Report

DSGVO 2018

www.Deubner-Steuern.de

Ein kostenloser Service des Deubner Verlags ©

Deubner
Steuern & Praxis

IMPRESSUM

© by Deubner Verlag GmbH & Co. KG
Alle Rechte vorbehalten. Nachdruck und Vervielfältigung
– auch auszugsweise – nicht gestattet.

Wichtiger Hinweis
Die Deubner Verlag GmbH & Co. KG ist bemüht, ihre Produkte jeweils nach neuesten Erkenntnissen zu erstellen. Deren Richtigkeit sowie inhaltliche und technische Fehlerfreiheit werden ausdrücklich nicht zugesichert.

Die Deubner Verlag GmbH & Co. KG gibt auch keine Zusicherung für die Anwendbarkeit bzw. Verwendbarkeit ihrer Produkte zu einem bestimmten Zweck. Die Auswahl der Ware, deren Einsatz und Nutzung fallen ausschließlich in den Verantwortungsbereich des Kunden.

Deubner Verlag GmbH & Co. KG
Sitz in Köln
Registergericht Köln
HRA 16268

Persönlich haftende Gesellschafterin:
Deubner Verlag Beteiligungs GmbH
Sitz in Köln
Registergericht Köln
HRB 37127
Geschäftsführer: Ralf Wagner, Werner Pehland

Deubner GmbH & Co. KG
Oststraße 11, D-50996 Köln
Fon +49 221 937018-0
Fax +49 221 937018-90
kundenservice@deubner-verlag.de
www.deubner-steuern.de

Spezialreport: Die Datenschutz-Grundverordnung (DSGVO)
Alle wichtigen Neuerungen und Änderungen des neuen Datenschutzrechts auf einen Blick

- Stand: Februar 2018
Von Assessor iur./Externer Datenschutzbeauftragter Jürgen Seul, Bad Neuenahr-Ahrweiler

Ziele: Die Europäische Datenschutzgrundverordnung (DSGVO) bringt auch für Kanzleien eine Reihe von Änderungen im Vergleich zur bisherigen Rechtslage mit sich. Die DSGVO gilt auch in Deutschland und löst das bisherige Bundesdatenschutzgesetz (BDSG) und die EU-Datenschutzrichtlinie (Richtlinie 95/46/EG), auf der das BDSG basiert, ab. Flankiert wird die DSGVO noch von einem deutschem Ergänzungsgesetz (Datenschutz-Anpassungs- und -Umsetzungsgesetz – DSAnpUG), das die DSGVO zum Teil modifiziert und konkretisiert. Eine weitere Ergänzung der DSGVO erfolgt durch die EU-e-Privacy-Verordnung, die Internet- und Telemediendienste betrifft.
Das Ziel der DSGVO ist die Schaffung eines weitgehend einheitlichen Datenschutzrechts innerhalb der EU, indem es vor allem die Rechte und Kontrollmöglichkeiten der Betroffenen stärken soll, deren personenbezogene Daten verarbeitet werden.
Wesentliche Elemente des bisherigen BDSG, wie die Grundsätze der Datenverarbeitung (Rechtmäßigkeit, Zweckbindung, Datensparsamkeit, Richtigkeit, zeitliche Speicherbegrenzung, Integrität und Vertraulichkeit sowie eine Rechenschaftspflicht der Verantwortlichen für die Einhaltung dieser Grundsätze), stellen auch den Kern der DSGVO dar. Die DSGVO muss vor allem im Zusammenspiel mit dem novellierten BDSG angewandt werden.
Die einzelnen Themen im Datenschutzmanagement reichen vom datenschutzkonformen Internetauftritt über die Kontrolle der Dienstleister, die Beschreibung und Bewertung sämtlicher datenschutzrelevanter Prozesse in der Steuer- und Rechtsanwaltskanzlei bis hin zur Sensibilisierung der Mitarbeiter. Das Gefährdungspotenzial ist in den vergangenen Jahren durch die moderne Technik stetig angestiegen (jederzeitige Verfügbarkeit von Daten etwa, Apps zum mobilen Zugriff auf Berufsgeheimnisdaten etc.). Als Berufsgeheimnisträger sind gerade Steuerberater und Rechtsanwälte besonders gefordert, auf die Einhaltung von datenschutz- und persönlichkeitsrechtlichen Vorgaben zu achten.
Aus Gründen der besseren Lesbarkeit wird im Folgenden von der Kanzlei, dem Kanzleiinhaber oder vom Verantwortlichen gesprochen. Dieser Spezialreport soll Kanzleien informieren, damit sie ihre Organisation und Prozesse an die neue Rechtslage anpassen können.

Der Aufbau der Verordnung gestaltet sich wie folgt:

Kapitel 1 – Allgemeine Bestimmungen (Artikel 1-4)
Kapitel 2 – Grundsätze (Artikel 5-11)
Kapitel 3 – Rechte der betroffenen Person (Artikel 12-23)
Kapitel 4 – Verantwortlicher und Auftragsverarbeiter (Artikel 24-43)
Kapitel 5 – Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen (Artikel 44-50)
Kapitel 6 – Unabhängige Aufsichtsbehörden (Artikel 51-59)
Kapitel 7 – Zusammenarbeit und Kohärenz (Artikel 60-76)

 © Deubner Verlag GmbH & Co. KG

Kapitel 8 – Rechtsbehelfe, Haftung und Sanktionen (Artikel 77-84)
Kapitel 9 – Vorschriften für besondere Verarbeitungssituationen (Artikel 85-91)
Kapitel 10 – Delegierte Rechtsakte und Durchführungsrechtsakte (Artikel 92-93)
Kapitel 11 – Schlussbestimmungen (Artikel 94-99)

Wesentliche Änderungen und Neuregelungen im Überblick:

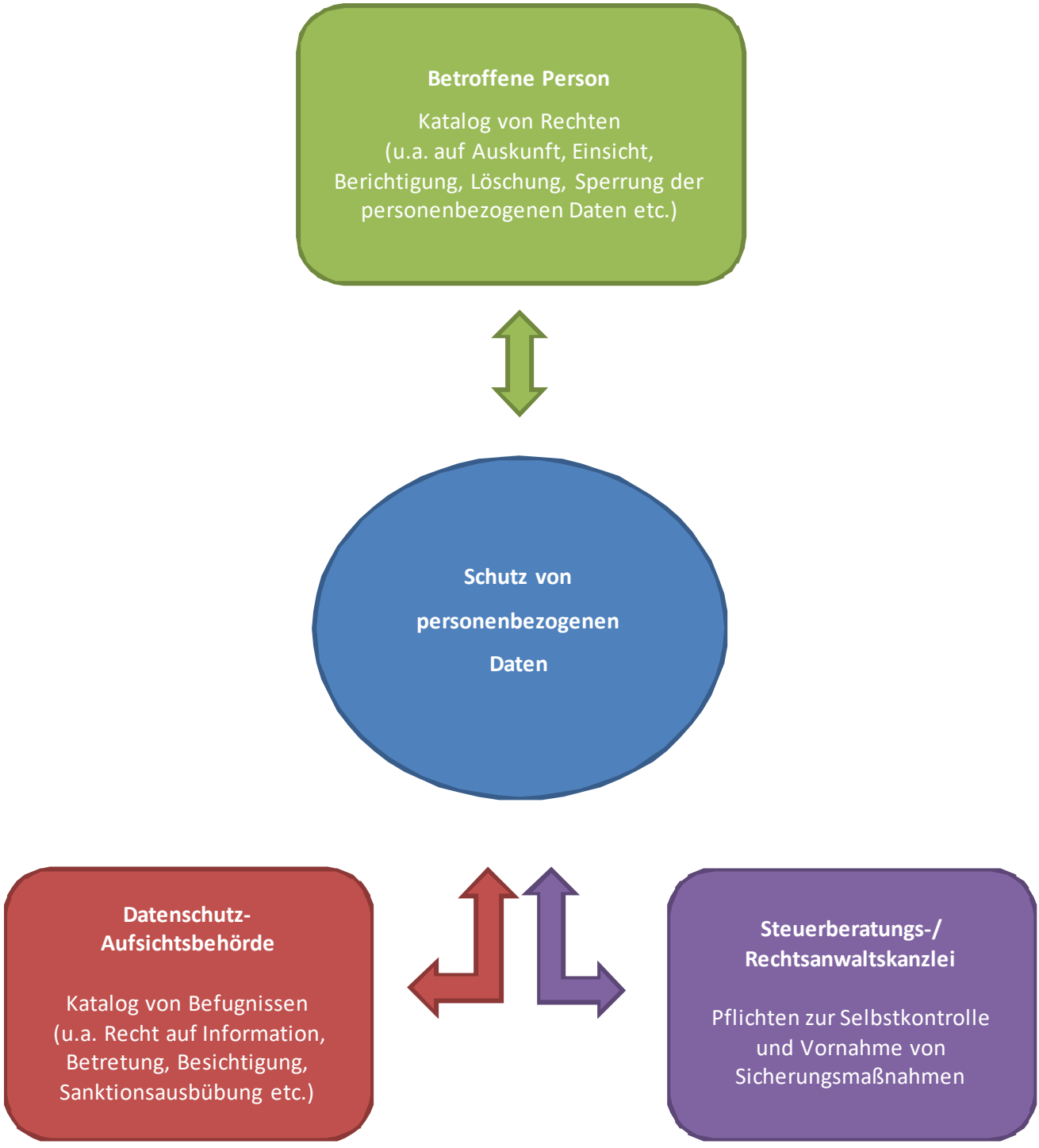
- **Marktortprinzip:** Das Datenschutzrecht gilt für alle Unternehmen, die auf dem europäischen Markt agieren. Der Firmensitz spielt keine Rolle; auch nicht der Ort, an dem die Datenverarbeitung stattfindet. Die DSGVO verpflichtet jedes Unternehmen, dass Waren oder Dienstleistungen in die EU liefert.
- **Grundsatz des Privacy by Default:** Datenschutzrechtliche Anforderungen gelten bereits bei der Planung neuer Techniken und neuer Verarbeitungen.
- **Grundsatz des Privacy by Design:** Datenschutzprobleme müssen schon bei der Entwicklung neuer Technologien festgestellt und geprüft werden. Datenschutz und Privatsphäre sind von vorneherein in die Gesamtkonzeption und Entwicklung einzubeziehen.
- **Datenschutzbeauftragter:** Künftig gibt es den Datenschutzbeauftragten EU-weit. Die Kontaktdaten des Datenschutzbeauftragten müssen veröffentlicht und der zuständigen Aufsichtsbehörde mitgeteilt werden.
- **Einwilligung:** Für die Verarbeitung personenbezogener Daten muss eine ausdrückliche und freiwillige Zustimmung der Kunden eingeholt werden. Voreingestellte Haken sind nicht mehr erlaubt. Kunden müssen ihre Einwilligung jederzeit widerrufen können.
- **Einsichtsrecht:** Kunden müssen jederzeit Einsicht in ihre personenbezogenen Daten erhalten.
- **Grundsatz der Transparenz:** Neben den Kontaktdaten des verarbeitenden Unternehmens sind auch die Kontaktdaten des Datenschutzbeauftragten in der Datenschutzerklärung anzugeben.
- **Hinweispflicht:** Kunden müssen auf ihre Datenschutzrechte (Zugang, Berichtigung, Sperrung, Beschwerderecht bei der Aufsichtsbehörde usw.) hingewiesen werden. Die Herkunft der Daten und die Speicherdauer müssen ebenfalls angegeben werden.
- **Kopplungsverbot:** Es ist Unternehmen verboten, eine Kopplung der Datenverarbeitung mit den erbrachten Leistungen oder Produkten vorzunehmen.
- **Pseudonymisierung:** Kundendaten müssen künftig pseudonymisiert werden.
- **Recht auf Datenlöschung:** Unternehmen müssen personenbezogene Daten auf Wunsch der Betroffenen löschen.
- **Pflicht zur Datensicherung:** Das Unternehmen muss die personenbezogenen Daten der Kunden vor Verlust zu schützen. Verantwortliche müssen die Datensicherheit regelmäßig überprüfen und evaluieren.
- **Grundsatz der Integrität und Vertraulichkeit:** Unbefugte dürfen keinen Zugang zu personenbezogenen Daten haben.
- **Auftragsdatenverarbeitung:** Zukünftig werden Auftraggeber und Auftragnehmer für die Datenverarbeitung gleichermaßen verantwortlich sein.

