



Fragen und Antworten zur DS-GVO und zum BDSG-neu – Stand: Mai 2019

Inhaltsverzeichnis

1.	Gilt das Datenschutzrecht für Rechtsanwälte?	2
2.	Wer ist für die Einhaltung des Datenschutzes verantwortlich?	2
3.	Gibt es besondere datenschutzrechtliche Grundsätze zu beachten?	2
4.	Wann ist die Verarbeitung personenbezogener Daten erlaubt?.....	3
5.	Haben Rechtsanwälte datenschutzrechtliche Informationspflichten?	4
6.	Was regelt die DS-GVO in Bezug auf die Kanzlei-Homepage?	6
7.	Hat der Rechtsanwalt eine Informationspflicht gegenüber Gegnern?	7
8.	Müssen Rechtsanwälte Daten löschen?	7
9.	Muss ich als Rechtsanwalt einen Datenschutzbeauftragten bestellen?	8
10.	Wer kann zum Datenschutzbeauftragten benannt werden?	9
11.	Wie ist die Stellung des Datenschutzbeauftragten?	9
12.	Welche Aufgaben hat der Datenschutzbeauftragte?	9
13.	Muss die Bestellung des Datenschutzbeauftragten veröffentlicht werden?	10
14.	Müssen Rechtsanwälte Vereinbarungen über die Verarbeitung von Daten im Auftrag abschließen?	10
15.	Was ist Auftragsverarbeitung und was nicht? (Abgrenzung Auftragsverarbeitung und eigene Verantwortlichkeit)	11
16.	Muss eine Auftragsverarbeitungsvereinbarung bzgl. des beA abgeschlossen werden?	11
17.	Müssen Rechtsanwälte ein Verzeichnis über ihre Verarbeitungstätigkeiten führen?.....	12
18.	Wem ist das Verarbeitungsverzeichnis vorzulegen?	13
19.	Gibt es Vorgaben für die Kanzlei-Angestellten?	13
20.	Muss eine Verpflichtung der Kanzlei-Mitarbeiter auf die Vertraulichkeit erfolgen?.....	14
21.	Müssen Rechtsanwälte eine Datenschutz-Folgenabschätzung durchführen?.....	14
22.	Hat die Tatsache, dass ein Rechtsanwalt eine Datenschutz-Folgenabschätzung durchführen muss, Auswirkungen auf die Frage der Bestellung eines Datenschutzbeauftragten?	15
23.	Gibt es Vorgaben zur Sicherheit der Verarbeitung?	15
24.	Müssen Rechtsanwälte verschlüsselt kommunizieren?	16
25.	Gibt es Meldepflichten bei der Verletzung des Datenschutzes?	16
26.	Wer ist für die Aufsicht über Rechtsanwälte zuständig?	17
27.	Welche Befugnisse hat die Datenschutz-Aufsichtsbehörde?	17



28.	Sehen die DS-GVO und das BDSG-neu Sanktionen vor?	18
29.	Haften Rechtsanwälte bei Datenschutz-Verstößen?	19
30.	Wo findet man Informationen und praktische Hinweise zur DS-GVO?	19

1. Gilt das Datenschutzrecht für Rechtsanwälte?

Ja. Die EU-Datenschutz-Grundverordnung (**DS-GVO**) ist unmittelbar auch auf Rechtsanwälte anwendbar. Auch das neue Bundesdatenschutzgesetz (**BDSG-neu**), das die Verordnung zum Teil ergänzt, ist für Anwälte anwendbar. DS-GVO und BDSG-neu gelten ab dem 25.05.2018.

Der sachliche Anwendungsbereich der Verordnung ist in Art. 3 DS-GVO geregelt. Die DS-GVO 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.“ Die Begriffsbestimmungen finden sich in Art. 4 DS-GVO.

Die DS-GVO wird – vergleichbar mit einer Gesetzesbegründung – erläutert durch die jeweiligen **Erwägungsgründe**.

Der Text der DS-GVO ist im Amtsblatt der EU (ABl. EU-Nr. L 119/1) veröffentlicht worden: <https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=OJ:L:2016:119:TOC>.

Die GDD-Praxishilfe VI mit der Textausgabe DS-GVO mit der Zuordnung des BDSG findet sich hier: https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_6.pdf

2. Wer ist für die Einhaltung des Datenschutzes verantwortlich?

Für die Einhaltung des Datenschutzes in der Kanzlei sind der bzw. die Kanzleihinhaber, d. h. die Partner, verantwortlich.

„Verantwortlicher“ ist die „natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; ...“ (Legaldefinition in Art. 4 Nr. 7 DS-GVO).

3. Gibt es besondere datenschutzrechtliche Grundsätze zu beachten?

Die DS-GVO legt in Art. 5 Abs. 1 die Grundsätze für die Verarbeitung personenbezogener Daten fest. Diese sind insbesondere:

- Rechtmäßigkeit
- Transparenz
- Zweckbindung
- Datenminimierung/Datensparsamkeit

- Richtigkeit
- Speicherbegrenzung
- Integrität und Vertraulichkeit/Datensicherheit (durch geeignete technische und organisatorische Maßnahmen).

Insbesondere trägt der Kanzleihinhaber nicht nur die Verantwortung für die Einhaltung der Grundsätze, sondern muss deren Einhaltung auch nachweisen können, weshalb entsprechende Dokumentationen vorhanden sein sollten (**Rechenschaftspflicht**, Art 5 Abs. 2 DS-GVO).

4. Wann ist die Verarbeitung personenbezogener Daten erlaubt?

Die Verarbeitung personenbezogener Daten ist nur dann erlaubt, wenn sie rechtmäßig ist, also eine Rechtsgrundlage für die Verarbeitung besteht oder eine Einwilligung der betroffenen Person vorliegt (vgl. Art. 6 DS-GVO).

Rechtsgrundlage für die Verarbeitung personenbezogener Daten des Mandanten ist regelmäßig Art. 6 Abs. 1b DS-GVO, da sie zur Erfüllung des Mandatsvertrages – dazu gehören auch vorvertragliche Maßnahmen – erforderlich ist und auf Anfrage des Mandanten erfolgt.

Im Übrigen dient Art. 6 Abs. 1f DS-GVO (berechtigte Interessen) als Rechtsgrundlage. Dabei muss eine Interessenabwägung zwischen den berechtigten Interessen des Anwalts und den Interessen des Betroffenen stattfinden.

Auch die Beschäftigtendaten der Angestellten der Kanzlei dürfen regelmäßig zur Erfüllung des Arbeitsvertrages und der daraus bezüglichen Pflichten verarbeitet werden § 26 Abs. 1 BDSG-neu.

Ebenso erlaubt ist die Aufbewahrung aufgrund von gesetzlichen Vorschriften, beispielsweise nach dem UStG, der AO, dem SGB, der BRAO etc.

