DS-GVO Checkliste für Anwaltskanzleien

Am **25.05.2018** tritt die EU-weit geltende Datenschutz-Grundverordnung (DS-GVO) in Kraft, die u.a. auch für Anwaltskanzleien gilt.

Die Unsicherheit darüber, was jetzt veranlasst werden muss, ist groß, und noch größer ist die Zahl von Internet-Ratgebern, Aufsätzen und Veranstaltungen, die zu dem Thema angeboten und mit dem Drohszenario hoher Geldbußen und verstärkter Abmahnungen beworben werden.

Um etwas Licht ins Dunkel zu bringen, stellt die Rechtsanwaltskammer Düsseldorf ihren Mitgliedern und allen Interessierten die nachfolgende Checkliste zur Verfügung, die bewusst kurz und möglichst übersichtlich gehalten ist. Vorschläge für die Erstellung eines **Verarbeitungsverzeichnisses** sind in die Checkliste eingefügt (vgl. Ziff. 4.).

Das **Muster einer Datenschutzerklärung für die Kanzlei-Website** und ein **Merkblatt zur Erfüllung der Informationspflichten bei Mandatsbeginn** finden Sie ebenfalls auf der Homepage der Rechtsanwaltskammer.

Hier nun **10 Punkte**, die Sie beachten sollten:

1. Befassung mit der Materie dokumentieren

Das Wichtigste zu Beginn:

Damit Sie Gutes nicht nur tun, sondern notfalls (nämlich dann, wenn der/die Landesdatenschutzbeauftragte nachfragt) auch darüber reden können, sollten Sie in einer Art „Datenschutz-Tagebuch“ möglichst minutiös dokumentieren, welche Anstrengungen Sie und - sofern vorhanden - Ihr Datenschutzbeauftragter unternommen haben, um die Anforderungen der DS-GVO zu erfüllen.

Das „Tagebuch“ sollte stets auf dem neuesten Stand sein und Antworten auf die nachfolgenden Fragen enthalten:

- Welche Veröffentlichungen haben Sie gelesen?
- Welche Informationsveranstaltungen haben Sie besucht?

- Welche Informationsveranstaltungen hat der von Ihnen bestellte Datenschutzbeauftragte besucht?

- Welche Firewall wurde wann installiert?

- Wie halten Sie und Ihre Mitarbeiter sich „IT-technisch“ auf dem Laufenden?

- Welche Verträge wurden wann mit externen Dienstleistern geschlossen?

- Welche „Qualitätschecks“ führen Sie in welchen Abständen durch?

- Welchen „Notfall-Plan“ haben Sie für den Fall des Auftauchens eines Datenlecks oder z.B. den Verlust eines Smartphones mit Kanzleidaten?

Sollte es Probleme mit der Datenschutzbehörde geben, bietet eine gute, umgehend zur Verfügung stehende Dokumentation die Möglichkeit, einem Bußgeld zu entgehen.

2. Aufsatz zur DS-GVO lesen

Auf der Homepage der Rechtsanwaltskammer finden Sie den Aufsatz *Offermann-Burckart*, Die Datenschutz-Grundverordnung - erste Erkenntnisse und ihre Anwendung auf die anwaltliche Berufspraxis.

Wenn Sie (und Ihre Kollegen und Mitarbeiter) diesen Beitrag lesen, verfügen Sie schon einmal über einen Grundstock an Informationen, die sich nicht nur auf die DS-GVO und das BDSG-2018 beziehen, sondern auch die Vernetzung dieser Themen mit berufsrechtlichen Bestimmungen aufzeigen.

Im Hinblick auf Ziff. 1 sollten Sie notieren, wann Sie den Beitrag studiert und wie lange Sie dazu gebraucht haben.

3. Datenschutzbeauftragten benennen, sofern erforderlich

Nach Art. 37 Abs. 4 DS-GVO i.V.m. § 38 Abs. 1 BDSG-2018 müssen Sie einen Datenschutzbeauftragten bestellen, wenn in Ihrer Kanzlei in der Regel **mindestens 10 Personen** mit der automatisierten Verarbeitung personenbezogener Daten (also insbesondere der Daten von Mandanten und Mitarbeitern) beschäftigt sind.

Nach Art. 37 Abs. 7 DS-GVO müssen die Kontaktdaten des Datenschutzbeauftragten (z.B. auf der Kanzlei-Homepage) veröffentlicht und der Aufsichtsbehörde, also dem/der Landesdatenschutzbeauftragten, mitgeteilt werden.