- **Meldepflichten von Datenschutzverstößen:** Zukünftig müssen alle Datenschutz-Pannen gemeldet werden, wenn ein Datenschutzrisiko besteht. Die Meldung muss binnen 72 Stunden nach Kenntnis bei der Aufsichtsbehörde eingereicht werden. Auch die Betroffenen sind „ohne unangemessene Verzögerung“ zu benachrichtigen.
- **Beweislastumkehr:** Unternehmen müssen künftig nachweisen, dass sie die datenschutzrechtlichen Regeln eingehalten haben.
- **Erhöhte Strafen:** Bei extremen Datenschutzverstößen müssen Unternehmen künftig bis zu 20 Millionen Euro oder vier Prozent ihres weltweit erzielten Jahresumsatzes als Bußgeld zahlen.

Inkrafttreten: Die DSGVO trat am 25.05.2016 in Kraft. Ihre Umsetzung in der Praxis muss zum 25.05.2018 erfolgt sein.

 © Deubner Verlag GmbH & Co. KG

Datenschutz im Überblick



 © Deubner Verlag GmbH & Co. KG

1. Die Bedeutung des Datenschutzes für eine Kanzlei

Der Hauptzweck der DSGVO besteht im Schutz der Grundrechte (u.a. auf „informationelle Selbstbestimmung“) und Grundfreiheiten natürlicher Personen und vor allem deren Recht auf Schutz personenbezogener Daten (Art. 1 Abs. 2 DSGVO).

Die technologische Entwicklung der automatisierten Datenverarbeitung führte in den vergangenen Jahren zu einer steigenden Gefährdung des Datenmissbrauchs, da immer mehr Daten nahezu unbegrenzt gespeichert, verknüpft und ausgewertet werden können. Eine Folge dieser Entwicklung ist die Beeinträchtigung des Einzelnen in seinen Persönlichkeits- und Freiheitsrechten. Gerade in Kanzleien werden eine Vielzahl personenbezogener Mandantendaten gespeichert, verknüpft und ausgewertet, weshalb die Regelungen des neuen Datenschutzrechts hier eine herausragende Bedeutung zukommt. Betroffen sind daneben aber auch die Mitarbeiter, Dienstleister und sonstige Dritte. Es gilt, das Grundrecht auf informationelle Selbstbestimmung sicherzustellen und die Daten der betroffenen Betroffenen vor Missbrauch zu schützen.

1.1. Personenbezogene Daten

Die DSGVO gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Der Anwendungsbereich der Verordnung ist eröffnet, wenn eine elektronische Datenverarbeitung zum Einsatz kommt.

Hinweis:
Als **personenbezogene Daten** gelten alle Informationen, die sich auf eine **identifizierte** oder **identifizierbare natürliche Person** beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, vor allem mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann (Art. 4 Nr. 1 DSGVO).

Zu den **personenbezogenen Daten** zählen allgemein:

- Namen
- Geburtsdatum
- Familienstand
- Staatsangehörigkeit
- Beruf
- Erscheinungsbild
- Gesundheitszustand
- Politische oder religiöse Überzeugungen
- Adresse
- Telefonnummer
- Familienstand
- Pseudonyme
- Ausweisnummer
- Darstellungen in Bild und Ton
- Feste (statische) IP-Adresse
- eine den Inhaber benennende E-Mail-Adresse

Für den Tätigkeitsbereich einer Kanzlei kommen als betroffene Bereiche mit **personenbezogenen Daten** in Betracht:

- zentrale Stammdaten
- Finanzbuchhaltung
- Lohnbuchhaltung
- Jahresabschluss/Steuern
- Wirtschaftsberatung/Controlling
- Rechtsberatung

Der Begriff der **Datenverarbeitung** umfasst den Umgang mit personenbezogenen Daten wie:

- Datenerhebung,
- Datenspeicherung,
- Datenänderung,
- Datennutzung,
- Datenübermittlung,
- Datenverknüpfung oder
- Datenlöschung.

In allen diesen Fällen handelt es sich um ein Verarbeiten im Sinne der DSGVO. Abzugrenzen ist von einer Datenverarbeitung ausschließlich für persönliche und familiäre Tätigkeiten (z. B. private Adressbücher oder Fotos), die nicht in den Anwendungsbereich der DSGVO fällt.

Hinweis:
Jeder Kanzleimitarbeiter muss mit personenbezogenen Daten sorgfältig und achtsam umgehen, da ihm ansonsten strafrechtliche, arbeitsrechtliche als auch schadensersatzpflichtige Konsequenzen drohen.

Die DSGVO ist auch von allen Kanzleien zu beachten, deren Angebot sich an einen bestimmten nationalen Markt innerhalb der EU richtet. Es gilt das **Marktortprinzip**, wonach Firmensitz und auch der Ort einer Datenverarbeitung keine Rolle spielen.

Hinweis:
Die DSGVO gilt nicht für die Verarbeitung personenbezogener Daten zum Zweck der Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Steuerstraftaten oder Steuerordnungswidrigkeiten (Art. 2 Abs. 2 Buchst. d DSGVO). Insoweit gelten die Vorschriften des Ersten und des Dritten Teils des BDSG, soweit gesetzlich nichts anderes bestimmt ist (§ 2a Abs. 4 AO).

2. Die Zulässigkeit einer Datenverarbeitung

2.1. Grundsätze der Verarbeitung personenbezogener Daten

Der Kanzleiinhaber trägt als verantwortliche Stelle die Verantwortung für die Verarbeitung personenbezogene Daten, sei es mittels IT oder in strukturierten Datensammlungen wie z.B. Mandanten- oder Personalakten. Die Zulässigkeit der Verarbeitung ist nicht auf Dateien beschränkt; vielmehr unterliegt jede personenbezogene Information dem Datenschutz.
Die Beachtung der Grundsätze der Datenverarbeitung und das Datenschutzmanagements müssen vom Kanzleiinhaber nachgewiesen werden.
Zu den Grundsätzen der Verarbeitung personenbezogener Daten nach Art. 5 DSGVO gehören:

- Zweckbindung
- Richtigkeit

- Datenminimierung
- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
- Speicherdauerbegrenzung
- Integrität und Vertraulichkeit

Die DSGVO fordert von einem Kanzleiinhaber ein Datenschutzmanagement, dessen technische und organisatorische Maßnahmen umgesetzt, überprüft und aktualisiert werden.