Von dem Erfordernis der ausdrücklichen Einwilligung (Art. 9 Abs. 1 lit a. DS-GVO) im Hinblick auf die Verarbeitung sog. besonderer Kategorien personenbezogener Daten der Mandanten nach Art. 9 Abs. 1 DS-GVO (z. B. rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, die Gewerkschaftszugehörigkeit, genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung) sind Rechtsanwälte als Berufsgeheimnisträger gem. Art. 9 Abs. 3 DS-GVO i. V. m § 43a BRAO sowie gem. Art. 9 Abs. 2 lit. f) DS-GVO befreit.

Eine Einwilligung ist aber dann als Rechtsgrundlage der Verarbeitung denkbar, wenn zwar Daten eines Vertragspartners, also insbesondere Mitarbeiters verarbeitet werden sollen, diese Datenverarbeitung aber nicht zur Erfüllung des Vertrages erforderlich ist, etwa im Fall von Fotos der Mitarbeiter für die Kanzlei-Homepage. Unter Umständen sind dann auch die erhöhten Formanforderungen gem. § 26 Abs. 2 Satz 3 DS-GVO einzuhalten (siehe auch Frage 13). Bei der Datenverarbeitung auf Grundlage einer Einwilligung ist zu beachten, dass diese jederzeit für die Zukunft widerrufen werden kann (Art. 7 Abs. 3 DS-GVO) und der Verantwortliche die Einwilligung dokumentieren muss (Art. 7 Abs. 1 DS-GVO).

Bezüglich der Rechtsgrundlage für die Verarbeitung personenbezogener Daten auf der Kanzlei-Homepage siehe 6.

Für die Übermittlung von Daten in Drittstaaten gelten die zusätzlichen Anforderungen gem. Art. 44 ff. DS-GVO. Weitere Informationen dazu finden Sie hier:

https://www.brak.de/w/files/02_fuer_anwaelte/datenschutz/2019-03-21_datenuebermittlung-drittdaender_brexit_final.pdf

5. Haben Rechtsanwälte datenschutzrechtliche Informationspflichten?

Ja. Der Kanzleiinhaber muss geeignete Maßnahmen treffen, um der betroffenen Person alle Informationen zur Verarbeitung „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln“ (vgl. Art. 12 DS-GVO – transparente Information).

Rechtsanwälte haben durch die DS-GVO Informationspflichten bei Erhebung der Daten direkt beim Betroffenen, z. B. beim Mandanten. Es bietet sich an, diese Informationen im Mandatsvertrag zur Verfügung zu stellen (z. B. in einer Anlage zum Vertrag). Diese Pflichten gelten nicht nur für den Mandanten, sondern für jede Person, deren personenbezogene Daten durch den Rechtsanwalt verarbeitet werden. Zum Zeitpunkt der Erhebung müssen folgende Informationen mitgeteilt werden (vgl. Art. 13 Abs. 1 DS-GVO):

- Namen und Kontaktdaten des Kanzleiinhabers ggf. seines Vertreters;
- ggf. die Kontaktdaten des Datenschutzbeauftragten;
- der **Zweck** bzw. die Zwecke, für die die personenbezogenen Daten verarbeitet werden (z. B. Erfüllung des Mandatsvertrages) sowie die **Rechtsgrundlage** für die Verarbeitung (regelmäßig ist dies bei Mandantendaten Art. 6 Abs. 1b DS-GVO);
- falls die Verarbeitung auf einer Interessenabwägung gem. Art. 6 Abs. 1f DS-GVO, müssen die berechtigten Interessen dargestellt werden, die von dem Kanzleiinhaber oder einem Dritten verfolgt werden;
(z. B. werden bei Besuch der Kanzlei-Homepage Daten der Nutzer erfasst, um die Homepage sicher betreiben und Fehler beheben zu können. Hierbei überwiegt das berechtigte Interesse des Rechtsanwalts an der Sicherstellung des sicheren Webseiten-Betriebs gegenüber dem Interesse der Betroffenen, anonym im Internet zu surfen.)
- ggf. Empfänger oder Kategorien von Empfängern der personenbezogenen Daten
- ggf. die Absicht, die Daten in ein Drittland zu übermitteln;
(Dabei ist zu beachten, dass eine Drittlandübermittlung bei der Inanspruchnahme einiger IT-Dienstleistungen enthalten ist, ohne dass dies offensichtlich sein muss.)

Zusätzlich müssen folgende Informationen mitgeteilt werden (vgl. Art. 13 Abs. 2 DS-GVO):

- Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

Diese Kriterien können sich z. B. bei einem Mandatsverhältnis u.a. an der Aufbewahrungspflicht für Handakten (sechs Jahre gem. § 50 Abs. 1 Satz 2 BRAO), der Aufbewahrungspflicht

für Rechnungen (10 Jahre gem. § 14b UStG) oder ggf. an Verjährungsfristen (bis zu max. 30 Jahre) orientieren. **Entscheidend ist hier, die Kriterien für die Festlegung der jeweiligen Dauer darzustellen.**

- Hinweis des Betroffenen auf seine Rechte:
 - Recht auf Auskunft (Art. 15 DS-GVO)
 - Recht auf Berichtigung (Art. 16 DS-GVO)
 - Recht auf Löschung, „Recht auf Vergessenwerden“ (Art. 17 DS-GVO)
 - Recht auf Einschränkung der Verarbeitung (Art. 18 DS-GVO)
 - Recht auf Datenübertragbarkeit (Art. 20 DS-GVO).
- Wenn die Datenverarbeitung auf einer Einwilligung gem. Art. 6 Abs. 1a oder Art. 9 Abs. 2a DS-GVO beruht, muss darauf hingewiesen werden, dass die Einwilligung jederzeit, ohne Angaben von Gründen für die Zukunft widerrufen werden kann.
- Hinweis des Betroffenen auf sein Recht, sich bei der Aufsichtsbehörde zu beschweren.
- Information darüber, ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte und
- das Bestehen einer automatisierten Entscheidungsfindung einschließlich „Profiling“.

Falls der Rechtsanwalt beabsichtigen sollte, die personenbezogenen Daten zu einem anderen als dem ursprünglichen Zweck weiterzuverarbeiten, so stellt er der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen gem. Absatz 2 zur Verfügung (Art. 13 Abs. 3 DS-GVO).

Die zuvor genannten Informationspflichten bestehen nicht, wenn und soweit der Betroffene bereits über die Informationen verfügt (Art. 13 Abs. 4 DS-GVO).

