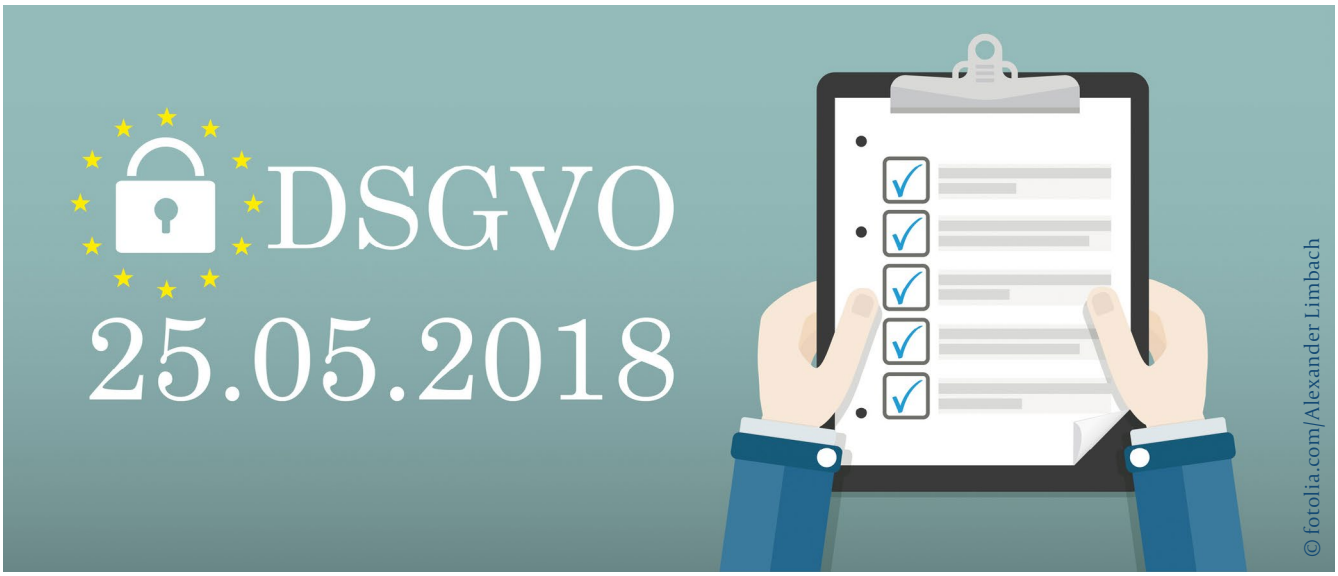
GRATIS

Fachinfo-Broschüre

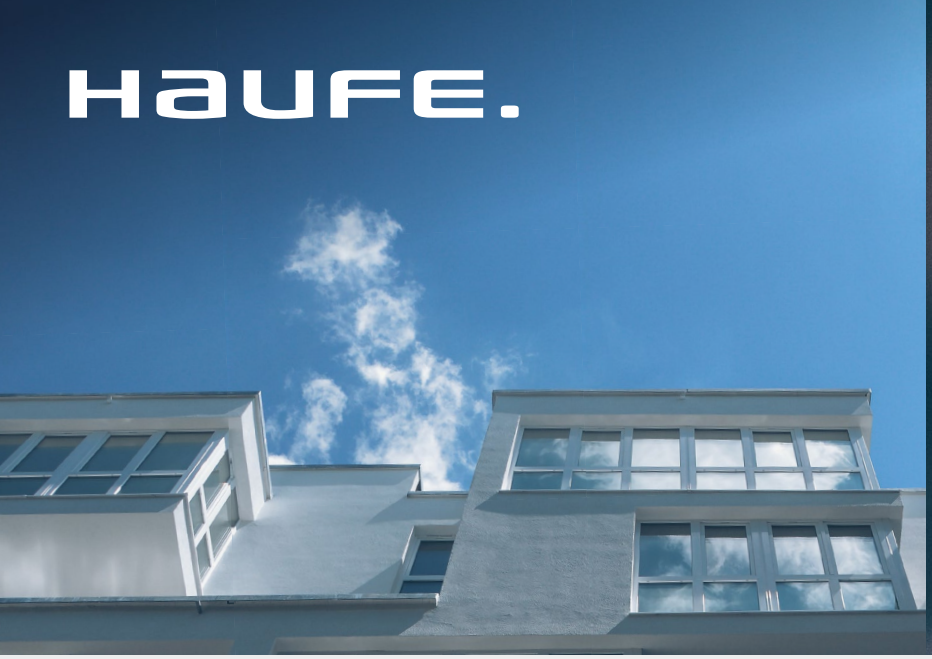


Dr. Astrid Auer-Reinsdorff/Kjell Vogelsang

DSGVO: Die fünf wichtigsten Sofortmaßnahmen für Anwaltskanzleien

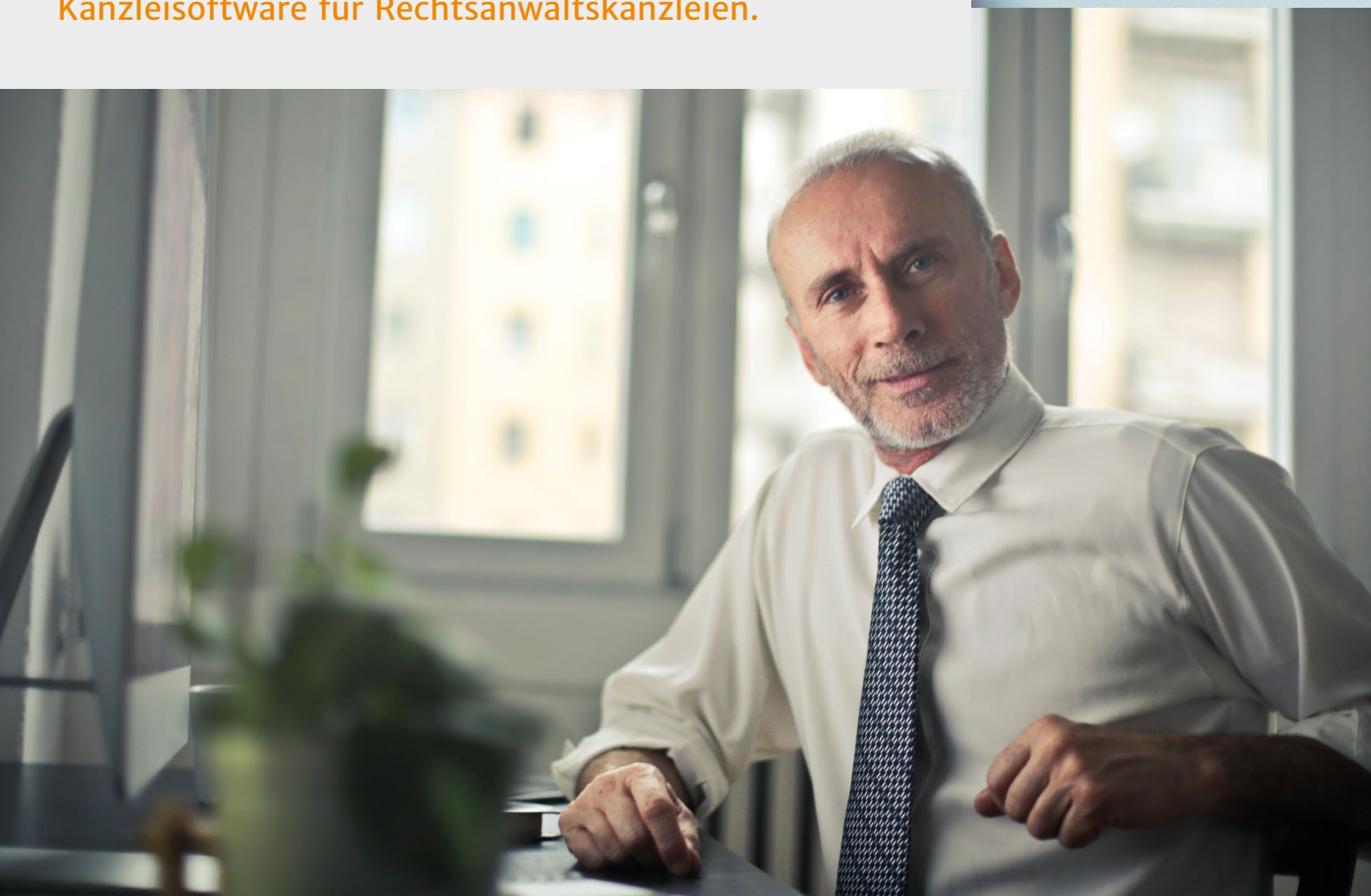
Eine Last Minute-Gebrauchsanleitung

HAUFE.



STÄRKEN VERBINDEN. ZUKUNFT GESTALTEN.

Haufe – Fachwissen, Online-Seminare und Kanzleisoftware für Rechtsanwaltskanzleien.



DSGVO: Die fünf wichtigsten Sofortmaßnahmen für Anwaltskanzleien

Eine Last Minute-Gebrauchsanleitung

Dr. Astrid Auer-Reinsdorff
Rechtsanwältin Dr. Astrid Auer-Reinsdorff ist GfA-Vorsitzende der Arbeitsgemeinschaft IT-Recht im DAV und seit rund 20 Jahren als Rechtsanwältin mit Schwerpunkt der gestaltenden Beratung tätig. Als Fachanwältin für IT-Recht berät sie sowohl KMU als auch börsennotierte Unternehmen in IT-Projekten sowie in allen Fragen der Digitalisierung.
www.auer-company.de

Kjell Vogelsang
Kjell Vogelsang ist Rechtsanwalt und Fachanwalt für IT-Recht. Er ist Gründer und Partner von Vogelsang Rechtsanwälte Partnerschaft, einer kleinen, hoch spezialisierten Kanzlei in Köln, die Mandanten bundesweit in allen rechtlichen Fragen der IT berät und vertritt. Kjell Vogelsang beherrscht verschiedene Programmiersprachen und administriert seit 20 Jahren seine eigenen Linux-Server und hostet seine eigene Kanzleisoftware. Er ist Speaker für die Themen IT-Recht, IT-Sicherheit und Projektmanagement sowie Dozent und Trainer für IT-Recht und gewerblichen Rechtsschutz.
www.vrae.de

Inhalt

Impressum
Copyright 2018 by
Freie Fachinformationen GmbH
Leyboldstr. 12
50354 Hürth
Anregungen und Kritik zu diesem Werk senden Sie bitte an info@ffi-verlag.de.
Autoren und Verlag freuen sich auf Ihre Rückmeldung.

ISBN: 978-3-96225-014-0

Satz
Helmut Rohde, Euskirchen

Bildquellennachweis
Cover: © fotolia.com/Alexander Limbach

Einleitung

Mit dem 25. Mai 2018 werden die Regelungen der Datenschutzgrundverordnung (DSGVO) nebst der Neufassung des nationalen Bundesdatenschutzgesetzes (BDSG) wirksam. Ein wahrlich bedeutender Schritt zur Realisierung eines europaweit harmonisierten Datenschutzrechts, das international Wirkung entfaltet und geeignet ist, sich Geltung gegenüber weltweit agierenden Unternehmen zu verschaffen.

Doch nicht nur die Konzerne sind gefragt. Jede datenverarbeitende Stelle ist damit aufgerufen, die bisherige Ausgestaltung der Datenschutzanforderungen zu prüfen und zu aktualisieren.

