 7 BDSG)
Verarbeitung	⇒ Datenverarbeitung, automatisierte
Verbindlichkeit	Die Verbindlichkeit ist gewahrt, wenn die Urheberschaft und der Empfang beweisbar sind sowie die Korrektheit (oder Unversehrtheit) der übertragenden Informationen gewährleistet ist.
Verfahrensverzeichnis/Verfahrensdokumentation	Ein Verfahrensverzeichnis bezeichnet eine Übersicht mit bestimmten Angaben, die sich aus § 4 e BDSG ergeben. Für das Verzeichnis, das auf Antrag Jedermann und gemäß § 4 g Abs. 2 dem ⇒ Datenschutzbeauftragten zur Verfügung gestellt werden muss, handelt es sich um folgende Angaben: 1. Name oder Firma der verantwortlichen Stelle, 2. Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen, 3. Anschrift der verantwortlichen Stelle, 4. Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung, 5. eine Beschreibung der betroffenen Personengruppen und der diesbezüg-

	lichen Daten oder Datenkategorien, 6. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können, 7. Regelfristen für die Löschung der Daten, 8. eine geplante Datenübermittlung in Drittstaaten. sowie nur für den Datenschutzbeauftragten, nicht für jedermann: 9. eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 9 zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind.
Verfügbarkeit	Die Verfügbarkeit ist gewahrt, wenn Informationen und IT-Komponenten von Berechtigten bei Bedarf genutzt werden können.
Verpflichtungserklärung	Die bei der Datenverarbeitung beschäftigten Personen sind vor der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten (§ 5 Satz 2 BDSG). Die Verpflichtung zur Wahrung des Datengeheimnisses besteht auch nach Beendigung der Tätigkeit fort. Die Verpflichtung muss in geeigneter Weise durchgeführt werden, die Durchführung ist zu dokumentieren und bei Bedarf zu wiederholen.
Verschlüsselung	Als Verschlüsselung wird ein Sicherheitsmechanismus zur Erreichung von Vertraulichkeit bezeichnet. Die Verschlüsselung erlaubt eine Transformation von Daten in eine Darstellung, die ohne Kenntnis des kryptographischen Schlüssels und ohne unverhältnismäßig hohen Aufwand keine Rückschlüsse auf die ursprünglichen Daten erlaubt (⇒ Chiffrat). In der Anlage zu § 9 BDSG weist der Gesetzgeber explizit die Verwendung von dem Stand der Technik entsprechende Verschlüsselungsverfahren bei der Zugangs-, Zugriffs- und Weitergabekontrolle hin, Diese sollen in einem angemessenen Verhältnis zum angestrebten Schutzzweck stehen (§ 9 Satz 2 BDSG).
Versicherung gegen Datenverluste	In Deutschland entsteht jährlich ein gesamtwirtschaftlicher Schaden von mehr als 10 Milliarden Euro durch illegale Datenbeschaffung und Sabotage im Internet. Daneben gibt es eine Reihe anderer Gefahrenquellen für Daten. Die Versicherungswirtschaft hat darauf reagiert und bietet verschiedenen Versicherungsschutz wie z. B. Internetpolicen an. Die zwei wichtigsten Komponenten bei einer **Hacker- und Virenversicherung** sind die Übernahme der Kosten für die Wiederbeschaffung von Daten und Software nach einem Angriff und der Ersatz der Ertragsausfälle, die entstehen können, wenn die Computer einer Firma lahm gelegt werden (**Betriebsunterbrechungsversicherung**). Auch ist es möglich, den Versicherungsumfang der **Vermögensschaden-Haftpflichtversicherung** (gegen Prämienzuschlag) zu erweitern, um sich gegen materielle oder immaterielle Schäden aus Verletzungen von Persönlichkeitsrechten, insbesondere im Sinne des ⇒ Bundesdatenschutzgesetzes abzusichern. Erhältlich ist auch eine **Haftpflichtversicherung gegen die Ansprüche Dritter**. Vom eigenen Datenverlust können nämlich auch andere betroffen sein. Es müssen aber nicht immer Hacker sein, die das Netz lahm legen. Wenn bei Bauarbeiten versehentlich eine Leitung durchtrennt wird oder technische Probleme auftauchen, kann es zu einem Ausfall der externen Netze kommen. Eine (Mit-) Haftung des Steuerberaters ist etwa in den Fällen denkbar, in denen er die Arbeiten in Auftrag gegeben und Informationen zu