Die **GDD-Praxishilfe VII zu den Transparenzpflichten bei der Datenverarbeitung** findet sich hier:

https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_7.pdf

Das **Muster zur Mandanteninformation** der RAK Sachsen finden Sie hier: <https://www.rak-sachsen.de/documents/2018/05/muster-mandanteninformationen-datenschutz.pdf/>

Das **Muster** der RAK Sachsen der **Datenschutzbelehrung für die Homepage** ist unter folgendem Link einsehbar: <https://www.rak-sachsen.de/documents/2018/05/muster-formular-datenschutzbelehrung-fuer-homepage.pdf/>

Eine unverbindliche **Muster-Datenschutzerklärung** für die Website der RAK München findet sich hier:

https://rak-muenchen.de/fileadmin/downloads/01_Rechtsanwaelte/Mitgliederservice/Datenschutz_in_Anwaltskanzleien/Muster_Datenschutzerklaerung_Website.pdf und den Fragebogen dazu hier: [https://rak-muenchen-](https://rak-muenchen.de/fileadmin/downloads/01_Rechtsanwaelte/Mitgliederservice/Questionnaire_Datenschutz_in_Anwaltskanzleien.pdf)

[chen.de/fileadmin/downloads/01_Rechtsanwaelteliste/Mitgliederservice/Datenschutz_in_Anwaltskanzleien/Fragebogen_Datenschutzerklaerung.pdf](https://www.bfdi.bund.de/DE/Content/Rechtsanwaelteliste/Mitgliederservice/Datenschutz_in_Anwaltskanzleien/Fragebogen_Datenschutzerklaerung.pdf)

Das **Kurzpapier zum Auskunftsrecht** und das **Kurzpapier zum Recht auf Löschung / "Recht auf Vergessenwerden"** der Datenschutz-Konferenz kann unter folgendem Link eingesehen werden:

https://www.bfdi.bund.de/DE/Content/Kurzmeldungen/DSGVO_Kurzpapiere1-3.html.

6. Was regelt die DS-GVO in Bezug auf die Kanzlei-Homepage?

Der Verantwortliche hat einerseits dafür zu sorgen, dass auf der Website keine unzulässigen Datenverarbeitungen stattfinden. Andererseits muss er die Besucher über die stattfindenden Datenverarbeitungen informieren.

Wird auf der Kanzleihomepage ein Kontaktformular verwendet, so ist zu beachten, dass die Erhebung von Daten auf das notwendige Maß beschränkt werden muss (Grundsatz der Datenminimierung). Um zu verhindern, dass die personenbezogenen Daten nach Eingabe des Benutzers in das Kontaktformular auf dem Übertragungsweg abgefangen werden, und somit zu Dritten und nicht zur Kanzlei weitergeleitet werden, empfiehlt sich die Verwendung des sichereren „https-Protokolls“.

Schließt der Mandant später einen Mandatsvertrag mit dem Rechtsanwalt, liegt ein typischer Fall von Art. 6 lit. b) DS-GVO vor.

Für rein informatorische Besuche auf der Website bietet Art. 6 lit. f) eine Rechtsgrundlage. In der Regel überwiegt hierbei das berechtigte Interesse des Rechtsanwalts an der Sicherstellung des sicheren Webseitenbetriebs gegenüber dem Interesse des Betroffenen, anonym im Internet zu surfen. Technisch notwendige Verarbeitungen für die Bereitstellung eines Dienstes sind daher unstrittig nach Art. 6 Abs. 1 lit. b) oder f) zulässig.

Über den Einsatz von Cookies, die Erstellung von Logfiles oder andere Mechanismen zur Analyse des Nutzerverhaltens muss explizit und verständlich aufgeklärt werden, wenn diese – wie üblich – personenbezogene Daten (z. B. IP-Adresse) verarbeiten. Ein besonderes Augenmerk ist auf in die Kanzleihomepage eingebundene Tools von Drittanbietern (Google Analytics, Piwik, Facebook, Newsletter-Anbieter, kostenlose Routenplaner) zu richten.

Auf welcher Rechtsgrundlage (Einwilligung oder berechtigtes Interesse?) Tracking-Mechanismen erlaubt sind, hängt vom Einzelfall ab und ist teilweise umstritten. Weitere Informationen hierzu finden Sie in den Handreichungen der Datenschutzkonferenz des Bundes und der Länder (DSK), des unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) sowie der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD) unter:

<https://www.datenschutzzentrum.de/uploads/praxisreihe/Praxisreihe-4-Informationspflichten.pdf>

https://www.lidi.nrw.de/mainmenu_Datenschutz/submenu_Technik/Inhalt/TechnikundOrganisation/Inhalt/Zur-Anwendbarkeit-des-TMG-fuer-nicht-oeffentliche-Stellen-ab-dem-25.-Mai-2018/Positionsbestimmung-TMG.pdf

<https://www.gdd.de/aktuelles/startseite/zulaessigkeit-des-tracking-nach-der-ds-gvo>

Für sämtliche Verarbeitungsvorgänge, ist den Besuchern der Homepage mitzuteilen, welche Daten für welche Zwecke und welchen Zeitraum verarbeitet werden. Außerdem schreibt Art. 13 DS-GVO Informationen über diverse Betroffenenrechte vor. Dies geschieht regelmäßig über eine hinter dem Wort „Datenschutz“ verlinkte und leicht auffindbare „Datenschutzerklärung“ oder auch „Datenschutzhinweisen“. Dieser „Datenschutz“-Link muss während des gesamten Webauftritts sichtbar und die dahinterliegende Erklärung abrufbar sein. Welche Informationspflichten im Einzelnen bestehen, ist Art. 13 DS-GVO zu entnehmen; Formulierungsbeispiele finden sich im Internet, etwa unter

https://www.bstbk.de/de/presse/news/2018-05-08_Muster-Datenschutzerklaerung/index.html

Diese Verarbeitungen müssen auch im Verzeichnis der Verarbeitungstätigkeit mit den notwendigen Informationen aufgeführt sein. (siehe 17.)

In der Praxis sind mit der Erstellung und Wartung der Kanzleihomepage oder bzgl. der Nutzung von Tools häufig externe Dienstleister involviert. Sofern dabei der Zugriff auf personenbezogene Daten erfolgt, sind sie Auftragsverarbeiter und es sind entsprechende Verträge zu schließen. (siehe 14. und 15.)

7. Hat der Rechtsanwalt eine Informationspflicht gegenüber Gegnern?

Grundsätzlich sieht Art. 14 DS-GVO eine Informationspflicht vor, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden. Diese decken sich in weiten Teilen mit den in Art. 13 DS-GVO geforderten Angaben. Zusätzlich muss u. a. angegeben werden, aus welcher Quelle die personenbezogenen Daten stammen (Art. 14 Abs. 2 lit. f) DS-GVO). Die weiteren Vorgaben in Art. 13 Abs. 2 bis 5 DS-GVO sind ebenfalls zu beachten.