Für die Bestimmung der Personenzahl spielt es keine Rolle, ob ein Mitarbeiter in Teil- oder Vollzeit arbeitet, freier oder fester Mitarbeiter, Auszubildender oder Praktikant ist. Entscheidend ist die Anzahl der Köpfe.

Liegt Ihre Kanzlei unter der 10-Personen-Grenze, bedeutet das natürlich nicht, dass Sie auf Datenschutzmaßnahmen verzichten können. Allerdings können die entsprechenden Aufgaben dann rein intern, etwa vom Kanzleiinhaber oder dem Bürovorsteher wahrgenommen werden.

Trotz Unterschreitens der „Kopfzahl“ von 10 gilt eine Ausnahme für solche Kanzleien, in denen Daten verarbeitet werden, für die eine Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO durchgeführt werden muss. Das ist bei allen Daten der Fall, deren Erhebung und Verarbeitung für die Betroffenen mit einem hohen Risiko verbunden sein können, wie dies etwa bei Daten zur ethnischen Herkunft, sexuellen Orientierung, Gesundheit oder politischen Einstellung der Fall ist.

Wer in Asylangelegenheiten tätig wird (z.B. ein „Fachanwalt für Migrationsrecht“) oder mit sensiblen Patientendaten umgeht (z.B. ein „Fachanwalt für Medizinrecht“), ist deshalb gut beraten, in jedem Fall einen offiziellen Datenschutzbeauftragten zu bestellen und nach außen zu präsentieren.

Auch wenn gelegentlich scherzhaft geäußert wird, ein schlechter Datenschutzbeauftragter sei besser als gar keiner, sollten Sie für diese Funktion nur jemanden auswählen, der - belegbar und von Ihnen dokumentiert - über die erforderliche Fachkunde verfügt und sich durch regelmäßige Fortbildung (ebenfalls dokumentiert) auf dem Laufenden hält.

Nach **Art. 39 Abs. 1 DS-GVO** obliegen dem Datenschutzbeauftragten „zumindest“ die folgenden Aufgaben:

- die Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach der DS-GVO sowie nach sonstigen Datenschutzvorschriften der Union bzw. der Mitgliedstaaten

- die Überwachung der Einhaltung der DS-GVO, anderer Datenschutzvorschriften der Union bzw. der Mitgliedstaaten sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten, einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen

- (auf Anfrage) die Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gem. Art. 35 DS-GVO

- die Zusammenarbeit mit der Aufsichtsbehörde

- die Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gem. Art. 36 DS-GVO und ggf. die Beratung zu allen sonstigen Fragen.

Die Tätigkeit des Datenschutzbeauftragten ist also umfangreich und anspruchsvoll und lässt sich - insbesondere in größeren Kanzleien - nicht einfach „nebenher“ erledigen.

4. Verarbeitungstätigkeiten in einem Verzeichnis erfassen

Jede Kanzlei muss ein sog. „Verzeichnis der Verarbeitungstätigkeiten“ anlegen.

Hierzu besagt **Art. 30 Abs. 1 DS-GVO**:

> „Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält sämtliche folgenden Angaben:
>
> a) den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;
>
> b) die Zwecke der Verarbeitung;
>
> c) eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;

d) die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;

e) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;

f) wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;

g) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.“

In jeder (auch kleineren) Kanzlei sollte ein Verantwortlicher, nebst Stellvertreter, benannt werden, der für die Anlage und das Führen des Verarbeitungsverzeichnisses zuständig ist.

Zu Beginn ist es hilfreich, unter Beteiligung aller Kollegen und Mitarbeiter, die mit der Datenverarbeitung in der Kanzlei zu tun haben, ein Brainstorming durchzuführen, bei dem die verschiedenen Arbeitsabläufe (etwa vom ersten telefonischen Kontakt mit einem neuen Mandanten über das Anlegen der Akte in papierner und/oder elektronischer Form bis hin zur Endabrechnung des Mandats) identifiziert und erfasst werden.

Abgefragt werden sollte u.a.

- Welche Daten werden wann erhoben?

- Welchem Zweck dient die Datenerhebung?

- Welche Informationen erhalten Betroffene (z.B. die Mandanten, Mitarbeiter, Bewerber) über die Erhebung und Speicherung personenbezogener Daten?