	in der Erde befindlichen Leitungen nicht erteilt hat. Angeboten wird auch eine **Vertrauensschaden-, Computer- und Datenmissbrauchversicherung**. Sie sichert vor Vermögensschäden, die durch Diebstahl, Untreue und Computerbetrug entstehen und versichert Schäden durch eigene Mitarbeiter sowie Datenmissbrauch, der durch betriebsfremde Dritte verursacht wurden. Eine **Straf-Rechtsschutzversicherung** bietet Schutz für die Verteidigung gegen den Vorwurf einer beruflich verursachten Ordnungswidrigkeit oder fahrlässigen Verletzung von Strafbestimmungen bzw. bei Verstößen gegen das Steuer- und sonstige Abgabenrecht und standesrechtliche Verfahren nach §§ 89 ff. StBerG. Diese Versicherung könnte etwa für den Fall sinnvoll sein, wenn der Datenmissbrauch/Datenklau durch die eigenen Mitarbeiter mit dem Vorwurf verbunden ist, der Steuerberater habe gegen die Verschwiegenheitspflicht verstoßen bzw. den Straftatbestand des § 203 StGB (Verletzung von Privatgeheimnissen) erfüllt. Ein sorgloser Umgang mit den Daten ist selbstverständlich auch mit Versicherung nicht zulässig. So wird z. B. verlangt, dass Kunden Sicherheitsvorkehrungen wie Virenschutz oder Firewalls auf dem neuesten Stand halten, Duplikate anlegen und aktuelle Datensicherungen vornehmen. Auch fordern die Versicherer von ihren Kunden grundsätzlich, dass sie ihre Mitarbeiter anweisen, firmeneigene EDV-Geräte nicht privat zu nutzen. Selbst die Nutzung unbekannter Quellen aus dem Netz ist teilweise untersagt. Bei Verstoß muss die Versicherung nicht zahlen. Sogar die Zusammenarbeit mit Sicherheitsspezialisten kann Auflage sein, um die Police überhaupt zu bekommen.
Videoüberwachung	§ 6b BDSG regelt die Videoüberwachung im öffentlich zugänglichen Raum. Im innerbetrieblichen Einsatz sind arbeitsrechtliche Regelungen zu beachten. Sie ist vorabkontrollpflichtig (=> Vorabkontrolle)
Viren	Computerviren sind sich selbstverbreitende Computerprogramme, die sich z. B. in andere Programme einschleusen können und sich damit reproduzieren. Ein Virus kann vom Anwender nicht kontrollierbare Änderungen am Status der Hardware (z. B. Netzwerkverbindungen), am Betriebssystem, oder an der vorhandenen Software bewirken. Ein absoluter Schutz gegen Viren ist nicht möglich. Es empfiehlt sich die mindestens tägliche Aktualisierung eines ⇒ Virenschutzprogrammes. <u>Verhalten bei Verdacht auf Virenbefall:</u> 1. Zügige Beendigung der Arbeit, Herunterfahren und Ausschalten des Rechners 2. Der Datenaustausch zwischen einzelnen Rechnern sollte rückverfolgt werden, um festzustellen, welche weiteren Rechner möglicherweise infiziert sind. 3. Die betroffenen Anwender (Mitarbeiter in der eigenen Steuerberaterpraxis, Mandanten, andere Geschäftspartner, Freunde oder Bekannte) sind sofort darüber zu unterrichten, dass ihnen u. U. infizierte Dateien oder Datenträger zugegangen sind, um die weitere Verbreitung des Virus zu begrenzen. 4. Zur Vermeidung eines künftigen Virusbefalls ist es zweckmäßig, den Weg der Erstinfektion zu ermitteln. 5. Nach der Virenentfernung ist besondere Vorsicht geboten beim Aufspielen von Datensicherungsdisketten, da diese u. U. auch von dem Virus befallen sind. Hier muss zunächst eine Virenprüfung und ggf. -