Eine Ausnahme dazu findet sich jedoch in Art. 14 Abs. 5 lit. d) DS-GVO, wonach die Informationspflicht dann keine Anwendung findet, wenn die Daten gemäß dem EU- oder mitgliedstaatlichen Recht einem Berufsgeheimnis unterliegen und daher vertraulich zu behandeln sind. § 29 Abs. 1 BDSG-neu sieht zudem vor, dass ergänzend zu den in Art. 14 Abs. 5 DS-GVO genannten Ausnahmen, eine Pflicht zur Information der betroffenen Person nicht besteht, soweit durch ihre Erfüllung Informationen offenbart würden, die ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen (§ 29 Abs. 1 Satz 1 BDSG-neu).

8. Müssen Rechtsanwälte Daten löschen?

Rechtsanwälte müssen personenbezogene Daten löschen, wenn keine Rechtsgrundlage mehr für deren Speicherung besteht. Dies ergibt sich aus dem Grundsatz der Speicherbegrenzung (Art. 5 Abs. 1 e) DS-GVO) und aus Art. 17 DS-GVO.

Art. 17 Abs. 3 b) DS-GVO sieht vor, dass die Löschung nicht erforderlich ist, soweit die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erfolgt, die die Verarbeitung erfordert. Dies können z. B. folgende Fälle sein:

- berufsrechtliche Aufbewahrungspflicht für Handakten (sechs Jahre gem. § 50 Abs. 1 Satz 2 BRAO),

- Pflicht zur Durchführung einer Interessenkollisionsprüfung bei Übernahme eines Mandats (§ 43a Abs. 4 BRAO)
- Aufbewahrungspflicht für Rechnungen (zehn Jahre gem. § 14b UStG) oder
- ggf. Orientierung an Verjährungsfristen (bis zu max. 30 Jahre) auch im Interesse des Mandanten.

Wichtig ist in diesem Zusammenhang die entsprechende Dokumentation in der Kanzlei, aus der hervorgeht, welche Beweggründe zur Festsetzung der Löschrufen geführt haben.

Auch für Mitarbeiter und Bewerber gelten besondere Aufbewahrungsfristen, siehe hierzu unter Frage 18.

9. Muss ich als Rechtsanwalt einen Datenschutzbeauftragten bestellen?

Gem. Art. 37 Abs. 2 b und c DS-GVO benennen Verantwortliche und Auftragsverarbeiter auf jeden Fall einen Datenschutzbeauftragten, wenn

a) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder

b) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 besteht.

In Deutschland bestehen gem. Art. 37 Abs. 4 DS-GVO (Öffnungsklausel) in Verbindung mit § 38 BDSG-neu weitergehende Verpflichtungen. Ein Datenschutzbeauftragter ist hiernach zu bestellen, soweit in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind (§ 38 Abs. 1 Satz 1 BDSG-neu). Mitgezählt werden auch Halbtagsstellen, Auszubildende und Referendare. Auch die Partner der Kanzlei werden mitgezählt.

Zudem ist zu beachten, dass ein Datenschutzbeauftragter zwingend dann zu benennen ist, wenn ausnahmsweise eine Datenschutz-Folgenabschätzung gem. Art. 35 DS-GVO (vgl. Fragen 29 und 21) durchgeführt werden muss, unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen (§ 38 Abs. 1 Satz 2 BDSG-neu).

Das **Kurzpapier Nr. 12** zum Thema **Datenschutzbeauftragte bei Verantwortlichen und Auftragsverarbeitern** der Datenschutz-Konferenz kann unter folgendem Link eingesehen werden: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_12.pdf.

10. Wer kann zum Datenschutzbeauftragten benannt werden?

Zum Datenschutzbeauftragten können Beschäftigte der Kanzlei und externe Dienstleister benannt werden. Wichtig ist, dass der Kanzleihinhaber als Verantwortlicher nicht Datenschutzbeauftragter sein kann.

Art. 37 DS-GVO regelt die Einzelheiten der Benennung. Der Datenschutzbeauftragte wird auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt sowie auf Grundlage seiner Fähigkeiten zur Erfüllung seiner in Art. 39 DS-GVO genannten Aufgaben.

Das **Kurzpapier Nr. 12** zum Thema **Datenschutzbeauftragte bei Verantwortlichen und Auftragsverarbeitern** der Datenschutz-Konferenz kann unter folgendem Link eingesehen werden:

https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_12.pdf.

11. Wie ist die Stellung des Datenschutzbeauftragten?

Der Kanzleihinhaber muss sicherstellen, dass der Datenschutzbeauftragte frühzeitig und ordnungsgemäß in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird (Art. 38 Abs. 1 DS-GVO). Dem Datenschutzbeauftragten, dies gilt auch für Angestellte der Kanzlei, müssen vom Kanzleihinhaber die für die Erfüllung seiner Aufgaben erforderlichen Ressourcen und der Zugang zu personenbezogenen Datenverarbeitungsvorgängen zur Verfügung gestellt werden. Das bedeutet, dass der Datenschutzbeauftragte, der Beschäftigter ist, ggf. für seine Aufgabe als Datenschutzbeauftragter zumindest zum Teil von seiner sonstigen Tätigkeit freigestellt werden muss. Außerdem müssen ihm die „zur Erhaltung seines Fachwissens“ erforderlichen Fortbildungsmaßnahmen finanziert werden (Art. 38 Abs. 2 DS-GVO).

Auch muss beachtet werden, dass der Datenschutzbeauftragte bzgl. der Erfüllung seiner Aufgaben **weisungsfrei** ist; dies gilt auch für angestellte Datenschutzbeauftragte (Art. 38 Abs. 3 DS-GVO). Der interne Datenschutzbeauftragte genießt besonderen Kündigungsschutz (§ 6 Abs. 4 BDSG-neu) und kann, solange er seine Funktion innehat, lediglich außerordentlich (§ 626 BGB) gekündigt werden. Dieser Kündigungsschutz bleibt nach einer Abberufung als betrieblicher Datenschutzbeauftragter für ein weiteres Jahr bestehen, § 6 Abs. 4 Satz 3 BDSG-neu.

Bei internen und externen Datenschutzbeauftragten ist zu beachten, dass kein Interessenkonflikt mit anderen Aufgaben vorliegen darf (Art. 38 Abs. 6 DS-GVO). Dieser wird regelmäßig beim IT-Dienstleister der Kanzlei gegeben sein.

Das **Kurzpapier Nr. 12** zum Thema **Datenschutzbeauftragte bei Verantwortlichen und Auftragsverarbeitern** der Datenschutz-Konferenz kann unter folgendem Link eingesehen werden:

https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_12.pdf.

12. Welche Aufgaben hat der Datenschutzbeauftragte?

Die Aufgaben des Datenschutzbeauftragten sind in Art. 39 DS-GVO festgelegt.