2.2. Verbot mit Erlaubnisvorbehalt

Jede Datenverarbeitung bedarf einer gesetzlichen Rechtfertigung. Bei einer Datenerhebung ist außerdem der Zweck, für den die Daten verarbeitet werden sollen, konkret festzulegen.
Als wichtigster Fall für eine zulässige Datenverarbeitung gilt auch nach der DSGVO der allgemeine **Grundsatz des Verbots mit Erlaubnisvorbehalt**. Danach ist grundsätzlich verboten, was nicht ausdrücklich erlaubt ist. Hieraus folgt, dass die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten verboten sind, es sei denn,

- sie sind durch eine Rechtsvorschrift ausdrücklich erlaubt oder angeordnet oder
- der Betroffene hat dazu seine Einwilligung erklärt.

Soll eine Einwilligung Grundlage für eine Erhebung, Verarbeitung oder Nutzung sein, ist zu beachten, dass

- sie **freiwillig** erfolgen muss,
- grundsätzlich der **Schriftform** bedarf (es sei denn, wegen besonderer Umstände ist eine andere Form angemessen),
- der Betroffene vorher über die Tragweite seiner Einwilligung **aufgeklärt** wurde,
- der Betroffene auch darüber zu informieren ist, was geschieht, wenn er nicht einwilligt.

Bei der Verarbeitung **besonderer Arten personenbezogener Daten** muss sich die Einwilligung ausdrücklich auf diese Daten beziehen. Es handelt sich hierbei um Angaben über

- rassische und ethnische Herkunft
- politische Meinungen
- religiöse oder politische Überzeugungen
- Gewerkschaftszugehörigkeit
- Gesundheit
- Sexualleben

Die Möglichkeiten der Erhebung, Verarbeitung und Nutzung personenbezogener Daten unterliegen einer Vielzahl von Einschränkungen. Bereits bei der Erhebung personenbezogener Daten sind die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen. Dies gilt auch für die geschäftsmäßige Datenverarbeitung. Eine Verwendung für andere Zwecke kommt u.a. nur in Betracht:

- zur Wahrung berechtigter Interessen der verantwortlichen Stelle oder eines Dritten oder
- wenn die Daten allgemein zugänglich sind oder veröffentlicht werden dürften.

Hinweis:
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 (= Kanzleiinhaber).

Es muss stets zwischen den entgegenstehenden schutzwürdigen Interessen des Betroffenen und dem Interesse an der Zweckänderung abgewogen werden. Es besteht eine grundsätzliche **Zweckbindung**, von der nicht ohne weiteres abgewichen werden darf. Änderungen des Verarbeitungszwecks sind grundsätzlich nur erlaubt, wenn sie mit dem ursprünglichen Erhebungszweck vereinbar sind. Die DSGVO sieht Kriterien vor, die bei der Beurteilung der Vereinbarkeit einer **Zweckänderung** zu berücksichtigen sind. Hierzu gehört u. a.:

- die Verbindung zwischen den Zwecken,
- der Gesamtkontext, in dem die Daten erhoben wurden,
- die Art der personenbezogenen Daten,
- mögliche Konsequenzen der zweckändernden Verarbeitung für den Betroffenen oder
- das Vorhandensein von angemessenen Sicherheitsmaßnahmen (z.B. eine Verschlüsselung).

Eine Zweckänderung liegt vor, wenn die Daten verwendet werden für:

- die Rechnungsprüfung,
- die Wahrnehmung von Aufsichts- und Kontrollbefugnissen,
- Organisationsuntersuchungen sowie
- Ausbildungs- und Prüfungszwecke der speichernden Stelle.

Eine strikte Zweckbindung besteht für Daten, die ausschließlich zur Datenschutzkontrolle, Datensicherung, zur Sicherung eines ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage oder zur wissenschaftlichen Forschung gespeichert werden.

2.3. Beachtung des Prinzips der Datensparsamkeit

Auch nach der DSGVO gilt das Prinzip der Datensparsamkeit, wonach die Erhebung und Verarbeitung personenbezogener Daten dem Zweck angemessen und sachlich relevant sowie auf das für den Zweck der Datenverarbeitung notwendige Maß beschränkt sein muss.
Bei Unternehmen wird der größte Teil der personenbezogenen Daten (u.a. Kundendaten) zur Erfüllung eigener Geschäftszwecke verwendet. Die Daten sind grundsätzlich beim Betroffenen zu erheben. Es ist ihm mitzuteilen, zu welchem Zweck dies geschieht. Ohne Mitwirkung des Betroffenen dürfen Daten nur erhoben werden, wenn

- eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder
- die Erhebung beim Betroffenen einen unverhältnismäßig hohen Aufwand zur Folge hätte und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen des Betroffenen beeinträchtigt werden.

Ob die befragte Stelle die erbetenen Daten übermitteln darf, muss besonders geprüft werden. Wenn die personenbezogenen Daten beim Betroffenen erhoben werden, muss er informiert werden. Er hat Anspruch darauf zu erfahren,

- welche die verantwortliche Stelle ist, die die Daten erhoben hat und
- welche Zweckbestimmung der Datenerhebung zugrunde liegt.

Nur so ist gewährleistet, dass der Betroffene seine Datenschutzrechte wahrnehmen kann.

Hinweis:
Die Aufsichtsbehörde kann von dem Kanzleiinhaber verlangen, dass er nachweisen kann, welche personenbezogenen Daten von Mitarbeitern, Kunden, Lieferanten oder Vereinsmitgliedern er verarbeitet, auf welcher Rechtsgrundlage er dies konkret macht, für welchen Zweck er die Daten verwendet und wie lange er sie noch speichern möchte.

2.4. Auftragsverarbeitung

Entschließt sich eine Kanzlei zum Outsourcing einzelner Tätigkeiten müssen dabei verschiedene rechtliche, technische und organisatorische Voraussetzungen erfüllt werden.

Hinweis:
Auftragsverarbeitung liegt vor, wenn eine natürliche oder juristische Person (z. B. GmbH, KG, AG), Behörde, Einrichtung oder andere Stelle personenbezogene Daten im Auftrag eines Verantwortlichen verarbeitet.

Werden dem Auftragnehmer personenbezogene Daten zu diesem Zweck überlassen, findet datenschutzrechtlich gesehen keine Übermittlung statt, da der Auftragnehmer nicht Dritter ist. Gegenüber dem Geschäftspartner oder Mandanten bleibt der Kanzleiinhaber als Auftraggeber der Datenverarbeitung voll dafür verantwortlich, dass mit ihren personenbezogenen Daten rechtmäßig umgegangen wird. Der Kanzleiinhaber muss

- einen schriftlichen Auftrag erteilen und
- die erforderlichen Maßnahmen zur Datensicherheit vorgeben.

Der Auftragnehmer darf und muss im Rahmen der Weisungen seines Auftraggebers tätig werden. Der Kanzleiinhaber muss sich vor Beginn der Datenverarbeitung und anschließend regelmäßig über die Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugen (Kontrollrechte) und das Ergebnis dieser Überprüfung dokumentieren. Es ist möglich, diese Aufgabe gegebenenfalls an vertrauenswürdige Dritte (z.B. durch unabhängige Sachverständige) zu delegieren, welche die Einhaltung der Vorgaben mittels Zertifikat bescheinigen.
Auch die Beendigung einer Auftragsvergabe muss datenschutzrechtlich geregelt sein. Hierzu gehört u.a. die Festlegung, wann Unterlagen zurückzugeben oder Daten zu löschen bzw. zu vernichten sind.
Umgekehrt stellt sich in der Praxis häufig die Frage, ob ein Steuerberater selber Auftragnehmer im Sinne des Datenschutzrechts ist. Soweit der Steuerberater „klassische“ Steuerberatungstätigkeiten erbringt (Erstellung Jahresabschluss, Steuerberatung etc.) handelt er

ausweislich § 32 Abs. 2 Steuerberatungsgesetz („StBerG“) i. V. m. den tätigkeitsbeschreibenden Normen im StBerG eigenverantwortlich und damit aufgrund gesetzlicher Vorgaben weisungsfrei. Aus dieser Weisungsfreiheit ergibt sich bereits, dass ein Steuerberater hinsichtlich dieser Tätigkeiten nicht den Vorgaben der Auftragsdatenverarbeitung und damit der Weisungsgebundenheit des Auftraggebers unterworfen werden kann.

2.5. Mitarbeiterfotos im Internet und Intranet

Auf Internetauftritten von Steuerberatern und Rechtsanwälten finden sich sehr häufig auch Bilder von Mitarbeitern einer Kanzlei.

Die DSGVO beinhaltet selber keine ausdrückliche Regelung für den Umgang mit Mitarbeiterfotos. Die Verordnungsgeberin ging davon aus, dass die allgemeinen Regelungen der DSGVO für personenbezogene Daten ausreichen, um solche Fälle zu lösen.

Das deutsche Recht kennt seit über 100 Jahren im Kunsturhebergesetz (KUG) die gesetzlichen Regelungen zum Recht am eigenen Bild. Das KUG enthält die Regelungen, die das Recht am eigenen Bild betreffen. Nach § 22 KUG dürfen **Bildnisse nur mit Einwilligung des Abgebildeten** verbreitet oder öffentlich zur Schau gestellt werden. Die Einwilligung gilt im Zweifel als erteilt, wenn der Abgebildete dafür, dass er sich abbilden ließ, eine Entlohnung erhielt. Nach dem Tode des Abgebildeten bedarf es bis zum Ablauf von 10 Jahren der Einwilligung der Angehörigen des Abgebildeten (überlebende Ehegatter oder Lebenspartner, Kinder und – wenn dieser Personenkreis nicht vorhanden ist – die Eltern des Abgebildeten).