- Wie werden diese Informationen erteilt (z.B. auf der Homepage, in einem Merkblatt, als Bestandteil des Mandatsvertrags)?

☐ Wie werden die erhobenen Daten weiterverarbeitet?

☐ Werden Daten anonymisiert?

☐ Wo werden die Daten gespeichert?

- Werden die Daten durch technische und organisatorische Maßnahmen ausreichend geschützt?

☐ Wie lange werden welche Daten gespeichert?

- Gibt es Aufbewahrungs- und/oder Löschfristen?
  Wie wird deren Einhaltung sichergestellt?

☐ Werden Daten weitergegeben?
Wenn ja, an wen?

- Ist der Datenempfänger ebenfalls für den Datenschutz verantwortlich?
  Muss er hierauf hingewiesen werden?

- Wo werden die Daten vom Empfänger gespeichert?
  Werden sie außerhalb der EU gespeichert?
  Falls ja: Sind die Voraussetzungen zur Übermittlung an Drittstaaten erfüllt?

- Werden die Daten vom Empfänger durch technische und organisatorische Maßnahmen ausreichend geschützt?

Aus den Antworten auf diese und weitere Fragen ergibt sich dann - gewissermaßen zwangsläufig - das Verarbeitungsverzeichnis, das (ohne Anspruch auf Vollständigkeit) wie folgt aussehen könnte:

Kategorie 1: Mandanten-Stammdaten

Verantwortlich:	Managing-Partner RA Dr. Max Mustermann, Kontaktdaten.
Zweck:	Erbringen der anwaltlichen Dienstleistung;

	Abrechnung; Kollisionskontrolle.
Betroffene:	Alle aktuellen Mandanten der Kanzlei; alle früheren Mandanten, deren Handakten gem. § 50 Abs. 1 BRAO (oder aufgrund sonstiger Bestimmungen) noch aufbewahrt werden müssen.
Einwilligung des Betroffenen:	Jeder Mandant wird zu Beginn des Mandatsverhältnisses schriftlich auf die Erfassung seiner Daten hingewiesen und darauf aufmerksam gemacht, dass er die Daten jederzeit einsehen und - vorbehaltlich entgegenstehender gesetzlicher Regelungen (z.B. § 50 Abs. 1 BRAO) - deren Löschung veranlassen kann.
Wer kann auf die Daten zugreifen?	Alle Partner und anwaltlichen Angestellten der Kanzlei; freie anwaltliche Mitarbeiter, die nichtanwaltlichen Kanzleiangestellten und Stagen-Referendare im Rahmen der ihnen konkret übertragenen Aufgaben.
Datenkategorie:	Name, Anschrift, Kontaktdaten; konkrete Beauftragung; eventuell Vorgeschichte des Mandats; zuständiger Sachbearbeiter; Rechtsschutzversicherung; Beratungshilfe, PKH oder VKH.
Übermittlung an Dritte?	Ja, und zwar: Deckungsschutzanfragen bei der Rechtsschutzversicherung; Einbindung von Sachverständigen; Schriftsätze an Gegner, Gerichte, sonstige Behörden etc.
Übermittlung an Drittstaaten?	Nein.
Aufbewahrungs-/Löschfristen:	Für die Dauer von 6 Jahren nach Ablauf des Kalenderjahres, in dem der Auftrag beendet wurde (§ 50 Abs. 1 BRAO);

	sonstige Fristen nach Spezialnormen (z.B. der AO oder des GwG).
Rechtsgrundlagen:	Art. 6 Abs. 1 lit. b DS-GVO; §§ 50, 56 BRAO; Spezialnormen der AO oder des GwG.

Kategorie 2: Mitarbeiter-Daten

Verantwortlich:	Bürovorsteherin Monika Mustermann, Kontaktdaten.
Zweck:	Mitarbeiterführung und -betreuung; Lohnbuchhaltung.
Betroffene:	Alle aktuellen festangestellten und freien anwaltlichen und nicht-anwaltlichen Mitarbeiter der Kanzlei; alle Auszubildenden; alle Referendare, studentischen Hilfskräfte, Praktikanten. (Anmerkung: Für Bewerber sollte eine eigene Kategorie gebildet werden.)
Einwilligung des Betroffenen:	Bestandsmitarbeiter werden mündlich über die Erfassung ihrer Daten in einer Personalakte informiert. Neue Mitarbeiter werden zu Beginn des Beschäftigungsverhältnisses schriftlich auf die Erfassung ihrer Daten in einer Personalakte hingewiesen.
Wer kann auf die Daten zugreifen?	Alle Partner der Kanzlei; Bürovorsteherin Monika Mustermann; die für die Ausbildung von ReFas zuständige Mitarbeiterin XY; der Buchhalter XY.
Datenkategorie:	Name, Anschrift, Kontaktdaten; Bewerbungsschreiben und Bewerbungsunterlagen nebst Lebenslauf (mit Lichtbild) und Zeugnissen; Daten des Bankkontos, auf das die