Der Datenschutzbeauftragte muss u. a. den Kanzleiinhaber und die Mitarbeiter der Kanzlei über ihre datenschutzrechtlichen Pflichten unterrichten und beraten, die Einhaltung der Vorgaben der DS-GVO und des BDSG-neu überwachen, die Mitarbeiter schulen und mit der Aufsichtsbehörde zusammenarbeiten.

Das **Kurzpapier** zum Thema **Datenschutzbeauftragte bei Verantwortlichen und Auftragsverarbeitern** der Datenschutz-Konferenz kann unter folgendem Link eingesehen werden:

https://www.bfdi.bund.de/DE/Home/Kurzmeldungen/DSGVO_Kurzpapiere1-3.html.

13. Muss die Bestellung des Datenschutzbeauftragten veröffentlicht werden?

Der Kanzleiinhaber muss die Kontaktdaten des Datenschutzbeauftragten veröffentlichen. Dies kann z. B. auf der Kanzleihomepage geschehen. Zudem muss er diese Kontaktdaten der Aufsichtsbehörde mitteilen (Art. 37 Abs. 7 DS-GVO). Die Mitteilung gegenüber der Aufsichtsbehörde soll über das elektronische Portal der Aufsichtsbehörde des jeweils zuständigen Landes erfolgen. Dort stehen standardisierte Formulare zur Anmeldung oder auch Abmeldung des Datenschutzbeauftragten bereit.

Die Kontaktdaten der Aufsichtsbehörden und deren Homepages sind über folgenden Link zu finden:

https://www.bfdi.bund.de/DE/Infothek/Anschriften_Links/anschriften_links-node.html

14. Müssen Rechtsanwälte Vereinbarungen über die Verarbeitung von Daten im Auftrag abschließen?

Rechtsanwälte müssen dann Vereinbarungen i. S. v. Art. 28 DS-GVO abschließen, wenn eine andere „Einheit“ **für sie** personenbezogene Daten im Auftrag verarbeitet. Der Auftragsverarbeiter ist von den Weisungen des Rechtsanwaltes abhängig (Art. 29 DS-GVO).

Erfolgt eine Verarbeitung im Auftrag eines Kanzleiinhabers, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DS-GVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet“ (Art. 28 Abs. 1 DS-GVO).

Die Verarbeitung durch den Auftragsverarbeiter erfolgt auf Grundlage eines Vertrags, der schriftlich oder elektronisch abgeschlossen werden kann. Darin müssen „*Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt*“ werden. Der Vertrag soll zudem u. a Regelungen nach Maßgabe von Art. 28 Abs. 3 Satz 2a – h DS-GVO enthalten.

Bespiele für Auftragsverarbeitungsverhältnisse:

- Daten- bzw. Aktenvernichtungsunternehmen,
- externes Rechenzentrum,
- externes Archiv,
- Cloud-Dienstleister,
- externes Lohn- und Gehaltsbuchhaltungsbüro.

Der Auftragsverarbeiter muss den Rechtsanwalt bei der Behebung von Datenpannen und deren Meldung bzw. bei der Wahrnehmung von Betroffenenrechten unterstützen.

Der Rechtsanwalt muss seinen Auftragsverarbeiter sorgfältig auswählen und kontrollieren. Es bietet sich an, ein zertifiziertes Unternehmen zu wählen.

Das **Kurzpapier zur Auftragsverarbeitung** der Datenschutz-Konferenz kann unter diesem Link eingesehen werden: https://www.bfdi.bund.de/DE/Home/Kurzmeldungen/DSGVO_Kurzpapiere1-3.html.

Die GDD-Praxishilfe zur DS-GVO Muster zur Auftragsverarbeitung findet sich hier:

https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_4.pdf

Eine Mustervertragsanlage des bitkom findet sich hier: <https://www.bitkom.org/NP-Themen/NP-Vertrauen-Sicherheit/Datenschutz/EU-DSG/170515-Auftragsverarbeitung-Anlage-Mustervertrag-online.pdf>

15. Was ist Auftragsverarbeitung und was nicht? (Abgrenzung Auftragsverarbeitung und eigene Verantwortlichkeit)

Nicht jede Beauftragung mit Dienstleistungen unterfällt der Auftragsdatenverarbeitung gem. Art. 28 DS-GVO. Vielmehr kann der Beauftragte selbst Verantwortlicher im Sinne der DS-GVO sein mit der Folge, dass er die Anforderungen der DS-GVO umsetzen muss und nicht der Auftraggeber. Die Frage stellt sich bei externen IT-Dienstleistungen oder Wartung genauso wie bei der Einholung externer Fachleistungen.

Vgl. **zur Abgrenzung** von Verantwortlichkeit und Auftragsdatenverarbeitung die **Beispielsliste** des BayLDA unter:

https://www.lida.bayern.de/media/FAQ_Abgrenzung_Auftragsverarbeitung.pdf

Vgl. speziell zum **Hosting rein statischer Webseiten** das BayLDA unter:

https://www.lida.bayern.de/media/FAQ_Hosting_keine_Auftragsverarbeitung.pdf

Vgl. zu **IT- und Infrastruktur-Wartung** das Kurzpapier Nr. 13 der Datenschutzkonferenz (DSK) zur Auftragsdatenverarbeitung unter:

https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf

16. Muss eine Auftragsverarbeitungsvereinbarung bzgl. des beA abgeschlossen werden?

Es ist nicht erforderlich, Verträge zur Auftragsverarbeitung zwischen der BRAK und den das besondere elektronische Anwaltspostfach (beA) nutzenden Rechtsanwälten abzuschließen.

Die Datenverarbeitung ist auf der Grundlage von Art. 6 Abs. 1 e, Abs. 3 DS-GVO, § 3 BDSG i. V. m §§ 31a, 31c BRAO, 22 Abs. 2 Satz 1 RAVPV zulässig. Der Abschluss von Vereinbarungen über die Auftragsverarbeitung i. S. v. Art. 28 DS-GVO ist daher nicht erforderlich.

17. Müssen Rechtsanwälte ein Verzeichnis über ihre Verarbeitungstätigkeiten führen?

Jeder Verantwortliche, d. h. auch jeder Kanzleihinhaber, muss ein Verzeichnis aller Tätigkeiten führen, bei denen personenbezogene Daten verarbeitet werden (Art. 30 Abs. 1 Satz 1 DS-GVO). Das Verzeichnis von Verarbeitungstätigkeiten kann schriftlich oder elektronisch geführt werden. Das Verarbeitungsverzeichnis muss Angaben enthalten zu:

- Namen und Kontaktdaten des Kanzleihinhabers und ggf. des gemeinsam mit ihm Verantwortlichen (Partner, evtl. Bürogemeinschaft?), seines Vertreters und ggf. des Datenschutzbeauftragten.

Es bietet sich an, diese Informationen „vor die Klammer“ zu ziehen, und danach die einzelnen Verarbeitungsprozesse darzustellen.