Hinweis

Für die Veröffentlichung eines Mitarbeiterfotos auf der Homepage einer Kanzlei gilt die **Grundregel**, dass eine schriftliche Einwilligung der abgebildeten Person erforderlich ist (§ 22 KUG). Die Zustimmung muss vor der Veröffentlichung eingeholt werden. Eine nachträgliche Genehmigung durch den Mitarbeiter ist möglich.

Von Bedeutung für die Abbildung von Mitarbeiterbildern im Internet ist neben § 22 KUG die Neufassung des § 26 BDSG. Sie führt im Normalfall zu keinem anderen Ergebnis als die Regelungen des KUG. Es macht im Übrigen auch keinen Unterschied, ob Fotos im Internet oder in einem Intranet verwendet werden.

Es ist empfiehlt sich nicht, die Einwilligung zur Veröffentlichung von Mitarbeiterfotos in einer Klausel des Arbeitsvertrages einzubauen, da solche Klauseln als Allgemeine Geschäftsbedingungen gelten und eine Einwilligung immer individuell zu erfolgen hat. Alternativ sollten Einwilligungen auch nicht in Form von Betriebsvereinbarungen geregelt werden, da es sich beim Recht am eigenen Bild um ein höchstpersönliches Recht handelt, über das der Mitarbeiter nur selbst verfügen kann. Das Bundesarbeitsgericht hält es allerdings für zulässig, wenn Mitarbeiter eine Art „Sammeleinwilligung“ abgeben, indem sie auf einer Namensliste unterschreiben. Mit einer solchen Unterschrift bestätigen die Mitarbeiter, dass Film- und Fotoaufnahmen ihrer Person zur freien Nutzung im Rahmen der Öffentlichkeitsarbeit der Kanzlei verwendet bzw. ausgestrahlt werden dürfen. Notwendig ist allerdings, dass der Verwendungszweck für Fotos und Filme auf einer solchen Sammeleinwilligung sehr genau beschrieben wird. Die Einwilligung des Mitarbeiters kann aus wichtigem Grund widerrufen werden.

Hinweis
Ein wichtiger Widerrufsgrund kann sein, dass der auf der Kanzleihomepage abgebildete Mitarbeiter aus der Firma ausgeschieden und inzwischen für eine Konkurrenzkanzlei tätig ist.

2.6. Datenübermittlung in Drittstaaten

Eine Übermittlung von personenbezogenen Daten in ein Drittland oder an eine internationale Organisation ist nur zulässig, wenn die Kanzlei die zur Datenübermittlung in Drittländer und zu internationalen Organisationen niedergelegten Bedingungen erfüllen und auch die sonstigen Bestimmungen der DSGVO beachtet werden.
Eine Übermittlung ist danach zulässig, wenn die EU-Kommission entschieden hat, dass ein angemessenes Schutzniveau besteht. Fehlt eine solche Entscheidung, dürfen personenbezogene Daten in ein Drittland oder an eine internationale Organisation nur übermittelt werden, wenn geeignete Garantien vorliegen und durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen. Hierzu gehören:

- unternehmensinterne Datenschutzvorschriften (sog. „Binding Corporate Rules“) oder
- Standarddatenschutzklauseln,

die von der Kommission oder der Aufsichtsbehörde angenommen werden.

Ob in einem Land ein angemessenes Datenschutzniveau besteht, kann festgestellt werden

- durch die Kanzlei selbst durch Überprüfung der relevanten Kriterien wie Art der Daten, Zweckbestimmung, Dauer der geplanten Verarbeitung, Herkunft und Bestimmungsland, für den Empfänger geltende Rechtsnormen, Standesregeln und Sicherheitsmaßnahmen und
- durch die Europäische Kommission.

Darüber hinaus kommt eine Übermittlung von Daten an einen Drittstaat auch im Rahmen weitreichender Ausnahmeregelungen in Betracht.

3. Maßnahmen zur Datensicherheit

3.1. Schutzziele der IT-Sicherheit

Als zentrales Prinzip des Datenschutzes wurde in der DSGVO auch die Gewährleistung von Datensicherheit verankert. Sie fordert für die Systeme und Dienste, die im Zusammenhang mit der Datenverarbeitung stehen, Vertraulichkeit (Verbergung von Informationen gegenüber Unbefugten), Integrität (Sicherstellung der Unversehrtheit von Daten) und Verfügbarkeit (jederzeitige Nutzbarkeit der vorhandenen Daten). Diese Eckpfeiler der Datensicherheit können auf verschiedene Weise verletzt werden.

Beispiel 1 [Verletzung der Vertraulichkeit]
Auf der abendlichen Heimfahrt in der U-Bahn arbeitet der Steuerberater mit seinem dienstlichen Laptop an einem Brief an seinen Mandanten, um Einzelheiten eines Erbvertrages durchzugehen, der am Folgetag besprochen werden soll. Dabei bemerkt er nicht, dass andere Fahrgäste, die sich eine Sitzreihe hinter ihm befinden, den Inhalt des Bildschirms fast genauso gut sehen können wie er selbst und dadurch vertrauliche Details interessiert mitlesen.

Beispiel 2 [Verletzung der Integrität]
Ein neuer Auszubildender benutzt für seine Tätigkeit, eine Excel-Tabelle nach Umsätzen einen Firmenkunden auszuwerten, an einem PC mit Vollzugriff auf das Kanzleinetzwerk. Aus Neugierde öffnet er verschiedene Dateien, die an sich nichts mit seiner Beschäftigung zu tun haben, jedoch auf dem gleichen Netzwerklaufwerk liegen wie die von ihm behandelte Excel-Tabelle. Da sich der Auszubildende nicht gut mit dem System auskennt, verändert er versehentlich wichtige Mandantendaten und speichert die Veränderungen auch noch ab.

Beispiel 3 [Verletzung der Integrität]
Ein Hacker erkennt bei einer Steuerberaterkanzlei eine weit verbreite Schwachstelle, die einen unmittelbaren Zugriff auf elektronische Mandantenakten ermöglicht. Auslöser der Schwachstelle waren fehlende Software-Updates, die der Hacker zum gezielten Löschen einzelner Mandanten-Stammdaten nutzt.

In allen Fällen drohen Störungen der Mandatsausübung, finanzielle Schäden, Schädigungen des Rufs oder die Offenbarung von Geschäftsgeheimnissen an Unbefugte.

3.2. Schutzmaßnahmen

3.2.1. Allgemeine organisatorische Anforderungen

Der Kanzleiinhaber sollte aus den genannten Gründen unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie der Art, der Umstände und Zweck der Datenverarbeitung, aber auch der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die persönlichen Rechte und Freiheiten alle geeigneten technischen und organisatorischen Maßnahmen einsetzen, um die Datensicherheit zu gewährleisten.
Je komplexer die Datenverarbeitungssysteme werden, desto wichtiger ist es, frühzeitig Datenschutzrisiken zu erkennen, technische und organisatorische Maßnahmen vorzusehen, die eine für den Betroffenen einfache und effiziente Möglichkeit zum Selbstschutz bieten, und Anreize zu schaffen, Datenschutz möglichst frühzeitig in technische Systeme zu integrieren.
Schon bei der Konzeption von IT-Systemen müssen Belange des Datenschutzes gewährleistet werden („Privacy by Design“). Dabei geht es in erster Linie darum, den Umfang der erhobenen und verarbeiteten personenbezogenen Daten auf ein Minimum zu beschränken.
Zu einer datenschutzgerechten Technikgestaltung gehören auch entsprechende Voreinstellungen von IT-Systemen und elektronischen Diensten („Privacy by Default“).
Mit einem „Datenschutzaudit“ können Anbieter von Datenverarbeitungssystemen und -programmen als auch verantwortliche Stellen ihre Datenschutzkonzepte sowie ihre technischen Einrichtungen mit einem datenschutzrechtlichen Gütesiegel versehen lassen und damit werben. Die Prüfung sollte durch unabhängige und zugelassene Gutachter erfolgen.
Besondere Bedeutung kommt auch der Pflicht zur Information bei Datenschutzpannen zu. Danach müssen Kanzleien im Falle des Verlusts von als besonders gefährdet eingestuften Daten die Betroffenen sowie die Aufsichtsbehörde informieren. Unterbleibt diese Information oder ist sie nicht richtig, nicht vollständig oder nicht rechtzeitig, droht ein Bußgeld.
Die DSGVO sieht für Verantwortliche und Auftragsverarbeiter deutlich erweiterte Nachweispflichten vor (sog. „accountability“). So wird vorgeschrieben, dass der für die

Verarbeitung Verantwortliche die Einhaltung der Datenschutzgrundsätze nachweisen kann. Folgende Prozesse und Dokumente sollte eine Kanzlei prüfen und vorhalten:

- Einführung eines Berechtigungsmanagements (mit der Regelung, wer unter welchen Voraussetzungen Zugriff auf bestimmte personenbezogene Daten erhält),
- Dokumentation der Datenverarbeitungsprozesse in der Kanzlei,
- Datenschutzerklärungen (Erweiterung der Informationspflichten)
- Einwilligungserklärungen (Verschärfung der formalen Vorgaben),
- Prozess für den Widerruf der Einwilligung,
- Anpassung der Betriebsvereinbarungen an die DSGVO,
- Prozesse zur Umsetzung von Widersprüchen,
- Vereinbarungen zur Auftragsverarbeitung (Haftungsregelung, Dokumentation),
- Überarbeitung des Prozesses bei Datenpannen, entsprechend der neuen Vorgaben,
- Verfahren, um Daten in einem gängigen elektronischen Format übertragen zu können,
- Durchführung von zielgruppengerechten Schulungen zu den Neuerungen der DSGVO und den eigenen Prozessen,
- Durchführung einer Risiko-Analyse zur Festlegung geeigneter technisch-organisatorischer Maßnahmen,
- Vornahme einer Datenschutz-Folgenabschätzung,
- Monitoring nationaler Gesetzgebung und Fortbildung,
- Implementierung eines Backup-Managements (d.h. eine organisierte Erstellung von Datensicherungen auf Medien, die nicht zum eigentlichen Kanzleinetzwerk gehören)
- Maßnahmen zur Zugangserschwernis bzw. Zugangsverwehrung (d.h. Vornahme von Schutzmaßnahmen für die eigenen Kanzleiräumlichkeiten, um Unbefugten den Zutritt physikalisch zu erschweren bzw. ihn zu verhindern).