Gerade Anwaltskanzleien verarbeiten personenbezogene bzw. personenbeziehbare Daten zur Erbringung ihrer Dienstleistungen, Vertretung und Interessenwahrnehmung. Aus den Anforderungen des Mandatsgeheimnisses ergeben sich zwar Besonderheiten, aber für die Verarbeitungstätigkeit der Kanzleien sind die Relevanz der Datenschutzprinzipien und etwaige Abweichungen genau zu prüfen und zu dokumentieren. Für Kanzleien, die besondere personenbezogene Daten typischerweise z. B. in arbeits-, familien-, erb- und strafrechtlichen Fällen verarbeiten, sind weitergehende Schutzmaßnahmen zu erwägen.

Vermutlich haben Sie schon an vielen Stellen gelesen, dass nun dringend Aktualisierungsbedarf besteht, aber womöglich scheint die Aufgabe derart groß und umfangreich, dass die Kanzlei noch in der Phase der Anwendungsfragen feststeckt.

Diese Kurzbroschüre soll es Ihnen und Ihrem Team ermöglichen, die anstehenden Aufgaben konzertiert anzugehen und als Leitungsaufgabe dauerhaft im Sinne eines Datenschutzrisikomanagements in die Kanzleiprozesse einzuführen.

Datenschutz betrifft in den Kanzleien üblicherweise die Verarbeitung von Daten von:

- Mandanten, Interessenten, Newsletter-Abonnenten, Followern in sozialen Netzwerken, Lieferanten, Beschäftigten und Bewerbern

durch die Kanzlei bzw. technische und organisatorische Dienstleister.

Teile der Datenverarbeitung werden zusätzlich von den Anforderungen des Mandatsgeheimnisses oder aber auch dem Geheimnisschutz für die kanzleiinternen Kennzahlen, Know-how und Strategien geprägt. Deshalb sollte die Umsetzung der datenschutzrechtlichen Anforderungen immer auch an den besonderen Bedingungen der Arbeit als Berufsgeheimnisträger sowie dem Interesse am Schutz der Integrität der eigenen Daten der Kanzlei ausgerichtet sein.

DSGVO: Die fünf wichtigsten Sofortmaßnahmen für Anwaltskanzleien

Eine Last Minute-Gebrauchsanleitung

Maßnahmen zur Statuserfassung und Vorbereitung der DSGVO-Umsetzung

Zunächst stellt sich die Frage, inwieweit eine Datenschutzorganisation in der Kanzlei bereits etabliert ist. Zu einer Bestandsaufnahme für die Überführung in die Vorgaben der DSGVO gehören folgende Punkte:

a) Status der Datenschutzverantwortlichkeit: In einem ersten Schritt ist zu ermitteln, wer in der Vergangenheit für die Etablierung und Prüfung der Datenschutzthemen in der Kanzlei verantwortlich war. Unabhängig davon, ob in der Vergangenheit ein Datenschutzbeauftragter bestellt war, haben die Kanzleipartner zunächst deutlich zu machen, dass Datenschutz eine Leitungsaufgabe ist und in Zukunft darauf verstärkt geachtet werden soll. Unabhängig vom Stand der Vorarbeit sollten sukzessive die nachfolgenden Fragestellungen in der Organisation abgefragt und der Kanzleileitung zur Entscheidung über die zukünftige Datenschutzorganisation vorgestellt werden.