- Zwecke der Verarbeitung (z. B. 1. Zeile: Erfüllung von Mandatsverträgen zur Beratung und gerichtlichen und außergerichtlichen Vertretung, 2. Zeile: Durchführung von Beschäftigungsverhältnissen, inklusive des Bewerbungsprozesses, 3. Zeile: ...).
- Beschreibung der Kategorien betroffener Personen (z. B. Mandanten, Beschäftigte) und der Kategorien personenbezogener Daten (z. B. mandantenbezogene personenbezogene Daten, Beschäftigtendaten).
- Die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden [einschließlich der Empfänger in Drittländern (Achtung: Eine Übertragung in Drittländer kann auch bei der Inanspruchnahme von IT-Diensten gegeben sein, ohne dass man sich dessen zwingend bewusst ist.)]. Dies können z. B. Gegner des Mandanten, deren anwaltliche Vertreter, Versicherungen, Gerichte und Behörden sein.
- Wenn möglich, die vorgesehenen Löschfristen der verschiedenen Datenkategorien (z. B. bei Bewerberdaten sechs Monate nach Mitteilung der ablehnenden Entscheidung, bei Mandatsakten die Aufbewahrungspflichten für Handakten (§ 50 Abs. 1 Satz 2 BRAO), die steuerrechtlichen Aufbewahrungspflichten und ggf. die aufgrund der Verjährung vorgegebenen Fristen).
- wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gem. Art. 32 Abs. 1 DS-GVO.

Die Vorgaben für das von Auftragsverarbeitern zu führende Verzeichnis enthält Art. 30 Abs. 2 DS-GVO. (Rechtsanwälte können keine Auftragsverarbeiter sein, da sie als Organe der Rechtspflege nicht weisungsgebunden sind.)

Das **Kurzpapier zum Verzeichnis von Verarbeitungstätigkeiten** der Datenschutz-Konferenz findet sich hier: https://www.bfdi.bund.de/DE/Home/Kurzmeldungen/DSGVO_Kurzpapiere1-3.html.

Das **Muster eines Verarbeitungsverzeichnisses** als Word-Dokument findet sich hier: <https://datenschutz.sachsen-anhalt.de/informationen/internationales/datenschutz-grundverordnung/verzeichnis-der-verarbeitungstaetigkeiten-nach-artikel-30-ds-gvo/>

Die **GDD-Praxishilfe** zur DS-GVO V zum **Verzeichnis von Verarbeitungstätigkeiten** inklusive eines Musters kann unter diesem Link eingesehen werden https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_5.pdf

18. Wem ist das Verarbeitungsverzeichnis vorzulegen?

Das Verarbeitungsverzeichnis bzw. „das Verzeichnis der Verarbeitungstätigkeiten“ muss vom Rechtsanwalt auf Anfrage der Aufsichtsbehörde vorgelegt werden, damit die Verarbeitungsvorgänge anhand des Verzeichnisses kontrolliert werden können (Art. 30 Abs. 4 DS-GVO, Erwägungsgrund 82).

19. Gibt es Vorgaben für die Kanzlei-Angestellten?

Der Beschäftigtendatenschutz ist in § 26 Abs. 1 Satz 1 BDSG-neu geregelt. Danach dürfen personenbezogene Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, soweit dies für die Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich ist. Anderenfalls ist die Verarbeitung auf eine Einwilligung gem. § 26 Abs. 2 oder 3 BDSG zu stützen (siehe dazu auch Frage 6).

Für Bewerber gilt gemäß § 26 Abs. 8 Satz 2 BDSG-neu das gleiche, sie gelten als Beschäftigte.

Nach Beendigung des Arbeitsverhältnisses gelten zum Teil nachvertragliche Aufbewahrungsfristen. Diese können sich insbesondere aus dem SGB, dem EStG, der AO oder dem ArbZG ergeben.

Bewerberunterlagen unterliegen keinen gesetzlichen Aufbewahrungsfristen. Insoweit kann die Klagefrist nach dem AGG auch datenschutzrechtlich erste Orientierung bieten. Diese beträgt nach § 15 Abs. 4 AGG zwei Monate seit Zugang der Ablehnung.

Bei Auszubildenden sind grundsätzlich dieselben Grundsätze wie bei den sonstigen Beschäftigten daten heranzuziehen.

Bei Aufnahme der Tätigkeit hat eine Verpflichtung der Mitarbeiter auf Vertraulichkeit zu erfolgen. Diese beinhaltet, dass der Verantwortliche die ihm unterstellten natürlichen Personen über die datenschutzrechtlichen Anforderungen zu informieren und auf diese zu verpflichten hat (vgl. Art. 24 Abs. 1, 28 Abs. 3 Satz 2 lit. b), 32 Abs. 4, 39 Abs. 1 lit. a) DS-GVO). Dabei unterscheidet sich diese Verpflichtung von der Verpflichtung auf das Anwaltsgeheimnis. Wie eine derartige Verpflichtung zu erfolgen hat, schreibt die DS-GVO nicht vor. Angesichts der Rechenschaftspflicht des Art. 5 Abs. 2 DS-GVO bietet sich jedoch eine schriftliche oder elektronische Form an.

Das **Kurzpapier zum Beschäftigtendatenschutz** der Datenschutz-Konferenz kann unter folgendem Link eingesehen werden: https://www.bfdi.bund.de/DE/Home/Kurzmeldungen/DSGVO_Kurzpapiere1-3.html.

20. Muss eine Verpflichtung der Kanzlei-Mitarbeiter auf die Vertraulichkeit erfolgen?

Das BDSG a. F. sah eine sog. „Verpflichtung auf das Datengeheimnis“ vor. Diese Vorgabe ist in der DS-GVO explizit nicht enthalten. Aus einer Reihe von Vorschriften ergibt sich jedoch, dass der Verantwortliche „die ihm unterstellten natürlichen Personen“ über die datenschutzrechtlichen Anforderungen zu informieren und auf diese verpflichten hat (vgl. Art. 24 Abs. 1, 28 Abs. 3 Satz 2 lit. b, 32 Abs. 4, 39 Abs. 1 lit. a DS-GVO). Der Inhalt dieser Verpflichtung unterscheidet sich von der „Verpflichtung auf das Anwaltsgeheimnis“. Die DS-GVO schreibt nicht vor, wie diese Verpflichtung zu erfolgen hat. In Anbetracht der Rechenschafts- und damit zusammenhängenden Nachweispflicht nach Art. 5 Abs. 2 DS-GVO empfiehlt die DSK (Kurzpapier Nr. 19) diese in schriftlicher oder elektronischer Form vorzunehmen. Die Verpflichtung hat zudem bei Aufnahme der Tätigkeit zu erfolgen. Die Verpflichtung auf das Anwaltsgeheimnis und die Verpflichtung auf das Datengeheimnis in einem Dokument ist möglich und angeraten.