Hinweis

Eine Kanzlei sollte über ein effektives Datenschutzmanagement–System mit den oben aufgeführten Prozessen verfügen und vor allem die einzelnen Schutzmaßnahmen dokumentieren, sodass auch gegenüber einer Aufsichtsbehörde der Nachweis geführt werden kann, dass geeignete Strategien und Maßnahmen ergriffen worden sind.

3.2.2 Verschlüsselung

Als geeignete Maßnahme zur Sicherheit der Datenverarbeitung führt Art. 32 Abs. 1a DSGVO die Verschlüsselung auf. Folgende Verschlüsselungsverfahren lassen sich in der Praxis meist problemlos umzusetzen und entfalten zugleich eine sehr große Wirkung:

- **Dateien, Dokumente und Nachrichten:** Mit geringem Aufwand lassen sich bei Dateien mit Hilfe von Zip-Verschlüsselungen schützen. Ähnliches gilt für E-Mails, die sich entweder per Zip-Verschlüsselung oder mit Hilfe etablierter Lösungen wie PGP oder S/MIME verschlüsseln lassen. Eine Verschlüsselung empfiehlt sich auch bei der Verwendung von Cloud-Diensten.
- **Einwahllösungen:** Für Besuche bei Mandanten benötigen Kanzleimitarbeiter gelegentlich Zugriff auf das eigene Kanzleinetzwerk. Es empfiehlt sich, mittels VPN einen Daten über sicheren Kanal auszutauschen.

- **E-Mail-Server:** Die Einstellungen STARTTLS und Perfect Forward Secrecy ermöglichen eine Transportverschlüsselung nach dem Stand der Technik. Auf diese Weise werden E-Mail-Nachrichten zwischen den beteiligten Mailservern im Idealfall durchgängig verschlüsselt, weshalb ein Mitlesen von Unbefugten auf dem Transport nicht möglich ist.
- **Mobile Geräte:** Beim Einsatz von mobilen Geräten (Smartphones, Tablets oder klassische Notebooks), ist es notwendig, diese neben dem Kennwort zum Entsperren des Nutzer-Accounts („Windows-Passwort“) auch mit einer Datenträgerverschlüsselung auszustatten.
- **Website:** Wenn personenbezogene Daten auf einer Website verarbeitet werden (z.B. über ein Kontaktformular auf der Kanzlei-Website), gilt HTTPS als Transportverschlüsselung als eine erforderliche Sicherheitsmaßnahme.
- **WLAN-Netze:** Wenn Kanzleien WLAN-Netze zur Verfügung stellen, ist zwingend darauf zu achten, dass diese ausreichend vor unbefugten Zugriffen geschützt werden (u.a. Verwendung von Passwörtern beim WLAN-Netz selbst und auch beim Zugriff auf den WLAN-Router). Voreingestellte Passwörter zur Konfiguration des WLAN-Routers sollten umgehend geändert werden.

4. Verzeichnis von Datenverarbeitungstätigkeiten

4.1 Pflicht zur Erstellung eines Verzeichnisses

Grundsätzlich müssen auch Kanzleien ein Verzeichnis über alle Datenverarbeitungstätigkeiten führen, die in ihrem Betrieb durchgeführt werden (z.B. Programme zur Mandats-, Personal- und Dienstleisterverwaltung). Es muss demnach dokumentiert werden, in welchem Zusammenhang mit personenbezogenen Daten gearbeitet wird (Art. 30 DS-GVO).

Ziel des Verzeichnisses ist es, eine Übersicht über alle Verarbeitungsvorgänge in der Kanzlei zu führen, in die personenbezogene Daten eingebunden sind. Es sollen alle Prozesse der Kanzlei Eingang in das Verzeichnis der Verarbeitungstätigkeiten finden. Dabei ist es unerheblich, ob die Verarbeitung auf Papier oder EDV-gestützt erfolgt. Ein handgeführtes Kanzleipostbuch oder die Personalakten der Mitarbeiter zählen ebenso zur Verarbeitung wie die Finanzbuchhaltung, der Abruf der Kontenauszugsdaten oder die regelmäßige Sicherung des Datenbestandes in einem Rechenzentrum.

4.2 Inhalt des Verzeichnisses

Das Verzeichnis muss bestimmte Mindestangaben enthalten (Art. 30 Abs. 1 DSGVO):

- den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten,
- die jeweilige Verfahrensbezeichnung (z. B. Bewerbung, Personalverwaltung, Finanzbuchhaltung, Mandanteninfoabend),
- die jeweilige Zweckbestimmung der Datenverarbeitung,
- eine Beschreibung der betroffenen Personengruppen (Beschäftigte, Mandanten, Mitarbeiter von Mandanten, Besucher des Internetauftritts),
- eine Beschreibung der personenbezogenen Daten oder Datenkategorien,

- die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden (z. B. IT-Dienstleister, Systempartner, Hosting-Dienstleister, Aktenvernichter), einschließlich Empfänger in Drittländern oder internationalen Organisationen,
- für den Fall von Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation die Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation,
- die Regelfristen für die Löschung der Daten, wobei zu beachten gilt, dass für Protokolldaten oder Videoüberwachung nicht die üblichen 10 oder 6 Jahre, sondern teilweise nur Wochen oder Stunden gelten,
- eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen.

4.3. Erweitertes Verzeichnisses

Es empfiehlt sich zur Kontrolle des eigenen Unternehmens, ein erweitertes Verzeichnis zu erstellen, in dem zusätzlich aufgeführt werden:

- die konkreten Verarbeitungstätigkeiten und
- die herangezogenen Rechtsgrundlagen (z. B. Art. 6 DS-GVO, Arbeitsvertrag, Betriebsvereinbarung, Einwilligung oder sonstige spezielle Regelungen)

aufgeführt werden.

4.4 Freistellung von der Verzeichniserstellungspflicht

Unternehmen sind von der Verpflichtung zur Erstellung eines Verzeichnisses der Verarbeitungstätigkeiten freigestellt, wenn sie

- weniger als 250 Mitarbeiter beschäftigen und
- die Verarbeitung nur gelegentlich erfolgt und auch keine besonderen Datenkategorien (z.B. Religionsdaten im Rahmen der Abführung von Kirchsteuer etc.) verarbeitet werden.

Eine solche Freistellung kommt für Kanzleien nicht in Betracht.

4.5. Vorlage des Verzeichnisses

Das Verzeichnis ist nicht öffentlich und muss auch den betroffenen Personen auch nicht offengelegt werden. Es dient ausschließlich zur Vorlage gegenüber der Aufsichtsbehörde, um nachweisen zu können, in welchem Verfahren in dem jeweiligen Unternehmen oder mit personenbezogenen Daten umgegangen wird.

4.6. Form des Verzeichnisses

Das Verzeichnis ist regelmäßig und schriftlich in deutscher Sprache zu führen. Es kann auch elektronisch vorgehalten werden.

4.7. Aktualisierung des Verzeichnisses

Das Verzeichnis muss auf aktuellem Stand gehalten werden. Änderungen sollten dokumentiert werden, um Aktualisierungen gegenüber der Aufsichtsbehörde nachweisen zu können.

5. Datenschutzbeauftragter

5.1. Notwendigkeit einer Bestellung

Die DSGVO sieht die Bestellung eines Datenschutzbeauftragten vor, wenn ein Unternehmen in irgendeiner Form eine automatisierte Verarbeitung von personenbezogenen Daten vornimmt. Bei einer Steuerberatungskanzlei werden vor allem die personenbezogenen Daten von Mandanten, aber auch der Mitarbeiter und anderer Dritter (Behörden, externe Dienstleister etc.) automatisiert bearbeitet.

Hinweis
Eine automatisierte Verarbeitung personenbezogener Daten liegt stets vor, wenn jemand am PC, Laptop oder sonst mit einem EDV-Gerät mit Daten von Menschen umgeht. Ob diese Tätigkeit bezahlt wird, ist im Übrigen unerheblich,

Dies allein führt noch nicht dazu, dass ein Datenschutzbeauftragter bestellt werden muss. Vielmehr müssen noch weitere Faktoren hinzukommen. Zum einen spielt die Zahl der Mitarbeiter eine Rolle. So hat der deutsche Gesetzgeber bestimmt, dass ein Datenschutzbeauftragter zu bestimmen ist, wenn in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Bei der Berechnung ist die Zahl der Köpfe, nicht die Zahl der Stellen maßgeblich.