	Gehaltszahlung erfolgt; Zwischenzeugnisse, Abmahnungen.
Übermittlung an Dritte?	Ja, und zwar: Steuerberaterkanzlei XY; Rentenversicherung im Falle von Betriebsprüfungen.
Übermittlung an Drittstaaten?	Nein.
Aufbewahrungs-/Löschfristen:	Für die Dauer des Beschäftigungsverhältnisses bzw. der Ausbildung, der Referendarstage etc. Mit ausdrücklicher Zustimmung der Betroffenen werden die reinen Adressdaten auch nach Ausscheiden aus der Kanzlei gespeichert, damit Geburtstagsglückwünsche und/oder die Einladung zur jährlichen Weihnachtsfeier erfolgen können.
Rechtsgrundlagen:	Art. 13 Abs. 1 u. 2 DS-GVO; arbeitsrechtliche Vorschriften; Vorschriften des JAG, BBiG etc.

Auf die gleiche Weise lassen sich **weitere Kategorien** bilden etwa für

- ☐ Bewerber um einen Ausbildungs- oder Arbeitsplatz
- ☐ andere Kanzleien, mit denen verfestigte Kooperationen bestehen
- IT-Dienstleister, Sachverständige, Übersetzer, Detektive, mit denen regelmäßig zusammengearbeitet wird
- interessierte Kollegen und/oder (potenzielle) Mandanten, die regelmäßig zu Inhouse-Seminaren, Vernissagen u.Ä. eingeladen werden

etc.

Sie müssen schließlich noch den Weg der Daten nachzeichnen, von der Erhebung (etwa der Online-Terminvergabe für ein erstes Beratungsgespräch) über die Speicherung (z.B. in der Cloud) bis hin zur Nutzung (z.B. durch die Mitarbeiter [welche?] bei Erstellen eines Schriftsatzes oder der Schlussrechnung).

Ein solches Verzeichnis war übrigens, was kaum jemand registriert hat, schon nach dem alten Bundesdatenschutzgesetz verpflichtend.

Und noch eines muss beherzigt werden:

Auch wenn der heute vor allem in technischem Zusammenhang gebräuchliche Begriff „Daten“ intuitiv mit einer technischen, automatisierten Verarbeitung in Verbindung gebracht wird, kann „Verarbeitung“ i.S. der DS-GVO auch nicht-technisch, nicht-automatisiert, also manuell (unter Verwendung von Papier und Aktenordnern) erfolgen, weshalb auch „analoge“ Abläufe erfasst werden müssen.

Eine gute Nachricht gibt es:

Gegner und sonstige „Drittbetroffene“ (z.B. potenzielle Zeugen oder zufällig in Mandatsunterlagen erwähnte Personen) müssen grundsätzlich nicht informiert werden.

Dazu sagt § 29 Abs. 2 BDSG-2018:

> „Werden Daten Dritter im Zuge der Aufnahme oder im Rahmen eines Mandatsverhältnisses an einen Berufsgeheimnisträger übermittelt, so besteht die Pflicht der übermittelnden Stelle zur Information der betroffenen Person gemäß Artikel 13 Absatz 3 der Verordnung (EU) 2016/679 nicht, sofern nicht das Interesse der betroffenen Person an der Informationserteilung überwiegt.“

5. Prozesse festlegen und schriftlich (in einem Prozesshandbuch) fixieren

Alle mit der Datenverarbeitung verbundenen Prozesse müssen dokumentiert und - wenn nötig - optimiert werden.

Dabei sind folgende Fragen maßgeblich:

- Wie werden Mandanten über die Verarbeitung ihrer Daten informiert?
- Wie reagieren Mitarbeiter, wenn Mandanten fragen, welche Daten von Ihnen gespeichert wurden?

- Wie wird verfahren, wenn ein Mandant darauf besteht, dass seine Daten gelöscht werden?
  Wie wird er über die Aufbewahrungsfristen nach BRAO, AO oder GwG etc. informiert?
  Wer ist dafür verantwortlich?