	beseitigung erfolgen.
Virenschutzprogramme	Virenschutzprogramme sind Softwarelösungen, die bekannte Computerviren, -würmer, -trojaner etc. aufspüren, blockieren und ggf. beseitigen.
V. o. I. P.	Als „Voice over Internet Protocol“ bezeichnet man die Telefonie über Computernetzwerke, die nach dem Internetstandard aufgebaut sind. Es können sowohl über Computer, auf IP-Telefonie spezialisierte Telefonendgeräte, als auch über spezielle Adapter angeschlossene klassische Telefone die Verbindung ins Netzt herstellen. Daten sind leichter abhörbar, als über eine Standardtelefonleitung.
Vorabkontrolle	Weist eine automatisierte Verarbeitung besondere Risiken für die Rechte und Freiheiten der Betroffenen auf, wie z. B. die Verarbeitung besonderer Datenarten (Angaben über rassische und ethnische Herkunft, politische Meinung, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben) oder soll damit die Persönlichkeit des Betroffenen einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens bewertet werden, ist vor dem Beginn der Verarbeitung eine Vorabkontrolle durchzuführen und dabei zu überprüfen, ob die Daten für die Aufgabenerfüllung überhaupt benötigt werden (§ 4 d Abs. 5 BDSG).
VPN	Als Virtual Private Network bezeichnet man eine Software zur Einbindung von Geräten eines anderen Netzwerks, an das eigene Netzwerk, ohne dass die Netzwerke zueinander kompatibel sein müssen. VPN basiert auf einer Tunneltechnik über ein spezielles Gateway (VPN-Einwahlknoten), in der die Partner virtuell miteinander verbunden sind.
Web-Cookies	⇒ Cookies
W-LAN	Wireless LAN (W-LAN, WLAN) bezeichnet ein „drahtloses“ lokales Funknetz. Diese können je nach Hardwareausstattung und Bedürfnissen der Betreiber in verschiedenen Modi betrieben werden. Bei der Nutzung von W-LAN sind grundlegende Sicherheitsmaßnahmen zu beachten. Dazu gehören einige Einstellungen am Router bzw. AP: Aktivierung der Verschlüsselung mit einer sicheren Verschlüsselungsmethode, d. h. mindestens WPA Vergabe eines sicheren Netzwerkschlüssels, Ersetzen der werkseitig voreingestellten Router- bzw. AP-Passwörter, Änderung des werkseitig voreingestellten SSID-Namens, Deaktivierung der Fernkonfiguration eines eventuell vorhandenen Routers.
XML/XBRL	Die Extensible Markup Language („erweiterbare Auszeichnungssprache“), abgekürzt XML, ist eine Auszeichnungssprache zur Darstellung hierarchisch strukturierter Daten in Form von Textdateien. Die Verwendung vom XML vereinfacht die Auswertung, Repräsentation und Verarbeitung der Daten und wird bevorzugt für den Austausch von Daten zwischen unterschiedlichen IT-Systemen eingesetzt, speziell über das Internet. Die Extensible Business Reporting Language (XBRL) ist eine frei verfügbare Sprache auf der Basis von XML. XBRL dient der Erstellung und dem technisch und inhaltlich standardisierten Austausch von Informationen der Geschäftsberichterstattung. Ziel von XBRL ist es, Ineffizienzen im Prozess des Datenaustauschs und der -analyse zu reduzieren sowie den Vergleich und die Vergleichbarkeit von Informationen zu erleichtern. XBRL ist auf dem Weg, ein internationaler Standard zu werden und deshalb für die Softwareentwickler sehr relevant.
Zeitstempel	Die qualifizierte elektronische Signatur unter einem Dokument kann mit dem (qualifizierten) Zeitstempel des Zertifizierungsdiensteanbieters versehen werden. Die Zeitsignatur eines Trustcenters verknüpft bestimmte Daten mit der gesetzlich gültigen Zeit und bestätigt digital, dass diese Daten, wie z. B. die qualifizierte elektronische Signatur oder ein elektronisches Dokument, zu dem angegebenen Zeitpunkt dem Trustcenter vorgelegen haben. D. h., an-