Beispiel
In einer Steuerkanzlei arbeiten zwölf Voll- und Teilzeitmitarbeiter, die ständig am PC mit Mandantendaten umgehen. Ihre Arbeitszeit ergibt zusammengerechnet lediglich eine Arbeitszeit von sieben Vollzeitbeschäftigten. Dennoch sind „mindestens zehn Personen“ (nämlich zwölf) damit beschäftigt, personenbezogene Daten zu verarbeiten.

Verarbeiten in einer Kanzlei tatsächlich weniger als zehn Mitarbeiter regelmäßig personenbezogene Daten, liegt die Umsetzung sämtlicher datenschutzrelevanter Themen in den Händen der Kanzleileitung. An dieser Vorgabe ändert sich ab 25.05.2018 im Grunde nichts.
Unabhängig der Beschäftigtenzahl kann eine Pflicht zur Bestellung eines Datenschutzbeauftragten in einem Unternehmen aus der besonderen Art der Daten (aus denen z.B. politische Meinungen, religiöse oder weltanschauliche Überzeugungen hervorgehen) resultieren. Die einschlägigen gesetzlichen Regelungen sind in Art. 37 Abs. 1 DSGVO und § 38 BDSG-neu enthalten. Sie ergänzen sich.
In formaler Hinsicht ist nicht vorgeschrieben, dass die Benennung schriftlich erfolgt, doch empfiehlt es sich, sie schriftlich durchzuführen. Denn nur aus einer schriftlichen Bestellung lässt sich gegenüber der Aufsichtsbehörde nachweisen, dass zu jedem Zeitpunkt tatsächlich der Datenschutzbeauftragte benannt war.
Der Datenschutzbeauftragte genießt einen besonderen Kündigungsschutz. So darf ihm während der Bestellung bzw. bis ein Jahr nach Beendigung der Bestellung nur aus wichtigem Grund (z.B. bei einer Arbeitsverweigerung) gekündigt werden.

5.2 Freiwillige Bestellung

Auch wenn aufgrund der niedrigen Beschäftigtenzahl die Benennung eines Datenschutzbeauftragten gesetzlich im Einzelfall nicht vorgeschrieben ist, eröffnet Art. 37 Abs.4 Satz 1 Halbsatz 1 DSGVO) die Möglichkeit, auch freiwillig einen Datenschutzbeauftragten zu benennen. Arbeitsrechtlich zu beachten ist, dass der besondere Kündigungsschutz nicht für freiwillig bestellte Datenschutzbeauftragte gilt.

5.3. Interner oder externer Datenschutzbeauftragter

Wenn in einer Kanzlei ein Datenschutzbeauftragter benannt werden muss bzw. soll, lässt Art. 37 Abs. 6 DSGVO zwei Varianten zu:

- Variante1: Ein eigener Mitarbeiter wird mit dieser Funktion beauftragt.
- Variante 2: Ein externer Dienstleister wird beauftragt.

Der bestellte Datenschutzbeauftragte muss in jedem Fall über die erforderliche Fachkunde verfügen. Das Maß der erforderlichen Fachkunde bestimmt sich nach dem Umfang der Datenverarbeitung und dem Schutzbedarf der personenbezogenen Daten (§ 4 f II Satz 2 BDSG). Eine besondere berufliche Qualifikation wird nicht vorausgesetzt.
Grundsätzlich kann in einer Kanzlei von einem hohen Schutzbedarf ausgegangen werden, weshalb auch das Know-how des Datenschutzbeauftragten im Hinblick auf die eingesetzten IT-Systeme und ihre entsprechende Absicherung überdurchschnittlich sein sollte. Die Bestellung eines kanzleiinternen Datenschutzbeauftragten ist also nur bedingt zu empfehlen.
Dem internen Datenschutzbeauftragten ist zum Erhalt der Fachkunde die Teilnahme an Schulungs- und Fortbildungsveranstaltungen zu ermöglichen. Die Kosten hierfür hat der Kanzleiinhaber zu tragen.
Ein eigener Mitarbeiter kann die Funktion als Datenschutzbeauftragter neben anderen Aufgaben und Pflichten wahrnehmen (Art. 38 Abs. 6 DSGVO), wobei allerdings darauf zu achten ist, dass es nicht zu einem Interessenkonflikt kommt (Art. 38 Abs. 6 Satz 2 DSGVO).
So dürfen Kanzleiinhaber selber nicht bestellt sein, was sich aus § 4 f Abs. 3 Satz 1 BDSG ergebt. Zur Vermeidung von Interessenskonflikten sollten auch keine IT- und Personalverantwortliche sowie IT-Systemadministratoren als Datenschutzbeauftragten bestellt werden.

5.4 Aufgaben des Datenschutzbeauftragten

Der Datenschutzbeauftragte ist dem Kanzleiinhaber unmittelbar zu unterstellen und in der Ausübung seiner Fachkunde weisungsfrei. In Bezug auf die Aufgaben in der Kanzlei vermeidet die DSGVO einen umfassenden Aufgabenkatalog. Vielmehr legt sie lediglich einige Hauptaufgaben fest:

- Unterrichtung und Beratung des Kanzleiinhabers und der Mitarbeiter hinsichtlich ihrer Pflichten nach dem Datenschutzrecht
- Überwachung der Einhaltung der gesetzlichen Datenschutzvorschriften
- Beratung im Zusammenhang mit Datenschutz-Folgenabschätzungen
- Zusammenarbeit mit der Aufsichtsbehörde
- Anlaufstelle für die Aufsichtsbehörde in Fragen, die mit der Verarbeitung personenbezogener Daten zusammenhängen
- Beratung betroffener Personen nach Art. 38 Abs. 4 DSGVO

Der Datenschutzbeauftragte kann zur Klärung von Fragen unmittelbar mit der Aufsichtsbehörde kommunizieren.

Beispiel
Die Überwachungspflicht des Datenschutzbeauftragten hat nicht zur Folge, dass er im Fall der Nichteinhaltung von Datenschutzvorschriften persönlich zur Verantwortung gezogen werden kann. Die Verantwortung für den Umgang mit personenbezogenen Daten i einer Kanzlei verbleibt bei ihrem Inhaber. Datenschutz ist und bleibt Chefsache.

5.4. Pflichten des Datenschutzbeauftragten

Auch für den Datenschutzbeauftragten in einer Kanzlei bestehen eine Reihe von Pflichten, die er beachten muss:

- **Zeugnisverweigerungs- und Schweigepflicht:** Der Datenschutzbeauftragte ist grundsätzlich nach § 4 f IV BDSG berechtigt und verpflichtet über die Identität und die näheren Umstände des Betroffenen Stillschweigen zu bewahren. Stillschweigen betrifft in diesem Zusammenhang den Fall, dass ein (Nicht-)Betroffener sich an den Datenschutzbeauftragten wendet. Es besteht ein Beschlagnahmeverbot für Akten und andere Schriftstücke des Datenschutzbeauftragten.
- **Recht zur Verschwiegenheit**: Der Datenschutzbeauftragte ist gegenüber dem Kanzleiinhaber zur Verschwiegenheit verpflichtet, es sei denn, seine Auskünfte dienen der Klärung von Unregelmäßigkeiten innerhalb der Verarbeitung von personenbezogenen Daten.
- **Strafbewehrte Schweigepflicht der mandantenbezogenen Datenverarbeitung**: Nach § 4 f Abs. 4a BDSG wird der Schutz des Berufsgeheimnisses mit einem Zeugnisverweigerungsrecht des Datenschutzbeauftragten ergänzt. Allerdings entscheidet der Kanzleiinhaber, ob und in welchem Umfang der Datenschutzbeauftragte dieses Recht ausüben darf.

5.5. Meldung an die Aufsichtsbehörde

Der Inhaber der Kanzlei muss die Kontaktdaten des Datenschutzbeauftragten der Aufsichtsbehörde mitteilen (Art. 37 Abs. 7 DSGVO). In vielen Fällen stellen die Aufsichtsbehörden für diese Meldung ein Online-Formular zur Verfügung.

5.6. Veröffentlichung der Kontaktdaten des Datenschutzbeauftragten

Das Gesetz sieht vor, dass der Kanzleiinhaber die Kontaktdaten des Datenschutzbeauftragten veröffentlicht. Auf diese Weise soll ermöglicht werden, dass sich Betroffene an den Datenschutzbeauftragten wenden können. Sinnvollerweise geschieht eine solche Veröffentlichung im Internet. Es genügt hierbei die Angabe der E-Mail-Funktionsadresse.
Dabei muss sichergestellt werden, dass Eingänge unter dieser Adresse regelmäßig abgerufen werden und dass diese auch nur vom Datenschutzbeauftragten oder seinem Vertreter gelesen werden können.

6. Rechte der betroffenen Personen

Natürliche Personen, deren Daten verarbeitet werden und deren Persönlichkeitsrechte Schutzobjekte des BDSG und der DSGVO sind, werden als „betroffene Personen“ bezeichnet. Betroffene Personen können Mitarbeiter, Mandanten oder der Ansprechpartner von Dienstleistern oder Behörden sein. Den betroffenen Personen räumt die DSGVO Transparenz- und Interventionsrechte ein.