b) Status des Vertragsmanagements: In der Kanzlei sind die Informationen zu Verträgen einzuholen, deren Gegenstand die Verarbeitung von personenbezogenen Daten ist oder sein kann, ggf. auch nur durch Vereinbarung zur Fernwartung/Remotezugriff – und zwar unabhängig davon, ob die Vereinbarungen mündlich, schriftlich oder in Textform abgeschlossen wurden. Dies umfasst die Zusammenstellung aller eigenen oder fremdentwickelten Fachanwendungen zur Datenverarbeitung. Eine Zusammenstellung aller Kanäle, über die die Erhebung und Übermittlung von personenbezogenen Daten erfolgt, in einem Datenflussdiagramm (z. B. in einer Mindmap) ist hilfreich, um alle Schnittstellen zu Dritten zu ermitteln. Dabei ist besonders darauf zu achten, dass auch jeweils etwaige Subunternehmer der Dienstleister sowie freie Mitarbeiter erfasst werden. Zudem ist es für den Schutz der Geschäftsgeheimnisse der Kanzlei natürlich auch interessant, im Rahmen dieser Sichtung mit zu erheben, wo geheimhaltungsbedürftige Daten sonstiger Art ausgetauscht werden und/oder wo welche besonderen Vertraulichkeitsvereinbarungen für Berufsgeheimnisträger geschlossen wurden oder abzuschließen sind.

c) Status Auftragsverarbeitungsvereinbarungen: Hier ist zu erheben, zu welchen Dienstleistern/Dritten Vereinbarungen zur Verarbeitung von Daten im Auftrag geschlossen sind (Auftragsdatenverarbeitungsvereinbarungen ADV nach BDSG alt). Alle Vereinbarungen sind zentral zu erfassen, einschließlich der Anlagen TOM (= technische und organisatorische Maßnahmen). Wo Vereinbarungen nicht schriftlich abgeschlossen sind, wäre dies nach BDSG nachzuholen. Nach der DSGVO reicht zukünftig die Textform aus. Die Vereinbarungen heißen zukünftig Auftragsvereinbarungen (AVV) und die TOM sind individualisiert abzufassen, weshalb sie zukünftig auch als Schutzmaßnahmen bezeichnet

werden können. Sobald der Status erfasst ist, ist bei den Dienstleistern abzufragen, ob sie bereits DSGVO-Mustervereinbarungen für ihre Kunden vorbereitet haben, welche die Kanzlei nach Prüfung und ggf. Kontrolle der Datenverarbeitung sowie Anpassung der Beschreibung der Schutzmaßnahmen abschließen kann. Können einzelne Dienstleister eine solche Mustervereinbarung nicht anbieten, so handelt es sich meist um kleinere Dienstleister, welche die vom Kunden vorgelegten Vereinbarungen übernehmen möchten, oder aber der Dienstleister ist mit seiner Datenschutzorganisation nicht „up to date", sodass seine Zuverlässigkeit umso kritischer zu hinterfragen ist.

d) Status IT-Sicherheit: Ist ein IT-Sicherheitskonzept vorhanden sowie ein Risikomanagement? Wer ist für die laufende Überwachung und Aktualisierung zuständig? Sind alle IT-technischen Einrichtungen, also Hardware und Software, erfasst?

e) Verfahrensverzeichnis: Liegt ein öffentliches, umfassendes Verfahrensverzeichnis mit den eigenen technischen und organisatorischen Maßnahmen vor? Dieses Verzeichnis ist zu überarbeiten und in ein Verzeichnis der Verarbeitungstätigkeiten zu überführen. Unter bestimmten Bedingungen – besonders bei der Verarbeitung von besonderen personenbezogenen Daten – kann zusätzlich eine sog. Datenschutzfolgenabschätzung (DSFA) erforderlich werden.

f) Datenerhebung: Es sollten alle Wege der Datenerhebung erfasst sein sowie die Beschreibung der Dokumentation der Datenerhebung sowie die jeweilige Zweckbindung und eine ggf. erteilte Einwilligung. Typischerweise werden die Daten der Mandanten, Gegner, Zeugen und sonstigen Beteiligten am Mandat beim Mandanten telefonisch, per Webformular, per Papierformular in der Kanzlei bzw. per E-Mail erhoben. Soweit die Daten für die Begründung und Durchführung des Mandates erforderlich sind, bedarf es keiner Einwilligung, eine darüberhinausgehende Datenverarbeitung hingegen schon. Dies betrifft z. B. Newsletter-Abos sowie die Speicherung der Daten über das Ende des Mandats und gesetzliche Aufbewahrungspflichten hinaus.

g) Datenübermittlung: Ausfluss der Prüfung der Zweckgebundenheit ist die Frage der Übermittlung von Daten an Dritte außerhalb einer Auftragsvereinbarung. Hier ist zum Beispiel an die Übermittlung von Daten an eine andere Kanzlei zu denken, die außerhalb eines Mandates auf Empfehlung das Mandat in ihrem Tätigkeitsbereich übernehmen soll. Es ist auch darauf zu achten, dass in Kanzleikooperationen kein grundsätzliches Privileg für eine gemeinsame Verarbeitung besteht. Wie in einem Konzern bedarf es der Prüfung eines besonderen berechtigten Interesses, das die Interessen der Betroffenen überwiegt, um eine privilegierte gemeinsame Verarbeitung anzunehmen.

h) Schulungen: Ist eine Datenschutzschulung für alle Mitarbeiter vorgesehen? Die Verpflichtung der Mitarbeiter auf den Datenschutz sollte zur Einführung der DSGVO erneuert werden. Bei dieser Gelegenheit kann auch eine neue berufsrechtliche Verpflichtung vorgenommen werden.

i) Lizenzmanagement: Im Rahmen der Statusabfragen sollte auch erfasst werden, ob alle IT-Produkte hinreichend lizenziert sind und welche ggf. als Open Source-Lösung zum Einsatz kommen. Dabei sollte kritisch hinterfragt werden, ob die eingesetzten Programmversionen aktuell sind und den IT-Sicherheitsanforderungen genügen und/oder ggf. auch überflüssig sind und nicht genutzt werden.

Ausgangspunkt bei der Umstellung auf die DSGVO ist eine Bestandsaufnahme, ggf. mit Lücken, um diese alsbald nach Priorität und Risikoabwägung zu schließen. Zudem sollte eine Datenschutzsensibilisierung in dem Sinne erfolgen, dass dies nicht eine Aufgabe ist, die auf den Datenschutzbeauftragten „abgewälzt" wird, sondern jeder Beteiligter für seine Fachanwendung und

die Datenschnittstellen Erhebung, Verarbeitung und Übermittlung verantwortlich ist und die erforderlichen Informationen und Unterlagen bereitzustellen hat. Im Rahmen der Etablierung der DSGVO ist das alte Verfahrensverzeichnis in ein Tätigkeitsverzeichnis überzuführen. Neu ist die Impact Analyse, d. h. bei jeder Anwendung und jeder Verarbeitung ist deren Erforderlichkeit sowie die Erforderlichkeit des Umfangs der erhobenen Daten zu betrachten und zu begründen, weshalb kein geringerer Eingriff in die Rechte der Betroffenen zur Zweckerreichung möglich ist. Ein weiterer wichtiger Bestandteil ist das Erstellen eines Sperr- und Löschkonzeptes, das vorsieht, welche Daten wann und in welchem Umfang in ein Archivsystem vor finaler Löschung zu überführen sind und welche Daten sofort oder eben erst nach Ablauf von Aufbewahrungs- und Dokumentationspflichten zu löschen sind.