Weitere **Hinweise** zur Einhaltung dieser Pflicht sowie eine **Mustererklärung** finden Sie im genannten **DSK Kurzpapier Nr. 19** über die Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen nach DS-GVO findet sich hier:

https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_19.pdf

Die **GDD-Praxishilfe zur DS-GVO** zur Verpflichtung auf die Vertraulichkeit inkl. Mustererklärung findet sich hier:

https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_11.pdf

Das **Muster der Belehrung** für die Kanzleimitarbeiter der **RAK Sachsen** finden Sie hier:

<https://www.rak-sachsen.de/documents/2018/05/muster-formular-belehrung-mitarbeiter-datenschutz.pdf/>

21. Müssen Rechtsanwälte eine Datenschutz-Folgenabschätzung durchführen?

Gem. Art. 35 DS-GVO muss **vorab** eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchgeführt werden, wenn eine Form der Verarbeitung aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

Im Regelfall müssen Rechtsanwälte keine Datenschutzfolgenabschätzung durchführen. Nur bei Zweifelsfällen muss ausnahmsweise eine Datenschutz-Folgenabschätzung (DSFA) gem. Art. 35 DS-GVO durch Rechtsanwälte durchgeführt werden. Erwägungsgrund 91, Satz 4 und 5 zur DS-GVO sieht eine Ausnahme für **Einzelanwälte** vor. Einige Länder sowie die DSK schränken derzeit in ihren Listen von Verarbeitungsvorgängen, für die ein DSFA durchzuführen ist, die Verpflichtung auf „**Große Anwaltssozietäten**“ ein.

Das **Kurzpapier Nr. 5 zur Datenschutz-Folgenabschätzung** der Datenschutz-Konferenz kann unter folgendem Link eingesehen werden:

https://www.bfdi.bund.de/DE/Home/Kurzmeldungen/DSGVO_Kurzpapiere1-3.html

Die **Liste der Datenschutz-Konferenz für den nicht-öffentlichen Bereich zu Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist**, finden Sie hier:

https://www.lidi.nrw.de/mainmenu_Aktuelles/submenu_EU-Datenschutzreform/Inhalt/EU-Datenschutzreform/DSK_DSFA_Muss-Liste_Version_1_1_Deutsch.pdf

Bespielhaft für die Länder steht die Liste von Verarbeitungsvorgängen nach Art. 35 Abs. 4 DS-GVO des ULD Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein unter https://www.datenschutzzentrum.de/uploads/datenschutzfolgenabschaetzung/20180525_LfD-SH_DSFA_Muss-Liste_V1.0.pdf .

Die die **GDD-Praxishilfe DS-GVO X zu den Voraussetzungen der Datenschutz-Folgenabschätzung** findet sich hier: https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_10.pdf

22. Hat die Tatsache, dass ein Rechtsanwalt eine Datenschutz-Folgenabschätzung durchführen muss, Auswirkungen auf die Frage der Bestellung eines Datenschutzbeauftragten?

Ja. Gem. § 38 Abs. 1 Satz 2 BDSG-neu muss der Rechtsanwalt, der ausnahmsweise eine Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO durchführen muss, unabhängig von der Anzahl der in der Kanzlei beschäftigten Personen, einen Datenschutzbeauftragten benennen.

23. Gibt es Vorgaben zur Sicherheit der Verarbeitung?

In Art. 32 DS-GVO werden Vorgaben zur Sicherheit der Verarbeitung gemacht. Art. 32 Abs. 1 DS-GVO sieht vor: *„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 treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen 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.“*

Bei der Beurteilung des angemessenen Schutzniveaus sind gem. Art. 32 Abs. 2 DS-GVO *„insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.“*

24. Müssen Rechtsanwälte verschlüsselt kommunizieren?

Bei der Beantwortung der Frage sind neben datenschutzrechtlichen Aspekten auch berufs- und strafrechtliche Aspekte zu beachten. Zu der Frage, ob eine Verschlüsselungspflicht gegeben ist bzw. ob und unter welchen Bedingungen unverschlüsselt kommuniziert werden darf, wird verwiesen auf den Beitrag von Rechtsanwalt Dr. Hendrik Schöttle, *Anwaltliche Kommunikation per E-Mail – nur verschlüsselt?*, BRAK-Mitt. 2018, 118 ff. sowie Rechtsanwalt Dr. Lutz Martin Keppler, CR 2019, 18 ff..

25. Gibt es Meldepflichten bei der Verletzung des Datenschutzes?

Die DS-GVO sieht Meldepflichten gegenüber der Aufsichtsbehörde und gegenüber den Betroffenen vor.

Im Falle einer Verletzung des Schutzes personenbezogener Daten muss der Rechtsanwalt grundsätzlich unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der zuständigen **Aufsichtsbehörde** - in der Regel auch online – melden; es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt (Art. 33 Abs. 1 Satz 1 DS-GVO). Der Ausnahmefall kann z. B. gegeben sein, wenn der Laptop eines Rechtsanwalts verloren geht, aber die Daten auf dem Gerät verschlüsselt sind. Die Mindestangaben der Meldung sind in Art. 33 Abs. 3 DS-GVO aufgelistet.

Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.

Der Kanzleiinhaber als Verantwortlicher muss Verletzungen des Schutzes personenbezogener Daten einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten dokumentieren. Dazu gehören auch deren Auswirkungen und die ergriffenen Abhilfemaßnahmen. Diese Dokumentation soll der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen nach Art. 33 DS-GVO ermöglichen.

Zudem muss der Rechtsanwalt die von der Verletzung des Schutzes personenbezogener Daten **betroffene Person** unverzüglich benachrichtigen (Art. 34 DS-GVO), wenn aus der Datenschutzverletzung ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen folgt. In klarer und einfacher Sprache muss der Rechtsanwalt die Art der Verletzung und die in Art. 33 Abs. 3 DS-GVO genannten Mindestangaben mitteilen.

Eine **Benachrichtigung des Betroffenen** ist **nicht erforderlich**, wenn eine der folgenden Bedingungen erfüllt ist:

- a) *„der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt wurden, insbesondere solche, durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden, etwa durch Verschlüsselung,*
- b) *der Verantwortliche durch nachfolgende Maßnahmen sichergestellt hat, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 aller Wahrscheinlichkeit nach nicht mehr besteht,*

- c) *dies mit einem unverhältnismäßigen Aufwand verbunden wäre. In diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.“*
- d) Eine weitere aus Sicht der Rechtsanwaltschaft relevante Ausnahme regelt § 29 Absatz 1 Satz 3 BDSG. Hiernach besteht auch keine Meldepflicht, soweit durch die Benachrichtigung Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen. Allerdings ist die betroffene Person zu benachrichtigen, wenn die Interessen der betroffenen Person, insbesondere unter Berücksichtigung drohender Schäden, gegenüber dem Geheimhaltungsinteresse überwiegen (§ 29 Absatz 1 Satz 4 BDSG).