6.1. Recht auf Benachrichtigung

Betroffene besitzen ein Anrecht darauf, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache" (vgl. Art. 12 Abs. 1 DSGVO) darüber informiert zu werden, was zu welchem Zweck mit den personenbezogenen Daten gemacht werden soll. Und zwar bevor es tatsachlich passiert. Konkret muss der Betroffene vor allem darüber informiert werden:

- Namen und Kontaktdaten des Verantwortlichen,
- Kontaktdaten eines vorhandenen Datenschutzbeauftragten,
- Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen inklusive die Angabe der dafür notwendigen Rechtsgrundlage,
- Angabe zur Dauer der Speicherung der Daten oder Kriterien für die Datenlöschung,
- Empfänger der Daten, wenn der Verantwortliche sie weitergeben möchte,
- Hinweis auf Beschwerderecht bei der Aufsichtsbehörde,
- Hinweis auf Recht auf Auskunft, Berichtigung, Löschung usw.,
- Hinweis darauf, dass eine Einwilligung jederzeit grundlos widerrufen werden kann und
- Interessen des Verantwortlichen, wenn er Daten auf der Basis einer Interessenabwägung verarbeiten möchte

6.2. Recht auf Auskunft

Eine Auskunft ist nicht automatisch zu erteilen, sondern nur, wenn ein konkreter Antrag vorliegt. Wichtig ist dabei, dass man sich als Verantwortlicher darüber vergewissert, dass der Antragsteller der ist, der er vorgibt, zu sein. Nur wenn man eine hinreichende Sicherheit darüber hat, dass es der richtige Antragsteller ist, darf man die entsprechende Auskunft erteilen.

In einer Kanzlei, in der die elektronische Speicherung der Daten auf einem PC oder einem kleinen Netzwerk erfolgt, sollte es relativ leicht möglich sein, den Anspruch auf Auskunft zu erfüllen. In jedem Fall besteht eine kostenlose Auskunftspflicht gegenüber dem Antragsteller.

Nur wenn der Antragsteller weitere Kopien haben möchte, kann der Verantwortliche dafür ein angemessenes Entgelt verlangen.

Dem Antragsteller ist zumindest eine schriftliche Abschrift der gespeicherten personenbezogenen Daten oder eine elektronische Zusammenfassung zu übermitteln.

Diese Zusammenfassung muss enthalten:

- die zur Person des Betroffenen gespeicherten Daten, einschließlich der Angabe, woher sie stammen,
- Zweck der Datenverarbeitung
- Kategorien personenbezogener Daten
- Datenempfänger

- geplante Speicherdauer
- Hinweis auf sonstige Betroffenenrechte und Beschwerdemöglichkeit bei der Aufsichtsbehörde

Wenn die auskunftspflichtige Stelle nicht oder und nur teilweise Auskunft erteilt, muss sie auf die Unvollständigkeit der Auskunft ausdrücklich hinweisen, damit der Betroffene eine Überprüfung verlangen kann.

6.3. Recht auf Einsichtnahme

Eine Kanzlei hat eine Übersicht über ihre automatisierten Verarbeitungen personenbezogener Daten zu führen hat. Diese Übersicht kann von jedermann unentgeltlich eingesehen werden.
Es ist Aufgabe des Datenschutzbeauftragten, auf Antrag die Angaben in dem Verfahrensverzeichnis dem Antragsteller in geeigneter Weise verfügbar zu machen. Auch eine Kanzlei ohne betrieblichen Datenschutzbeauftragten muss eine entsprechende Übersicht führen und zur Einsicht bereithalten. Bis auf die allgemeine Beschreibung, die es ermöglicht, die Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung zu beurteilen, sind alle Angaben öffentlich.

6.4. Recht auf Berichtigung

Der Anspruch bezieht sich auf die Korrektur falscher Daten. Jede Kanzlei ist verpflichtet, unrichtige Daten zu berichtigen. Es liegt aber auch am Betroffenen selbst, darauf hinzuweisen, wenn Daten unrichtig oder überholt sind. Geschätzte Daten müssen als solche deutlich gekennzeichnet werden.
Besteht Streit darüber, ob die Daten richtig oder unrichtig sind, hat die betroffene Person einen Anspruch auf Einschränkung der Verarbeitung. Der Verantwortliche darf die Daten dann zwar noch speichern, aber nicht mehr in sonstiger Art und Weise verarbeiten, also beispielsweise einem Dritten übermitteln oder für Werbezwecke nutzen.
Als Nachweis der Berichtigung kann der Verantwortliche dem Betroffenen die aktualisierten Daten mitteilen.

6.5. Recht auf Löschung

Eine Kanzlei hat personenbezogene Daten zu löschen, wenn:

- die Speicherung unzulässig ist,
- die erteilte Einwilligung zur Datenspeicherung widerrufen wurde,
- es sich um Daten über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit, über Gesundheit oder das Sexualleben, strafbare Handlungen oder Ordnungswidrigkeiten handelt und ihre Richtigkeit von der verantwortlichen Stelle nicht bewiesen werden kann, oder
- für eigene Zwecke verarbeitete Daten für die Erfüllung des Speicherungszwecks nicht mehr erforderlich sind,
- geschäftsmäßig zum Zweck der Übermittlung verarbeitete Daten aufgrund einer am Ende des vierten Kalenderjahres nach der ersten Speicherung vorzunehmenden Prüfung nicht mehr erforderlich sind; soweit es sich um Daten über erledigte

Sachverhalte handelt, muss bereits zum Ende des dritten Kalenderjahres nach der ersten Speicherung die Löschverpflichtung überprüft werden.

Eine Löschung ist nur für personenbezogene Daten vorgesehen, die entweder aus automatisierter Datenverarbeitung stammen oder aus einer manuellen Datei, jedoch nicht für einzelne Daten, die in nicht dateimäßig strukturierten Akten festgehalten sind. Sind allerdings komplette Akten unzulässig angelegt, so sind sie ebenfalls zu vernichten. Ebenso ist im Allgemeinen mit nicht mehr erforderlichen Akten zu verfahren.
Als besondere Ausformung des Löschungsanspruches wurde mit der DSGVO ein „Recht auf Vergessenwerden“ eingeführt. Dieses Recht greift, wenn die verantwortliche Stelle die zu löschenden Daten öffentlich gemacht hat (z. B. im Internet). Dann muss sie vertretbare Schritte unternehmen, um die Stellen, die diese Daten verarbeiten, zu informieren, dass die betroffene Person von ihnen die Löschung aller Links zu diesen Daten oder von Kopien oder Replikationen verlangt.
Wenn ein Verantwortlicher zu löschende personenbezogene Daten öffentlich gemacht hat, muss er andere Verantwortliche, die diese Daten verarbeiten, davon informieren, dass eine betroffene Person von ihnen die Löschung aller Links zu oder aller Kopien oder Replikationen von diesen personenbezogenen Daten verlangt hat.

Beispiel
Eine Kanzlei sollte die veränderten Anforderungen bei den Löschpflichten in ihren Löschkonzepten präzise abbilden, um künftig nachweisen zu können, dass sie die Vorgaben der DSGVO einhalten.

Als Nachweis der Datenlöschung kann, da die Daten nicht mehr vorhanden sind, lediglich eine Information darüber dienen, dass die Daten gelöscht wurden.

6.6. Recht auf Sperrung

Personenbezogene Daten sind immer dann zu sperren, wenn einer fälligen Löschung besondere Gründe entgegenstehen, etwa bei

- gesetzlich, satzungsmäßig oder vertraglich festgelegten **Aufbewahrungsfristen**,
- schutzwürdigen Interessen des Betroffenen, etwa weil ihm Beweismittel verloren gingen, oder
- ein unverhältnismäßig hoher Aufwand wegen der besonderen Art der Speicherung.

Personenbezogene Daten sind zu sperren, wenn der Betroffene ihre Richtigkeit bestreitet und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt. Die Tatsache dieser Sperrung darf dann gleichfalls nicht übermittelt werden.
Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur übermittelt oder genutzt werden, wenn dies

- zu wissenschaftlichen Zwecken,
- zur Behebung einer bestehenden Beweisnot oder
- aus sonstigen im überwiegenden Interesse der verantwortlichen Stelle oder eines Dritten liegenden Gründen

unerlässlich ist.

Zusätzlich schreibt das Gesetz vor, dass gesperrte Da-ten nur ausnahmsweise und nur dann für die genannten Zwecke übermittelt oder genutzt werden dürfen, wenn dies auch ohne Sperrung erlaubt wäre.

6.7. Recht auf Datenübertragbarkeit

Als einziges wirklich neues Betroffenenrecht der DSGVO gilt nunmehr das Recht auf Datenübertragbarkeit. Es räumt dem Betroffenen unter bestimmten Voraussetzungen einen Anspruch ein, eine Kopie der ihn betreffenden personenbezogenen Daten in einem üblichen und maschinenlesbaren Dateiformat zu erhalten. Der Nutzer hat das Recht, Daten von einem Anbieter zu einem anderen „mitzunehmen“. Die Regelung kann damit vor allem den Wechsel des Mandanten zwischen Kanzleien erleichtern. Es gilt aber letztlich bei jeder automatisierten Verarbeitung personenbezogener Daten die Notwendigkeit einer Einwilligung oder einer Vertragsbeziehung mit dem Betroffenen. Das Recht auf Datenübertragbarkeit ist auf die Daten beschränkt, die die betroffene Person dem Verarbeiter zur Verfügung gestellt hat.

6.8. Recht auf Widerspruch gegen die Datenverarbeitung

Wenn sich ein Verantwortlicher als Rechtfertigung für seine Datenverarbeitung auf eine Interessenabwägung beruft, kann eine betroffene Person dieser Verarbeitung widersprechen, muss dafür aber plausible Gründe nennen. Nur dann, wenn der Verantwortliche in Kenntnis dieser (neuen) Gründe des Betroffenen zwingende schutzwürdige eigene Gründe nachweisen kann, darf er die Verarbeitung fortsetzen.