Die 5 wichtigsten Sofortmaßnahmen

Einige Kanzleien beginnen mit dem Wirksamwerden der DSGVO überhaupt erst damit, eine Datenschutzorganisation zu etablieren. Statuserfassung und umfassende Aufarbeitungen können schon aus zeitlichen Gründen vor dem 25. Mai 2018 nicht mehr gelingen. Dann empfehlen wir, zumindest folgende fünf Maßnahmen umzusetzen:

1. Datenschutzbeauftragte, Datenschutzfolgenabschätzung
2. Datenschutzerklärung
3. Datenschutzverpflichtung der Mitarbeiter
4. Verpflichtung der externen Dienstleister/ Auftragsverarbeiter
5. Verschlüsselung prüfen und anbieten

1. Datenschutzbeauftragter, Datenschutzfolgenabschätzung

Jede Rechtsanwaltskanzlei muss die Regeln der DSGVO und des neuen BDSG beachten, unabhängig von der Größe und der Art der verarbeiteten Daten. Von der Größe und der Art der Datenverarbeitung hängt jedoch die Pflicht ab, einen Datenschutzbeauftragten zu bestellen.

Ein bestellter Datenschutzbeauftragter unterrichtet und berät den Verantwortlichen, sprich die Kanzlei, er überwacht die Einhaltung des Datenschutzrechts und er arbeitet mit dem oder der Landesdatenschutzbeauftragten zusammen. Seine Bestellung ist der Aufsichtsbehörde anzuzeigen und zu veröffentlichen, Art. 37 Abs. 7 DSGVO.

Der Datenschutzbeauftragte bedarf besonderer **Sachkunde**. Diese Sachkunde setzt sich zusammen aus:

- Kenntnissen im Datenschutzrecht,
- Kenntnissen der Datenverarbeitung im allgemeinen und
- Kenntnissen über die konkreten Datenverarbeitungsvorgänge bei der betroffenen Stelle.

Für den Nachweis der Sachkunde wird eine Vielzahl von Zertifizierungen angeboten. Gleichwohl ist eine solche **Zertifizierung** weder erforderlich noch ersetzt sie die Sachkunde. Die Anforderung an die Sachkunde steigt im Verhältnis zu Art und Umfang der Datenverarbeitung. Mit anderen Worten: Der Datenschutzbeauftragte muss jederzeit die konkrete Datenverarbeitung verstehen und rechtlich bewerten können.

Daneben muss der Datenschutzbeauftragte **unabhängig und frei von Interessenkollisionen** sein, Art. 38 Abs. 6 S. 2 DSGVO. Damit kommen folgende Personen von vornherein nicht in Betracht:

- Geschäftsführer,
- Gesellschafter,
- IT-Leiter,
- Bürovorsteher oder
- externe Dienstleister wie Rechtsanwälte, wenn sie die betroffene Stelle bereits als Rechtsanwalt beraten oder vertreten.

In kleinen und mittleren Kanzleien sind nicht selten alle Rechtsanwälte auch Partner. Das bedeutet, dass keiner der Rechtsanwälte Datenschutzbeauftragter werden kann. Einen angestellten Rechtsanwalt zum Datenschutzbeauftragten zu machen, begegnet keinen Bedenken. In der Regel scheuen kleine und mittlere Kanzleien jedoch den **besonderen Kündigungsschutz** für den Datenschutzbeauftragten.

Bei der Bestellung von Bürokräften zu Datenschutzbeauftragten stellt sich die Frage der Sachkunde. Es spricht jedoch nichts dagegen, Bürokräften eine entsprechende Sachkunde durch Fortbildung zu verschaffen. Inwieweit dies zum jeweiligen Talent und zur Lernbereitschaft passt, ist Frage der Personalführung. In der Regel werden kleine und mittlere Kanzleien auf **externe Datenschutzbeauftragte** zurückgreifen.

Grundsätzlich ist die Bestellung eines Datenschutzbeauftragten freiwillig. Es gibt jedoch einige Konstellationen, in denen eine **Pflicht zur Bestellung eines Datenschutzbeauftragten** besteht.

Der deutsche Gesetzgeber hat von seinem Recht Gebrauch gemacht, mittels Ausführungsgesetz die Regelungen der DSGVO zu ergänzen. Das Ausführungsgesetz ist das BDSG in neuer Fassung. In § 38 BDSG neu ist normiert, dass ein Datenschutzbeauftragter zu bestellen ist, wenn *„in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten (beschäftigt sind)"*.

Die Bestellung eines Datenschutzbeauftragten ist also Pflicht, wenn mindestens **zehn beschäftigte Personen** Daten **automatisiert verarbeiten**.

Der Begriff der beschäftigten Person ist nicht zu verwechseln mit dem Begriff des Arbeitnehmers. Vielmehr fallen alle Beschäftigungsverhältnisse unter diese Regelung, unabhängig davon, ob es sich um Arbeitnehmer, freie Mitarbeiter, Leiharbeitnehmer, Auszubildende oder Praktikanten handelt. Entscheidend ist allein die Anzahl der Personen, mitunter wird vom sogenannten **„Nasenprinzip"** gesprochen. Unerheblich ist demgemäß die Zahl der pro Woche gearbeiteten Stunden. Selbst eine Teilzeitkraft, die nur eine Stunde in der Woche tätig ist, zählt als eine volle Person.

Umstritten ist, ob Geschäftsführer, Vorstandsmitglieder, mitarbeitende Gesellschafter (mithin Partner einer Sozietät) oder unentgeltlich tätige Familienmitglieder unter den Begriff der beschäftigten Person fallen. Zum einen wird vertreten, dass solche Personen nicht beschäftigt sind im Sinne der Vorschrift. Andere Stimmen halten die Anzahl der mit der Datenverarbeitung beschäftigten Personen für maßgeblich. Gerade in kleinen Kanzleien sind es oft die Partner, deren Zählung zum Überschreiten der Grenze von zehn Personen führt. Die Frage, ob Partner Beschäftigte sind, ist für kleine Kanzleien damit wichtig. Wie bei vielen anderen offenen Fragen, wird es auch hier mutmaßlich einige Jahre dauern bis zu einer gerichtlichen Klärung. Es wird deshalb gut abzuwägen sein, aus anwaltlicher Vorsorge die Partner mitzuzählen bei der Ermittlung der 10-Personen-Grenze oder aber eine Beratungsanfrage bei der Aufsichtsbehörde zu stellen. In der Literatur wird auch in Frage gestellt, ob die neue Regelung nach dem BDSG europarechtskonform sei, da der nationale Gesetzgeber zwar weitere Voraussetzungen für das Erfordernis der Benennung eines DSB aufstellen könne, aber sich diese Kriterien wohl an den Regelungen der DSGVO messen sollen, welche den Umfang der Datenverarbeitung und das damit verbundene steigende Risiko im Blick haben.

Die 10-Personen-Regel betrifft sogenannte **nicht-öffentliche Stellen**. Es stellt sich mitunter die Frage, wer nicht-öffentliche Stelle ist. Einfach ist dies bei klassischen Sozietäten zu beantworten. Nicht-öffentliche Stelle ist die GbR, PartG und die GmbH (oder welche Rechtsform auch immer gewählt ist). Entsprechend einfach ist es, die Zahl der Beschäftigten zur Beurteilung der 10-Personen-Grenze zu ermitteln. Irrelevant für die Beurteilung der 10-Personen-Grenze ist der arbeitsrechtliche Begriff des Betriebs. Es ist unerheblich, wo die Beschäftigten ihre Tätigkeit ausführen. Demgemäß gilt die Grenze auch einheitlich für die **gesamte Sozietät**, wenn es sich um eine überörtliche Sozietät handelt. Auch Beschäftigte, die ausschließlich von zu Hause aus arbeiten, werden mitgezählt.