	hand des Zeitstempels kann festgestellt werden, ob die qualifizierte elektronische Signatur und z. B. das Attribut „Steuerberater“ zum Zeitpunkt der Vertragsunterzeichnung oder der Unterzeichnung einer E-Mail gültig waren. Über die ausgegebenen Zeitstempel werden von den Zertifizierungsdiensteanbietern Protokolldateien angelegt, sodass eine nachträgliche Fälschung kaum möglich ist.
Zertifikat	Das Zertifikat, auch „qualifiziertes Zertifikat“ genannt, ist eine mit der elektronischen Signatur des Zertifizierungsdiensteanbieters versehene digitale Bescheinigung darüber, dass der öffentliche Signaturschlüssel einer bestimmten Person zugeordnet wurde und die Identität dieser Person bei Ausstellung des Zertifikats eindeutig (z. B. durch Vorlage eines gültigen Personalausweises) festgestellt wurde. Mit der qualifizierten elektronischen Signatur übernimmt der Zertifizierungsdiensteanbieter eine Garantenfunktion für die Richtigkeit der Angaben in dem Zertifikat. Darüber hinaus ist der Zertifizierungsdiensteanbieter verpflichtet, das qualifizierte Zertifikat jederzeit für jeden über öffentlich erreichbare Kommunikationsverbindungen nachprüfbar und – unter der Voraussetzung der Zustimmung des Signaturschlüssel-Inhabers – abrufbar zu halten. Da qualifizierte Zertifikate rechtlich der eigenhändigen Unterschrift gleichgestellt sind, kann der öffentliche Signaturschlüssel per Zertifikat nur einer natürlichen Person zugeordnet werden, was die Ausstellung eines öffentlichen Schlüssels auf eine juristische Person oder ein Unternehmen ausschließt. Die Verbindung zu der juristischen Person, z. B. der Steuerberatungsgesellschaft XY, oder der Berufsbezeichnung, z. B. „Steuerberater“, kann über die Pseudonymisierung bzw. das Attributzertifikat hergestellt werden. Im Unterschied zur fortgeschrittenen elektronischen Signatur beruht die qualifizierte elektronische Signatur auf einem zum Zeitpunkt ihrer Erzeugung gültigen Zertifikat, das von einem Zertifizierungsdiensteanbieter ausgestellt sein muss.
Zertifizierungsdiensteanbieter	⇒ Akkreditierter Zertifizierungsdiensteanbieter
Zugangskontrolle (Datenverarbeitungssystem)	Eine Zugangskontrolle besteht in der Regel aus der Identifikation und der Authentifizierung eines Benutzers. ⇒ Zugriffsrechte
Zutrittskontrolle (Gebäude)	Eine physikalische Kontrolle ist z. B. durch Schließmechanismen und Alarmanlagen sicherzustellen.
Zugriffskontrolle (Daten)	⇒ Zugriffsrechte
Zugriffsrechte	Zugriffsrechte bezeichnen in der EDV die Regeln der administrativen Zugriffskontrolle nach denen entschieden wird, ob und wie Benutzer, Programme oder Programmteile ausführen und Netzwerke, Drucker, Dateisysteme nutzen dürfen. Am geläufigsten ist dieses Konzept bei Dateisystemberechtigungen in denen festgelegt wird, welche Benutzer welche Dateien und Verzeichnisse lesen, schreiben, ändern oder ausführen dürfen. Eine Möglichkeit Zugriffsrechte sehr flexibel zu gestalten, sind Zugriffskontrolllisten: Für jedes zu schützende Objekt gibt es eine Liste, die für jeden Benutzer (Benutzerrolle) oder jede Gruppe angibt, welche Zugriffe erlaubt sind und welche nicht. Manche Programmiersprachen haben auch ein eigenes, vom Betriebssystem unabhängiges Sicherheitssystem, das in die Laufzeitumgebung integriert ist. Beispiele hierfür sind die Sicherheitskonzepte von Java und .NET. Dabei sind die Zugriffsrechte zumeist nicht vom Benutzer abhängig, sondern davon, inwieweit eine bestimmte Programmbibliothek als vertrauenswürdig angesehen wird.
Zweckbindung der Daten	Die Zweckbindung der Daten bedeutet, dass personenbezogene Daten nur für den Zweck weiterverarbeitet werden dürfen, für den sie erhoben worden

	sind. Bei der Erhebung personenbezogener Daten sind die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen.