6.9. Recht, keiner automatisierten Entscheidung unterworfen zu werden

Betroffene besitzen auch das Recht, dass ihre Daten nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, die einer betroffenen Person gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Das bedeutet konkret, dass der Betroffene in aller Regel einen Anspruch darauf hat, dass nicht ein Computer alleine darüber entscheiden darf, wie mit seinen personenbezogenen Daten umgegangen wird bzw. welche Konsequenzen aus einer Verarbeitung gezogen werden. Das gilt vor allem dann nicht, wenn es eine Rechtsvorschrift gibt, die dies erlaubt oder anordnet oder wenn die betroffene Person ausdrücklich dazu eingewilligt hat.
Bei einer Kanzlei dürfte dieser Fall von untergeordneter Bedeutung sein, da in der Regel noch eine individuelle Kommunikation stattfinden wird.

7. Verletzung des Schutzes personenbezogener Daten

Bei einer Verletzung des Schutzes personenbezogener Daten muss der Verantwortliche dies im Normalfall unaufgefordert der zuständigen Aufsichtsbehörde melden (Art. 33 Abs. 1 Satz 1 DSGVO). Im Fall des Unterlassens einer Meldung droht unabhängig eines nachweisbaren Schadens für den Betroffenen ein erhebliches Bußgeld (Art. 83 Abs. 4 Buchstabe a DSGVO).

Hinweis
Die Verletzung des Schutzes personenbezogener Daten ist eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von bzw. zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

Als Verletzungsfolgen eines datenschutzrechtlichen Verstoßes kommen in Betracht:

- die Vernichtung der Daten,
- der Verlust der Daten,
- die Veränderung der Daten,
- die unbefugte Offenlegung der Daten,
- der unbefugte Zugang zu den Daten

Es kommt nicht darauf an, um welche Art von Daten es sich handelt, solange sie personenbezogen sind. Daher muss es sich auch nicht um besondere Kategorien von Daten im Sinne von Art. 9 DS-GVO handeln (z.B. Gesundheitsdaten). Es spielt auch keine Rolle, ob die Verletzung der Sicherheit absichtlich oder unbeabsichtigt erfolgt ist. Außerdem muss Verletzung nicht bedeuten, dass es zu einem Schaden für die betroffene Person kommen wird oder kann.

Beispiel:
Eine angestellte Steuerberaterin hat Zugriff auf alle Mandantendaten, die in der Kanzlei vorhanden sind. Deshalb kann sie auch auf Daten von Mandanten zugreifen, mit deren Bearbeitung sie nach der internen Arbeitsverteilung gar nichts zu tun hat. Die Daten wurden der Steuerberaterin damit unbefugt offengelegt. Damit konnte sie auch potentiell unbefugt Zugang zu den Daten erhalten. Es zählt also nicht, ob sie diese auch wirklich angesehen haben. Es liegt eine Verletzung des Schutzes personenbezogener Daten vor.

Wenn es zu einer Verletzung des Schutzes personenbezogener Daten gekommen ist, muss dies der Verantwortliche unverzüglich an die Aufsichtsbehörde melden (Art. 33 Abs. 1 Satz 1 DSDVO). Unverzüglich bedeutet, dass der Verantwortliche ohne schuldhaftes Zögern innerhalb von 72 Stunden handeln muss. Eine Ausnahme besteht, wenn die Verletzung voraussichtlich nicht zu keinem Risiko für die persönlichen Rechte und Freiheiten des Betroffenen (etwa aufgrund einer geeigneten Verschlüsselung) führt.
Der Betroffene, dessen Schutz personenbezogener Daten verletzt wurde, muss hiervon informiert werden, wenn die Schutzverletzung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten dieser Person zur Folge hat (Art. 34 Abs. 1 DS-GVO).

8. Sanktionen und Haftung

Verstöße gegen den Datenschutz können ernsthafte rechtliche Folgen nach sich ziehen. Die DSVO hat die bisher geltenden Regelungen deutlich verschärft, was sowohl im Hinblick auf denkbare Geldbußen als auch im Hinblick auf Schadensersatz einschließlich Schmerzensgeld gilt.
Die DSGVO enthält Bestimmungen für Geldbußen (Art. 83 DSGVO) und Bestimmungen für das Recht auf Schadensersatz (Art. 82 DSGVO). Sie werden ergänzt durch Regelungen des BDSG-neu (§ 42 BDSG-neu/Strafvorschriften und § 43 BDSG-neu/Bußgeldvorschriften).

8.1. Konsequenzen für die Kanzlei

Bußgeld

Die DSGVO sieht eine maximale Geldbuße von bis zu 20 Mill. Euro oder bis zu 4% des gesamten weltweit erzielten Jahresumsatzes im vorangegangenen Geschäftsjahres vor; je nachdem, welcher Wert der höhere ist. Es gilt der Jahresumsatz des gesamten Unternehmens, nicht der der einzelnen juristischen Person.

Bußgeldbemessung:

Zur Bemessung des Bußgeldes gibt es einen Katalog mit Kriterien in Art. 83 Abs. 2 (a) bis (k) DSGVO. Entscheidend sind:

- Art, Schwere und Dauer des Verstoßes
- Vorsätzlichkeit oder Fahrlässigkeit
- die vorgenommenen Maßnahmen zur Minderung des entstandenen Schadens
- Verantwortungsgrad unter Berücksichtigung aller getroffenen Maßnahmen
- etwaige einschlägige frühere Verstöße
- Umfang der Zusammenarbeit mit der Aufsichtsbehörde
- Kategorien personenbezogener Daten, die von dem Verstoß betroffen sind
- Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, insbesondere Selbstanzeige
- Einhaltung früher angeordneter Maßnahmen
- Einhaltung genehmigter Verhaltensregeln
- alle anderen Umstände des Einzelfalles (u.a. finanzielle Vorteile)

Schadensersatzpflicht

Wenn eine betroffene Person durch unzulässige oder unrichtige Datenerhebung, Verarbeitung oder Nutzung einen Schaden erleidet, ist das Unternehmen/Kanzlei schadensersatzpflichtig. Das kann auch ein immaterieller Schaden (z.B. Rufschädigung) sein.

Eine Exkulpierung ist nur möglich, wenn durch einen Dienstleister nachweisen werden kann, dass das Unternehmen/Kanzlei für den Verstoß nicht verantwortlich ist.

Unternehmen/Kanzlei und Dienstleister der Auftragsdatenverarbeitung haften dabei gesamtschuldnerisch.

Gegenüber kleinen Unternehmen wie einer Kanzlei kommen Geldbußen in Millionenhöhe selbstverständlich nicht in Betracht. Doch auch sie müssen bei ernsthaften Verstößen mit Geldbußen in vier- oder fünfstelliger Höhe rechnen. Denn Geldbußen müssen „in jedem Einzelfall wirksam, verhältnismäßig und abschreckend“ sein (Art. 83 Abs. 1 DS-GVO).

8.2. Konsequenzen für den Kanzleimitarbeiter

Straftaten	Schadensersatzpflichten	Arbeitsrechtliche Sanktionen
Strafrechtlich relevante Verstöße gegen den Datenschutz werden mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft. Antragsberechtigt ist nicht nur der Betroffene, sondern auch die Aufsichtsbehörde und das Unternehmen.	Auch für den verantwortlichen Mitarbeiter bestehen unter Umständen gegenüber seinem Arbeitgeber Schadensersatzpflichten, wenn er sich nicht an seine Pflichten zur Beachtung des Datenschutzes gehalten hat.	Verstöße gegen den Datenschutz können für den Mitarbeiter auch arbeitsrechtliche Konsequenzen von der Abmahnung bis zur Kündigung haben.

9. Aufsichtsbehörden

Die Datenschutzaufsichtsbehörden werden durch die DSGVO mit einer Reihe neuer Aufgaben betraut. Hierzu gehört u.a., dass sie bei Feststellung von Datenschutzverstößen die Befugnis besitzen, Geldbußen bis zu einer Höhe von 20.000.000 Euro festzusetzen. In ihrer Rechtsposition sind Aufsichtsbehörden völlig unabhängig, was bedeutet, dass sie selbst entscheiden, mit welcher Priorität sie ihre gesetzlichen Aufgaben erfüllen. Zu den Aufgaben der Aufsichtsbehörden gehören die:

- Überwachung und Durchsetzung der Anwendung der DSGVO
- Beratung von Unternehmen und Privatpersonen
- Anweisung, Verstöße abzustellen und künftig eine datenschutzrechtliche Verarbeitung durchzuführen
- Bearbeitung von Beschwerden von betroffenen Personen
- Kontrolle über die Anwendung der DSGVO
- Ahndung von datenschutzrechtlichen Verstößen mittels Geldbußen

Zur Erfüllung ihrer Aufgaben besitzen die Aufsichtsbehörden die Befugnis:

- Verantwortliche anweisen, alle Informationen bereitzustellen, die erforderlich sind, um die Einhaltung der Datenschutzvorschriften überprüfen zu können,
- zur Durchführung unangekündigter Datenschutzprüfung vor Ort (und am Computer) durchführen

Hinweis
Die Beschwerde eines unzufriedenen Kanzleimitarbeiters oder Mandanten kann sehr schnell dazu führen, dass die Aufsichtsbehörde vor der Kanzleitür steht und bei festgestellten Verstößen handelt bzw. handeln muss.

 © Deubner Verlag GmbH & Co. KG