Weitaus schwieriger zu beurteilen ist die Frage bei **Bürogemeinschaften**. Unabhängig von den berufsrechtlichen Fragen der Scheinsozietät, Interessenkollision, des Parteiverrats und des Verstoßes gegen die Verschwiegenheitsverpflichtung. Die datenschutzre-

levante Frage lautet, ob eine Bürogemeinschaft aus mehreren nicht-öffentlichen Stellen besteht oder eine einzige nicht-öffentliche Stelle ist. Dies kann maßgeblich dafür sein, ob ein Datenschutzbeauftragter zu bestellen ist. Eine Bürogemeinschaft überschreitet die 10-Personen-Grenze deutlich eher als jedes Mitglied der Bürogemeinschaft für sich genommen.

Eine pauschale Beurteilung von Bürogemeinschaften ist jedoch nicht möglich. Es hängt stark von den gemeinsam genutzten Ressourcen ab, konkret von der daraus resultierenden **gemeinsamen** Datenverarbeitung. Bürogemeinschaften, die sich darin erschöpfen, gemeinsame Räumlichkeiten zu unterhalten, dürften keine gemeinsame nicht-öffentliche Stelle darstellen. In einem solchen Fall unterhalten alle Mitglieder der Bürogemeinschaft eigene Telefonanschlüsse, eigene EDV und eigene Aktenschränke. Jeder Datenverarbeitungsvorgang ist damit separat zu beurteilen.

Es gibt jedoch auch Bürogemeinschaften, die versuchen, durch stärkere Zusammenarbeit Synergie-Effekte zu erzeugen. Eine **Zusammenarbeit in der Datenverarbeitung** kommt zum Beispiel in Betracht bei

- Nutzung eines gemeinsamen Telefonanschlusses,
- Nutzung einer gemeinsamen Telefonnummer,
- Nutzung eines gemeinsamen Webservers/eines gemeinsamen E-Mail-Servers,
- Nutzung eines gemeinsamen Netzwerks,
- Nutzung eines gemeinsamen internen Servers,
- Nutzung eines gemeinsamen Datenbestandes u.v.m.

In § 2 Abs. 4 BDSG sind nicht-öffentliche Stellen definiert als *„alle natürlichen und juristischen Personen, Gesellschaften und anderen Personenvereinigungen des privaten Rechtes“*. Selbst wenn man bei einer Bürogemeinschaft davon ausgeht, dass im Außenauftritt jedes Mitglied rechtlich eigenständig agiert, so besteht in Bezug auf die Datenverarbeitung doch eine Rechtsbeziehung zu den anderen Mitgliedern der Bürogemeinschaft. In der Literatur wird vertreten, dass „Voraussetzung (…) lediglich das Vorliegen einer **rechtlichen organisatorischen Einheit** (ist).“ (Paal/Pauly, DS-GVO BDSG, 2. Auflage 2018, BDSG § 2, RN 11). Danach dürfte es sich bei einer Bürogemeinschaft, die auch gemeinsame Datenverarbeitung betreibt, um **eine** nicht-öffentliche Stelle im Sinne des § 38 BDSG neu handeln.

Auch eine Beurteilung gemäß DSGVO dürfte zu keinem anderen Ergebnis kommen. Der relevante Begriff heißt dort „Verantwortlicher“ und ist in Art. 4 Nr. 7 DSGVO definiert als *„eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle“*. Verantwortlicher ist dabei, wer *„tatsächlich die Entscheidung über Zweck und Mittel der Datenverarbeitung (trifft)“* (Sydow, Europäische Datenschutzgrundverordnung, DSGVO Artikel 4, Rn. 114).

Selbst wenn man zu dem Ergebnis käme, eine Bürogemeinschaft, die gemeinsam Daten verarbeitet, sei keine nicht-öffentliche Stelle und entsprechend nicht an einer einheitlichen 10-Personen-Grenze zu messen, so wäre die Bürogemeinschaft dann doch **wechselseitig Auftragsverarbeiter** für die einzelnen Mitglieder der Bürogemeinschaft. Die Pflicht zur Bestellung eines Datenschutzbeauftragten ergäbe sich dann aus der Stellung als Auftragsverarbeiter.

Im Zweifel ist also eine Bürogemeinschaft, in der insgesamt zehn Personen oder mehr mit automatisierter Datenverarbeitung beschäftigt sind und eine gemeinsame Datenverarbeitung stattfindet, verpflichtet, einen Datenschutzbeauftragten zu bestellen.

Die von der Zahl der Beschäftigten abhängige Pflicht zur Bestellung eines Datenschutzbeauftragten bezieht sich auf die **„automatisierte Verarbeitung“** von Daten. Eine Verarbeitung von Daten ist bereits dann automatisiert, wenn Datenverarbeitungssysteme zum Einsatz kommen. Mit anderen Worten: Es handelt es sich nicht um automatisierte Verarbeitung, wenn ausschließlich auf Papier gearbeitet wird.

Unabhängig von der Zahl der Beschäftigten muss ein Datenschutzbeauftragter bestellt werden, wenn

- Daten aus den **besonderen Kategorien** oder Daten über **Beschuldigte, Angeklagte und Verurteilte** („Daten über strafrechtliche Verurteilungen und Straftaten") verarbeitet werden,
- die **Kerntätigkeit** des Verantwortlichen daraus besteht und
- diese Datenverarbeitung **umfangreich** ist.

Besondere Kategorien von Daten sind legal definiert in Art. 9 Abs. 1 DSGVO:

- rassische und ethnische Herkunft,
- politische Meinungen,
- religiöse oder weltanschauliche Überzeugungen,
- Gewerkschaftszugehörigkeit,
- genetische Daten,
- biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person,
- Gesundheitsdaten,
- Daten zum Sexualleben oder der sexuellen Orientierung.

Je nach bearbeitetem Rechtsgebiet werden in Rechtsanwaltskanzleien nie, selten oder häufig Daten aus den besonderen Kategorien verarbeitet. In Betracht kommen zum Beispiel:

- im Verkehrsrecht, Medizinrecht, Familienrecht, Erbrecht und Sozialrecht Gesundheitsdaten;
- im Arbeitsrecht die Gewerkschaftszugehörigkeit sowie Gesundheitsdaten;
- im Strafrecht die rassische und ethnische Herkunft, genetische Daten, biometrische Daten, Gesundheitsdaten und auch Daten zum Sexualleben und der sexuellen Orientierung;
- im Migrationsrecht alle Kategorien in Verbindung mit dem Asylgrund der Verfolgung im Heimatland;
- Strafverteidiger werden stets Daten über Beschuldigte, Angeklagte und Verurteilte verarbeiten.