- Wie wird sichergestellt, dass so viele Daten wie nötig, aber so wenige Daten wie möglich (Stichwort: Datensparsamkeit) erhoben und gespeichert werden?

- Wie wird sichergestellt, dass gespeicherte Daten stets richtig und auf dem neuesten Stand sind, Fehler korrigiert und falsche oder veraltete Daten gelöscht werden?

- Wie wird gewährleistet, dass elektronisch geführte Handakten 6 Jahre nach Ablauf des Kalenderjahres, in dem der Auftrag beendet wurde (vgl. § 50 Abs. 1 S. 2 u. 3 BRAO), gelöscht werden?
  Wie wird insofern mit Papierakten verfahren?

- Wie werden Partner und Mitarbeiter geschult, damit sie die erforderlichen Prozesse kennen und professionell ausführen können?

- Ist sichergestellt, dass Mitarbeiter nur auf solche Daten Zugriff haben, die sie zur Erfüllung der ihnen zugewiesenen Aufgaben benötigen?

- Sind die Rechner der Kanzlei ausreichend gegen den Zugriff Unbefugter, gegen Hackerangriffe und Malware geschützt?
  Gibt es eine Firewall?
  Sind aktuelle Virenscanner installiert?
  Welche „analogen“ Sicherungsmaßnahmen wurden ergriffen (Sicherheitsschlösser, Alarmanlage, Wachdienst)?

- Wie ist der Schutz von Daten, die in einer Cloud gespeichert sind, gewährleistet?

- Wie wird verfahren, falls es zu einem Datenleck gekommen ist oder ein mobiles Endgerät verloren wurde, und die Gefahr besteht, dass personenbezogene Daten in falsche Hände geraten sind?
  Achtung:
  (Mögliche) Datenschutzverletzungen müssen der Aufsichtsbehörde und dem Betroffenen binnen 72 Stunden angezeigt werden!

6. Technische und organisatorische Maßnahmen zur Gewährleistung der Datensicherheit ergreifen

Nach **Art. 32 Abs. 1 DS-GVO** müssen „unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen“ geeignete technische und organisatorische Maßnahmen getroffen werden, um „ein dem Risiko angemessenes Schutzniveau“ zu gewährleisten.

Nach dem Wortlaut der Verordnung schließen diese Maßnahmen

„gegebenenfalls unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.“

Die Regelung entspricht in etwa dem, was auch § 2 Abs. 7 BORA (der nach der neuesten Beschlussfassung der Satzungsversammlung vom 16.04.2018 demnächst zu Abs. 4 wird) vorschreibt, indem es heißt:

> „Die Verschwiegenheitspflicht gebietet es dem Rechtsanwalt, die zum Schutze des Mandatsgeheimnisses erforderlichen organisatorischen und technischen Maßnahmen zu ergreifen, die risikoadäquat und für den Anwaltsberuf zumutbar sind. Technische Maßnahmen sind hierzu ausreichend, soweit sie im Falle der Anwendbarkeit des Datenschutzrechts dessen Anforderungen entsprechen. Sonstige technische Maßnahmen müssen ebenfalls dem Stand der Technik entsprechen.“

Da die DS-GVO nicht den optimalen Schutz, sondern nur ein „angemessenes Schutzniveau“ fordert, verlangt sie vom Rechtsanwalt nichts Unmögliches und vor allem keinen finanziellen und organisatorischen Aufwand, der außer Verhältnis zur Größe der Kanzlei steht.

Die Einholung des Rates von IT-Experten kann allerdings nicht schaden.

Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit Sitz in Berlin hat sich gegenüber der Satzungsversammlung als Ansprechpartner für Rechtsanwälte angeboten.

7. Datenschutz-Folgenabschätzung durchführen, sofern erforderlich

Wer mit hochsensiblen Daten umgeht, wie dies bei Rechtsanwälten, die auf Medizinrecht, Asylrecht oder auch auf die Vertretung von Drogenabhängigen oder Sexualstraftätern spezialisiert sind, der Fall ist, muss besondere Vorsicht walten lassen und u.U. eine sog. Datenschutz-Folgenabschätzung durchführen.

Das gilt grundsätzlich für alle Kanzleien, die aufgrund ihrer Mandatsstruktur eine Identifizierung und Kategorisierung von Personen nach Themen wie z.B. Sexualität, Krankheiten, Finanzen, rassische oder ethnische Herkunft oder politische Ansichten ermöglichen, bei denen für die Betroffenen ein besonders hohes Risiko besteht, wenn diese Daten missbraucht werden.