Anhang 2: Verpflichtungserklärung zur Wahrung des Datengeheimnisses und der Verschwiegenheit

Hiermit bestätige ich, Herr/Frau (Name, Personal-Nummer), dass ich heute von Herrn/Frau StB/StBV auf die Wahrung des Datengeheimnisses nach § 5 BDSG sowie auf die besondere berufliche Verschwiegenheit des steuerberatenden Berufs gem. § 62 StBerG verpflichtet worden bin.

Über das Bundesdatenschutzgesetz, insbesondere die Vorschriften des § 5 (Datengeheimnis), bin ich belehrt worden. Danach ist mir unter anderem untersagt, geschützte personenbezogene Daten unbefugt zu einem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck zu erheben, zu verarbeiten, bekannt zu geben, zugänglich zu machen oder sonst zu nutzen. Zum Schutz der Daten ist im Rahmen der zugewiesenen Aufgabe die notwendige Sorgfalt anzuwenden. Bestehende Datensicherungsvorschriften sind zu beachten; festgestellte Mängel im Sicherungssystem sind unverzüglich zu beheben oder dem Praxisinhaber zu melden.

Ich bin darüber belehrt worden, dass sich die berufliche Verschwiegenheitspflicht auf alles erstreckt, was mir in Ausübung oder bei Gelegenheit meiner beruflichen Tätigkeit anvertraut worden oder bekannt geworden ist bzw. noch anvertraut oder bekannt wird.

Die Pflicht zur Verschwiegenheit bzw. zur Wahrung des Datengeheimnisses erstreckt sich insbesondere auf

1. Namen, Anschriften sowie die persönlichen und wirtschaftlichen Verhältnisse aller Auftraggeber (Mandanten), ihre Absichten, Objekte, Planungen und internen Verhältnisse
2. die persönlichen, wirtschaftlichen und steuerlichen Verhältnisse meines Arbeitgebers und der anderen im Büro tätigen Personen
3. alle Äußerungen nicht nur gegenüber Fremden, sondern auch gegenüber Angehörigen i. S. v. § 15 Abgabenordnung; das sind Verlobte, Ehegatten und sonstige in dieser Vorschrift genannte nahe stehende Personen.

Zur Wahrung der Verschwiegenheitspflicht habe ich weiter besonders zu beachten, dass

1. ich nicht berechtigt bin, fremden, mit der Sache nicht befassten Personen Einblick in Post, Geschäftssachen, Belege und sonstige Unterlagen zu gewähren oder derartige Unterlagen an mich zu nehmen oder sie ohne ausdrücklichen Auftrag an Dritte herauszugeben, auch nicht in Abschrift oder Fotokopie

2. alle im Büro vorkommenden Vorgänge unter Verschluss zu halten sind.

Die Verschwiegenheitspflicht und die Pflicht zur Wahrung des Datengeheimnisses besteht auch nach Beendigung des Dienstverhältnisses zeitlich unbegrenzt fort.

Sonstige Geheimhaltungspflichten, wie das Betriebs- oder Geschäftsgeheimnis, werden durch diese Verpflichtungserklärung nicht beeinträchtigt.

Mir ist bekannt, dass Verstöße gegen das Bundesdatenschutzgesetz oder andere Datenschutzvorschriften zur fristlosen Kündigung des Arbeitsverhältnisses und zu Schadensersatzforderungen führen können sowie gemäß §§ 43, 44 BDSG mit Geld- oder Freiheitsstrafen geahndet werden können.