Um eine **Kerntätigkeit des Verantwortlichen** handelt es sich dann, wenn die Datenverarbeitung dem Geschäftszweck unmittelbar dient. Geschäftszweck einer Anwaltskanzlei ist die Beratung und Vertretung von Mandanten. Die Verarbeitung von Daten im Rahmen dieser Beratung und Vertretung dürfte also stets Kerntätigkeit sein. Von einer Nebentätigkeit dürfte demgegenüber auszugehen sein bei Verwaltungsaufgaben oder den Geschäftsprozess begleitenden Maßnahmen, wie zum Beispiel der Auswertung von Google Analytics. Als Faustregel kann gelten: Alles was in die Mandatsakte aufgenommen wird, um Grundlage der anwaltlichen Beratung oder eventuellen Sachvortrags zu sein, ist der Kerntätigkeit zuzurechnen.

Zuletzt tritt die Pflicht zur Bestellung eines Datenschutzbeauftragten unabhängig von der Zahl der Beschäftigten auch dann ein, wenn die Kerntätigkeit des Verantwortlichen in der Verarbeitung besonderer Kategorien von Daten besteht und diese Verarbeitung **umfangreich** ist.

Eine verlässliche Definition des Begriffs „umfangreich" wird erst in einigen Jahren vorliegen, wenn die ersten Gerichte darüber entschieden haben. In der Literatur wird zum Beispiel vertreten, umfangreich bedeute *„viele Personen oder große Mengen von Daten betreffend"* (BeckOK Datenschutzrecht, Wolff/Brink, DS-GVO Artikel 37, Rn. 8). Diese Definition ist natürlich unbrauchbar. Eine andere Meinung vertritt, umfangreich bedeute *„das übliche Maß bei Weitem übersteigend"* (Paal/Pauly, DS-GVO Art. 37, Rn. 9). Diese Ansicht, die die Norm als Ausnahmevorschrift behandelt, wird jedoch mit guten Argumenten kritisiert (vgl. Sydow, Europäische Datenschutzgrundverordnung, Art. 37, Rn. 84 ff.). Die dortige Ansicht geht davon aus, dass eine Datenverarbeitung dann umfangreich ist, wenn sie im Sinne des Schutzzwecks des Datenschutzrechts *„relevant"* wird. Relevanz wird gesehen, wenn die Verarbeitung kein Einzelfall ist.

Die Beantwortung der Frage, wann eine Datenverarbeitung umfangreich ist, dürfte für viele kleine Anwalts-

kanzleien sehr wichtig werden. Viele Kanzleien haben einen bis drei Berufsträger und bleiben auch inklusive Büropersonal und Referendaren unter der 10-Personen-Grenze. Gleichzeitig bearbeiten häufig kleine Anwaltskanzleien Mandate aus den oben genannten Bereichen und verarbeiten demgemäß auch Daten aus den besonderen Kategorien nach Art. 9 und 10 DSGVO. Die Frage des Umfangs der Datenverarbeitung und der rechtlichen Beurteilung der Kategorie „umfangreich" ist für diese Kanzleien also relevant für die Bestellung eines Datenschutzbeauftragten. Für die meisten der kleinen Anwaltskanzleien dürfte nur ein externer Datenschutzbeauftragter in Betracht kommen, sodass aus der Bedeutung des Wortes „umfangreich" entweder ein Kostenfaktor durch Bestellung eines externen Datenschutzbeauftragten oder ein erhebliches rechtliches Risiko durch die Nicht-Benennung erwächst.

Es ist davon auszugehen, dass diese Frage in den nächsten Jahren gerichtlich geklärt wird. Aus jetziger Sicht ist anzuraten, sich der Ansicht anzuschließen, die eine umfangreiche Verarbeitung dann annimmt, wenn sie über den Einzelfall hinausgeht. Mit anderen Worten: Es sind all diejenigen Kanzleien betroffen, die regelmäßig Mandate aus den genannten Rechtsgebieten bearbeiten. Nicht betroffen dürften diejenigen Kanzleien sein, die zum Beispiel hauptsächlich Baurecht oder gewerblichen Rechtsschutz bearbeiten und „alle Jubeljahre" einen Verkehrsunfall mit strafrechtlicher Relevanz für einen Studienfreund übernehmen.

Ebenfalls unabhängig von der Zahl der Beschäftigten ist die Bestellung eines Datenschutzbeauftragten erforderlich bei Datenverarbeitungsvorgängen, die eine sogenannte **Datenschutzfolgenabschätzung** erforderlich machen.

Die Datenschutzfolgenabschätzung (DSFA) ist geregelt in Art. 35 DSGVO. Sie ist dann erforderlich, wenn hohe Risiken für die Betroffenen bestehen. Namentlich genannt wird der Einsatz „neuer Technologien". Ein solcher Einsatz in einer klassisch geführten Rechtsanwaltskanzlei ist eher nicht denkbar. Relevant könnten neue Technologien sein bei Legal Tech-Leistungen, wenn diese zum Beispiel mit künstlicher Intelligenz verknüpft werden. Abgesehen von solchen neuen Technologien dürfte die Regelung für eine Anwaltskanzlei keine eigenständige Bedeutung haben neben der Verarbeitung besonderer Kategorien von Daten. Allerdings stellt Erwägungsgrund 91 zur DSGVO klar, dass Einzelkanzleien zu keiner DSFA verpflichtet sind.

2. Datenschutzerklärung offline/online

Nach Art. 13 DSGVO ist der Verantwortliche verpflichtet, die Betroffenen bei der Erhebung über die wesentlichen Grundsätze der Datenverarbeitung durch ihn zu informieren. Dies erfolgt bei der Begründung des Mandats in der Anwaltskanzlei entweder durch Aushändigen der Datenschutzerklärung der Kanzlei mit den Mandatsvertragsunterlagen. Alternativ kann die Information durch Aushang in der Kanzlei erfolgen. Bei der Erhebung von Daten über die Website hat die Datenschutzerklärung der Website auch die Datenschutzhinweise bei der Verarbeitung von Daten im Mandat zu umfassen. Bei elektronischer Kontaktaufnahme des Mandanten ist der Datenschutzhinweis mit den weiteren Unterlagen zur Begründung eines Mandates in Textform zu übermitteln.

Die Datenschutzerklärung muss enthalten:

- Bezeichnung der verantwortlichen Stelle, deren Vertreter, Kontaktdaten
- Kontaktdaten des Datenschutzbeauftragten (sofern benannt/Angabe des Namens des Datenschutzbeauftragten ist nicht verpflichtend)
- Zwecke, für die die Verarbeitung der Daten erfolgt, sowie Kategorien der Daten und der Betroffenen, z. B. Personen- und Kontaktdaten der Mandanten für die Begründung und Führung des Mandats
- Rechtsgrundlagen der Datenverarbeitung für die jeweiligen Zwecke

- Bei Verarbeitung nach Art. 6 Abs. 1 f.) DSGVO die berechtigten Interessen, z. B. Personen- und Kontaktdaten der Gegner und Zeugen für die rechtliche Interessenvertretung des Mandanten
- Kategorien von Datenempfängern, z. B. Gerichte
- Informationen über die Absicht, die Daten in Drittländer außerhalb des Europäischen Wirtschaftsraumes zu übermitteln, z. B. Beauftragung einer Korrespondenzanwaltskanzlei in den USA zur dortigen selbstständigen Wahrnehmung des Mandats
- Soweit möglich Informationen zur regelmäßigen Dauer der Verarbeitung und Löschfristen
- Information über die Betroffenenrechte einschließlich des Beschwerderechts bei den Aufsichtsbehörden
- Information über das Widerrufsrecht bei Einwilligung in die Datenverarbeitung nach Art. 6 Abs. 1 a) DSGVO, für die Datenverarbeitung, die über das erforderliche Maß zur Mandatsbetreuung nach Art. 6 Abs. 1 b) DSGVO hinausgeht
- Information über etwaige automatisierte Entscheidungsfindungen, denkbar bei Legal Tech-Anwendungen

Die Betroffenen haben ein Recht auf Benachrichtigung und Auskunft über das „Ob" und „Wie" der Datenverarbeitung, auf die Berichtigung und Löschung sowie die Einschränkung der Verarbeitung. Zudem haben sie das Recht auf Übertragbarkeit der Daten und das Recht auf Widerspruch gegen die Verarbeitung, soweit die Kanzlei keine überwiegenden berechtigten Gründe für die Verarbeitung nachweist.