Ziel der in **Art. 35 DS-GVO** vorgeschriebenen Datenschutz-Folgenabschätzung ist es, die Risiken für die Persönlichkeitsrechte der betroffenen Personen zu erkennen, um so geeignete Schutzmaßnahmen treffen zu können.

Die Datenschutz-Folgenabschätzung besteht in

- der Beschreibung der Datenverarbeitungsvorgänge
- der Beschreibung des Zwecks der Datenverarbeitung und der Begründung, warum die Kanzlei ein berechtigtes Interesse an den Daten hat (Stichworte: Verhältnismäßigkeit der Datenerhebung und -verarbeitung zu ihrem Zweck, Datensparsamkeit)
- der Beschreibung der Risiken, die für betroffene Personen bestehen

- der Dokumentation der (besonderen) technischen und organisatorischen Maßnahmen, die zum Schutz der sensiblen Daten gegen unberechtigten Zugriff oder unberechtigte Weitergabe ergriffen werden

- der Dokumentation, welche Kontrollmechanismen sicherstellen, dass die Daten dauerhaft geschützt bleiben

- der Dokumentation, wie im Falle eines „Lecks“ etc. verfahren wird

Die Landesdatenschutzbehörden haben hier eine beratende Funktion.

8. Den richtigen Umgang mit „Auftragsverarbeitern“ pflegen

Kanzleien, die sich der Hilfe von sog. Auftragsverarbeitern (z.B. IT-Experten, Anbietern von Bürodienstleistungen, Übersetzern etc.) bedienen, müssen die besonderen Vorgaben des **Art. 28 DS-GVO** beachten.

„Auftragsverarbeiter“ ist nach der Begriffsbestimmung in Art. 4 Ziff. 8 DS-GVO

> „eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet“.

In § 43e BRAO findet sich der alternative Begriff „Dienstleister“, der in Abs. 1 S. 2 legal definiert wird als

> „eine andere Person oder Stelle, die vom Rechtsanwalt im Rahmen seiner Berufsausübung mit Dienstleistungen beauftragt wird“.

Art. 28 DS-GVO schreibt u.a. vor, dass jeder Auftragsverarbeiter sorgfältig auszuwählen, durch schriftlichen Vertrag zu binden und zu überwachen ist.

Das Nähere regelt für Rechtsanwälte in Deutschland der durch das *„Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen“* vom 30.10.2017 (BGBl. I 3618 v. 08.11.2017) neu in die Bundesrechtsanwaltsordnung eingefügte § 43e.

Bitte lesen Sie hierzu das entsprechende, ebenfalls auf der Kammer-Homepage verfügbare Merkblatt (nebst Executive Summary und Formulierungsvorschlag für eine Verschwiegenheits-Verpflichtungserklärung).

9. Die notwendigen Verschriftungen vornehmen

Um den Anforderungen der DS-GVO (und weiterer Bestimmungen z.B. des BDSG-2018) sowie des § 43e BRAO und des § 2 Abs. 7 (demnächst: Abs. 4) BORA zu genügen, muss Einiges schriftlich niedergelegt werden.

Erforderlich sind

- eine Datenschutzerklärung für die Kanzlei-Website
- ein „Merkblatt“ zur Erfüllung der Informationspflichten bei Mandatsbeginn (also eine Mandanten-Information)
- Verträge in Textform mit Auftragsverarbeitern bzw. Dienstleistern i.S. von § 43e BRAO (und die entsprechenden Verschwiegenheits-Verpflichtungserklärungen)

10. Und zu guter Letzt: Am Ball bleiben

Da die Dinge zurzeit noch sehr im Fluss sind und auf vielen Ebenen diskutiert werden, sollte man sich nach Ergreifen der ersten Maßnahmen nicht selbstzufrieden zurücklegen, sondern die Publikationen in der Fachpresse (allen voran den BRAK-Mitteilungen, dem Anwaltsblatt und natürlich den Mitteilungen der Rechtsanwaltskammer Düsseldorf nebst Newslettern und Homepage) auch weiterhin aufmerksam verfolgen, um ggf. notwendig werdende Anpassungen zeitnah vorzunehmen zu können.

gez. RAin Dr. Offermann-Burckart
Grevenbroich, den 06.05.2018