Über die dieser Verpflichtungserklärung beiliegenden gesetzlichen Bestimmungen[§] über die Verschwiegenheitspflicht des steuerberatenden Berufs sowie über die Pflicht zur Wahrung des Datengeheimnisses nach dem BDSG bin ich belehrt worden.

Eine Ausfertigung dieser Verpflichtungserklärung wurde mir ausgehändigt.

.....	.....
(Ort, Datum)	(Unterschrift)

[§] Die folgenden gesetzlichen Bestimmungen sind in ihrem Wortlaut dieser Verpflichtungserklärung beizulegen: §§ 57 Abs. 1, 62 StBerG; §§ 203, 204 StGB; §§ 53, 53 a, 97 StPO; §§ 383, 385 ZPO; §§ 102, 104 AO; § 84 FGO; § 17 MaBV; §§ 5, 43, 44 BDSG.

Anhang 3: Verpflichtungserklärung eines Fremdunternehmens zur Wahrung des Datengeheimnisses und der Verschwiegenheit (z. B. DV-Wartungsfirmen, Aktenvernichtungs-, Reparatur-, Reinigungs- oder private Briefdienste)

Verpflichtungserklärung

der Fa. .....

– nachstehend Auftragnehmer genannt –

gegenüber dem Steuerberater .....

– nachstehend Auftraggeber genannt –

(1) Der Auftragnehmer verpflichtet sich, im Rahmen der Auftragserfüllung das Datengeheimnis gemäß § 5 BDSG sowie die berufliche Verschwiegenheitspflicht des Steuerberaters zu wahren.

(2) Die Pflicht zur Wahrung des Datengeheimnisses und zur Verschwiegenheit besteht auch nach Beendigung des Auftragsverhältnisses zeitlich unbegrenzt fort.

(3) Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut machen sowie diese auf das Datengeheimnis verpflichten wird. Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften durch seine Beschäftigten und wird den Datenschutz und die Datensicherheit durch geeignete technische und organisatorische Maßnahmen sicherstellen.

(4) Der Auftragnehmer wurde darüber belehrt, dass die Angehörigen des steuerberatenden Berufs einer besonderen Verschwiegenheitspflicht im Hinblick auf die ihnen bekannt gewordenen Tatsachen ihrer Mandanten unterliegen. Der Auftragnehmer wird daher in geeigneter Form alle Mitarbeiter, die er im Rahmen der Auftragserfüllung einsetzt, über das Erfordernis außerordentlicher Vertraulichkeit unterrichten und diese auf die besondere Verschwiegenheit verpflichten.

(5) Der Auftragnehmer verpflichtet sich sicherzustellen, dass die Arbeiten nur durch die auf das Datengeheimnis und die besondere Verschwiegenheit verpflichteten Mitarbeiter durchgeführt werden.

(6) Die Einschaltung bzw. Beauftragung von Subauftragnehmern ist ausgeschlossen.

(7) Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die Bestimmungen des BDSG oder die berufliche Verschwiegenheitspflicht des Steuerberaters vorliegt.

(8) Der Auftragnehmer ist dem Auftraggeber für alle Schäden, die durch eine Verletzung dieser Verpflichtungserklärung entstehen, ersatzpflichtig.

Über die dieser Verpflichtungserklärung beiliegenden gesetzlichen Bestimmungen[**] über die Verschwiegenheitspflicht des steuerberatenden Berufs sowie über die Pflicht zur Wahrung des Datengeheimnisses nach dem BDSG ist der Auftragnehmer belehrt worden.

Eine Ausfertigung dieser Verpflichtungserklärung wurde dem Auftragnehmer ausgehändigt.

.....	.....
(Ort, Datum)	(Unterschrift)

[**] Die folgenden gesetzlichen Bestimmungen sind in ihrem Wortlaut dieser Verpflichtungserklärung beizulegen: §§ 57 Abs. 1, 62 StBerG; §§ 203, 204 StGB; §§ 53, 53 a, 97 StPO; §§ 383, 385 ZPO; §§ 102, 104 AO; § 84 FGO; § 17 MaBV; §§ 5, 43, 44 BDSG.