Dabei ist zu beachten, dass die Rechte auf Benachrichtigung und Auskunft nach § 29 Abs. 1 und 2 BDSG n. F. für Berufsgeheimnisträger im Interesse des Geheimnisschutzes über das Mandat und den betroffenen Mandanten und zulasten der betroffenen Gegner, Zeugen, Sachverständigen und anderen Beteiligten eingeschränkt sind. Die Kanzlei ist nur im Ausnahmefall – wenn die schutzwürdigen Interessen des dritten Betroffenen die Geheimhaltungsinteressen des Mandanten überwiegen – verpflichtet, über die Erhebung von Daten sowie über das „Ob" und „Wie" der Datenverarbeitung in der Kanzlei Auskunft zu erteilen. Dies ist eine Durchbrechung der Datenschutzgrundsätze der Transparenz und Direkterhebung wegen der speziellen Anforderungen der Mandatsarbeit.

Ebenso ist es dem Mandanten gestattet, die Daten seines Kunden, gegen den er z. B. eine Forderung anwaltlich durchsetzen lassen möchte, unter Durchbrechung des Zweckbindungsgrundsatzes nach § 29 Abs. 3 BDSG n. F. der Anwaltskanzlei zu übermitteln.

Für Datenerhebungen, die mit der Nutzung von Cookies und Tools auf der Website verbunden sind, ist die Datenschutzerklärung um Zweck und Umfang der Datenerhebung zu ergänzen. Hier sollte die Kanzlei äußerst kritisch prüfen, ob die eingesetzten Analyse- und Trackingtools und Social Plugins erforderlich sind und der Kanzlei einen Mehrwert in der Mandantenbetreuung bringen. Im Zweifel sollten diese Tools zukünftig nicht mehr genutzt werden. Im Fall der weiteren Nutzung sind die Datenschutzinformationen hierzu anzupassen und die Möglichkeiten eines Opt-In-Verfahrens zu nutzen. Die Datenschutzkonferenz hat sich kürzlich zum Verhältnis von DSGVO und dem Telemediengesetz in der geltenden Fassung geäußert und hält das Nutzen von Opt-In-Möglichkeiten für den Nutzer für erforderlich. Die bislang geübte Praxis, die Nutzer auf die Möglichkeiten der eigenen Browser-Einstellungen zu verweisen und einen Opt-Out vorzunehmen, reicht wohl zukünftig nicht mehr aus.

3. Muster einer Mitarbeiterverpflichtung zur Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutz-Grundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG)

Personenbezogene Daten dürfen nur verarbeitet werden, wenn eine Einwilligung bzw. eine andere gesetzliche Rechtsgrundlage (Artikel 6 DSGVO) die Verarbeitung gestattet. Es ist den Personen, die dem Verantwortlichen unterstellt sind, untersagt, (besondere) personenbezogene Daten unbefugt außerhalb der Zwecke der verantwortlichen Stelle und der arbeitsbezogenen datenschutzrechtlichen Richtlinien zu verarbeiten. Der Verantwortliche ist hinsichtlich der technischen und organisatorischen Maßnahmen zur Einhaltung der Datenschutzgrundsätze nach Art. 5 Abs. 2, 24 DSGVO rechenschaftspflichtig.

Die Grundsätze für die Verarbeitung personenbezogener Daten sind in Art. 5 Abs. 1 DSGVO festgelegt und umfassen im Wesentlichen folgende Verpflichtungen:

(Besondere) Personenbezogene Daten müssen:

a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);
b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“);
c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);
d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);
e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist („Speicherbegrenzung“);
f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“).

Verstöße gegen diese Verpflichtung können mit Geldbuße und/oder Freiheitsstrafe geahndet werden (Art. 84 DSGVO, § 42 BDSG n. F.). Ein Verstoß kann zugleich eine Verletzung von arbeitsvertraglichen Pflichten oder Geheimhaltungspflichten darstellen. Auch (zivilrechtliche) Schadenersatzansprüche können sich aus schuldhaften Verstößen gegen diese Verpflichtung ergeben.

_____	_____	_____
Vorname	Nachname	Position

bestätigt von der Verantwortlichen Stelle auf den Datenschutz verpflichtet worden zu sein. Die Verpflichtung gilt auch nach Beendigung der Tätigkeit fort.*

_____

Ort, Datum

_____	_____
Unterschrift des Verpflichteten	Verantwortliche Stelle

_____

* Hier kann z. B. noch ergänzt werden, dass eine Sensibilisierungsschulung einschließlich der Darstellung der technischen und organisatorischen Maßnahmen stattgefunden hat und ggf. auf Schulungsunterlagen und Informationsmaterialien verwiesen werden.

4. Verpflichtung von Auftragsverarbeitern

Die Kanzlei bedient sich zur Erfüllung ihrer Aufgaben typischerweise verschiedener Dienstleister, die auch Zugriff auf die personenbezogenen Daten erlangen (können). Mit diesen Dienstleistern muss in Textform eine Leistungsvereinbarung abgeschlossen werden, die durch eine nach den Anforderungen der DSGVO angepasste Auftragsverarbeitungsvereinbarung (AVV) ergänzt wird. Die Beschreibung der technischen und organisatorischen Maßnahmen (TOM) zur Gewährleistung der Integrität und Vertraulichkeit der Daten beim Dienstleister bzw. der Durchführung seines Auftrags wird ebenso Bestandteil der AVV. Daneben sind die Dienstleister auf das Berufsgeheimnis zu verpflichten.

Muster einer Verpflichtungserklärung

FIRMA, NAME, KONTAKTDATEN

erlangt im Rahmen seiner Beauftragung mit der ITK-Administration, Systembetreuung und Support sowie der Bereitstellung von Services, Dienstleistungen und Cloud-Leistungen Kenntnis von den betrieblichen Vorgängen der Kanzlei und kann Kenntnis von personenbezogenen sowie mandatsbezogenen Daten und Informationen erlangen.

FIRMA, NAME, KONTAKTDATEN verpflichtet sich daher gegenüber der Anwaltskanzlei

zur Verschwiegenheit über alle betrieblichen Vorgänge innerhalb und außerhalb der Betriebsstätte der Kanzlei, auch nach einer etwaigen Beendigung der Zusammenarbeit sowie der einzelnen Kauf-, Werk-, Miet-, Dienstleistungsverträge.

Dies gilt ganz besonders im Hinblick auf Informationen über Mandanten und Mandate der Kanzlei (Mandatsgeheimnisse). Ein Verstoß gegen die Geheimhaltungspflicht von Mandatsgeheimnissen ist nach § 203 Abs. 4 Strafgesetzbuch strafbar. FIRMA, NAME, KONTAKTDATEN ist verpflichtet, sich nur insoweit Kenntnisse von Mandatsgeheimnissen zu verschaffen, als dies zur Erfüllung seines Auftrages/Vertrags mit der Kanzlei erforderlich ist. Es ist untersagt, Unterlagen, Schriftstücke, Abschriften, Ablichtungen, Daten und/oder sonstige Informationsträger unbefugten Personen innerhalb oder außerhalb der Kanzlei zugänglich zu machen.

Diese Geheimhaltungspflicht gilt auch über das Ende des Auftragsverhältnisses hinaus.

FIRMA, NAME, KONTAKTDATEN ist befugt, weitere Personen zur Vertragserfüllung heranzuziehen. FIRMA, NAME, KONTAKTDATEN verpflichtet sich, diese Personen nach den vorgenannten Grundsätzen in Textform zu belehren und zu verpflichten. Die hinzugezogenen Personen sind zu benennen und die Belehrung und Verpflichtung ist auf Anforderung nachzuweisen.

Soweit Zertifizierungen zum Datenschutz und zur IT-Sicherheit vorliegen, sind diese nachzuweisen. Bei Hinzuziehung von Dritten als Subunternehmer ist dies vor Beauftragung der Kanzlei mitzuteilen und bedarf der Zustimmung.

Ort, _____

_____

Unterschrift / Stempel

5. Verschlüsselung

Die Verschlüsselung eines Datenbestandes verwandelt – grob gesagt – lesbare Daten in Datensalat/Datenmüll. Daten sind dabei alle in einem Computer gespeicherten Dinge, also Adressdaten, gespeicherte Schreiben aber auch Bilddateien und ganze Ordner.

Aus „**Die Datenschutzgrundverordnung**“ wird durch Verschlüsselung mit SSL zum Beispiel „**U2FsdGVkX18d-RoIYV1k5cZcxiTsLelaMHlH1Hx88kgI9Y4su1hMqwM-8opO9vN/iE**“.

Resultat der Verschlüsselung ist, dass ein Dritter ohne den Schlüssel die Daten nicht lesen kann, z. B.:

- Einzelne Dateien
- Ganze Ordner
- Ganze Festplatten
- Ganze mobile Geräte
- Datenfluss im Netzwerk

Eine Rechtsanwaltskanzlei sollte die Datenverschlüsselung prüfen und – wenn möglich – anwenden. Ein Einsatz von EDV in der Anwaltskanzlei ohne Verschlüsselungslösungen kann fahrlässig sein.

Ein wesentliches Kennzeichen der Anwaltstätigkeit ist die Verschwiegenheit. Gespeicherte Daten sind also der Rechtsanwaltskanzlei wie einem Treuhänder anvertraut. So wenig, wie man Fremdgeld in einer unabgeschlossenen Schublade herumliegen lässt, so wenig sollten Daten unverschlüsselt gespeichert werden.

Was sollte in der Kanzlei verschlüsselt werden? Es wird dringend empfohlen, alle Festplatten der Kanzleirechner zu verschlüsseln. Es gibt zahlreiche Möglichkeiten, Daten zu verschlüsseln. (Die Darstellung aller Möglichkeiten würde den Rahmen dieser Broschüre sprengen.) Im Alltag sollte mit Bordmitteln der Betriebssysteme Windows 7 (und neuer) von Microsoft verschlüsselt werden. Microsoft bietet dazu das Programm Bitlocker an. Mit Bitlocker kann komfortabel die gesamte Festplatte verschlüsselt werden. Die Entschlüsselung läuft parallel zum Betrieb. Mit anderen Worten: Man sieht auf dem Bildschirm entschlüsselte Daten, das Speichern auf der Festplatte erfolgt jedoch verschlüsselt.

Auf neuerer Hardware ist in der Regel ein spezieller Chip verbaut, das sogenannte **Trusted Platform Module (TPM)**. Dieser Chip enthält gewissermaßen das Passwort, um die Festplatte beim Starten des Computers zu entschlüsseln. Bei älterer Hardware ist es hingegen erforderlich, bei jedem Startvorgang eine PIN einzugeben.

Diese Verschlüsselung sollte auf jedem einzelnen Computer und auch auf dem Server der Kanzlei durchgeführt werden. Ferner sollten Netzwerkspeicher, sogenannte NAS, nicht vergessen werden. Ebenfalls verschlüsselt werden müssen Datensicherungssysteme und USB-Sticks. Die Verschlüsselung von einzelnen Dateien oder Ordnern ist daneben nicht mehr erforderlich.

Neben der Verschlüsselung von Festplatten, auch im Notebook, wird empfohlen, auch **Smartphones** zu verschlüsseln. Die iPhones der neueren Generationen sind beispielsweise standardmäßig verschlüsselt. Es wird dringend empfohlen, diese Verschlüsselung durch Aktivierung des Codes zum Entsperren des Geräts zu nutzen.

Der Diebstahl von Hardware oder das Liegenlassen eines Notebooks im Zug sind ärgerlich und kosten Geld. Sind jedoch die Daten nicht verschlüsselt, liegt daneben noch ein Problem der Geheimhaltung vor und möglicherweise ein strafbarer Verstoß gegen § 203 StGB. Ferner entsteht die sehr unangenehme Pflicht, den Verlust der Datenträger der Aufsichtsbehörde und allen Mandanten mitzuteilen. All dies tritt nicht ein, wenn die Festplatten verschlüsselt sind.

Die Datensicherheit ist in Art. 32 DSGVO normiert. Die Verschlüsselung von Daten ist dort ausdrücklich genannt. Die **Verschlüsselung von Festplatten ist seit**

langem Stand der Technik, verursacht keine zusätzlichen Lizenzkosten und ist einfach und mit geringen Kosten zu implementieren.

Die Verschlüsselung von Festplatten ist Pflicht. Die **Verschlüsselung von Datenverkehr im Netzwerk** ist die Kür. Die meisten Kanzleien setzen eine der gängigen Software-Lösungen ein. In der Regel bestehen diese Lösungen aus einem Server und mehreren Client-Rechnern. Über das Netzwerk werden Daten vom Client an den Server gesendet und umgekehrt. Dieser Netzwerk-Traffic kann je nach eingesetzter Kanzlei-Software ebenfalls verschlüsselt werden. Auch diese Verschlüsselung ist zu empfehlen. Dadurch wird vermieden, dass Daten einfach durch Dritte abgegriffen werden können.

Ebenfalls anzuraten ist es, die eigene Website mit einem **SSL-Zertifikat** zu sichern. Solchermaßen gesicherte Webseiten können erkannt werden am „https“ in der Adresszeile und, abhängig vom verwendeten Browser, an dem Symbol des grünen Vorhängeschlosses. Eine solche Verschlüsselung einzurichten, ist ein vergleichsweise geringer Aufwand. Ein notwendiges SSL-Zertifikat kann preisgünstig erworben werden. Mittels „let's encrypt“ erhält man sogar ein kostenfreies Zertifikat bei Einhaltung der Lizenzbedingungen der Open Source-Software.

Tipp!

Nehmen Sie am 25. Mai 2018 auch am gleichnamigen Webinar von Rechtsanwältin Dr. Astrid Auer-Reinsdorff teil:

www.anwaltswebinare.de

KONZENTRATION AUF DAS WESENTLICHE.

MACHEN SIE IHRE KANZLEI EFFIZIENTER.

Jetzt inklusive gesetzeskonformen (ERVV 1.1.2018) elektronischem Rechtsverkehr mit Einzelsignatur auch ohne beA.

PS: beA ist selbstverständlich bereits integriert.

HAUFE. Advolux

www.professionelles-kanzleimanagement.de