Eine Handreichung zur Meldepflicht von Datenschutzverletzungen des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit, der auf den Guidelines des Europäischen Datenschutzausschusses basiert, finden Sie hier:

<https://datenschutz-hamburg.de/pages/hinweise-databreach/>

26. Wer ist für die Aufsicht über Rechtsanwälte zuständig?

Die Aufsicht in berufsrechtlichen Angelegenheiten liegt bei der Rechtsanwaltskammer.

Die Aufsicht über die ordnungsgemäße Verarbeitung personenbezogener Daten und die Einhaltung der DS-GVO und des BDSG liegt bei den datenschutzrechtlichen Aufsichtsbehörden. Aufsichtsbehörde für Rechtsanwälte ist die jeweilige Landesdatenschutz-Aufsichtsbehörde, ggf. nach den Regelungen der Landes-Datenschutzgesetze. Gem. Art. 31 DS-GVO ist der Rechtsanwalt, d. h. der Kanzleiinhaber oder der Partner, verpflichtet, auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammenzuarbeiten.

27. Welche Befugnisse hat die Datenschutz-Aufsichtsbehörde?

Die Aufsichtsbehörde hat weitreichende Befugnisse, die in Art. 58 DS-GVO normiert sind. Sie kann u. a. Untersuchungen in Form von Datenschutzüberprüfungen durchführen und Zugang zu allen personenbezogenen Daten und Informationen, die zur Erfüllung ihrer Aufgaben notwendig sind, erhalten. Dies gilt auch für Rechtsanwaltskanzleien, allerdings im Bereich der beruflichen Verschwiegenheit eingeschränkt durch das Verbot der Offenbarung mandatsbezogener Informationen.

Die Aufsichtsbehörde verfügt zudem über sämtliche Abhilfebefugnisse. Sie kann u. a. den Kanzleiinhaber als Verantwortlichen anweisen, den Anträgen der betroffenen Person auf Ausübung der ihr zustehenden Rechte zu entsprechen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DS-GVO zu bringen und die von einer Verletzung des Schutzes personenbezogener Daten betroffene Person entsprechend zu benachrichtigen. Darüber hinaus kann die Aufsichtsbehörde vorübergehende oder endgültige Beschränkungen der Verarbeitung, einschließlich eines Verbots, verhängen.

Die Aufsichtsbehörde kann zudem gem. Art. 58 Abs. 2 i DS-GVO eine Geldbuße gem. Art. 83 DS-GVO verhängen, zusätzlich zu oder anstelle von Maßnahmen nach Art. 58 Abs. 2 DS-GVO, je nach den Umständen des Einzelfalls.

Der deutsche Gesetzgeber hat von der Öffnungsklausel des Art. 90 DS-GVO Gebrauch gemacht und zum Schutz von Berufsgeheimnissen mit § 29 BDSG-neu abweichende Regelungen geschaffen: Danach ist einer staatlichen Aufsichtsbehörde insbesondere der Zugang zu personenbezogenen Daten und Informationen einer Anwaltskanzlei ebenso verwehrt, wie der Zugang zu deren Räumlichkeiten oder Computeranlagen (§ 29 Abs. 3 BDSG-neu i. V. m. Art. 58 Abs. 2 Ziff. e und f DS-GVO).

28. Sehen die DS-GVO und das BDSG-neu Sanktionen vor?

Die allgemeinen Bedingungen für die Verhängung von Geldbußen sind in Art. 83 DS-GVO geregelt.

„Jede Aufsichtsbehörde soll sicherstellen, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen die DS-GVO gemäß den Absätzen 4, 5 und 6 in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist“ (vgl. Art. 83 Abs. 1 DS-GVO).

„Geldbußen werden je nach den Umständen des Einzelfalls zusätzlich zu oder anstelle von Maßnahmen nach Artikel 58 Absatz 2 Buchstaben a bis h und j verhängt. Bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag wird in jedem Einzelfall Folgendes gebührend berücksichtigt:

- a) *Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung sowie der Zahl der von der Verarbeitung betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens;*
- b) *Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes;*
- c) *jegliche von dem Verantwortlichen oder dem Auftragsverarbeiter getroffenen Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens;*
- d) *Grad der Verantwortung des Verantwortlichen oder des Auftragsverarbeiters unter Berücksichtigung der von ihnen gemäß den Artikeln 25 und 32 getroffenen technischen und organisatorischen Maßnahmen;*
- e) *etwaige einschlägige frühere Verstöße des Verantwortlichen oder des Auftragsverarbeiters;*
- f) *Umfang der Zusammenarbeit mit der Aufsichtsbehörde, um dem Verstoß abzuhelpen und seine möglichen nachteiligen Auswirkungen zu mindern;*
- g) *Kategorien personenbezogener Daten, die von dem Verstoß betroffen sind;*
- h) *Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, insbesondere ob und gegebenenfalls in welchem Umfang der Verantwortliche oder der Auftragsverarbeiter den Verstoß mitgeteilt hat;*
- i) *Einhaltung der nach Artikel 58 Absatz 2 früher gegen den für den betreffenden Verantwortlichen oder Auftragsverarbeiter in Bezug auf denselben Gegenstand angeordneten Maßnahmen, wenn solche Maßnahmen angeordnet wurden;*

- j) *Einhaltung von genehmigten Verhaltensregeln nach Artikel 40 oder genehmigten Zertifizierungsverfahren nach Artikel 42 und*
- k) *jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall, wie unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste“ (vgl. Art. 83 Abs. 2 DS-GVO).*

Es können Geldbußen von bis zu 20 000 000 Euro oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt werden, je nachdem, welcher der Beträge höher ist (Art. 83 Abs. 5 DS-GVO). Diese Regelung greift u. a. bei Verstößen gegen die Rechte der betroffenen Person gem. Art. 12 bis 22 DS-GVO, z. B. bzgl. der Informationspflichten.

Auch das **BDSG-neu** enthält Sanktionen, denn Art. 84 Abs. 1 DS-GVO ermöglicht es den Mitgliedstaaten, andere Sanktionen für Verstöße gegen die Verordnung festzulegen.

So sieht § 43 Abs. 1 BDSG für bestimmte Verstöße **Bußgelder** bis zu einer Höhe von 50.000 Euro vor.

Nach § 42 BDSG Abs. 1 und 2 BDSG-neu drohen **Freiheitsstrafen** von 2 bzw. 3 Jahren oder **Geldstrafe**, wenn nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen ohne Berechtigung einem Dritten übermittelt oder auf andere Art und Weise zugänglich gemacht werden oder diese Daten verarbeitet oder durch unrichtige Angaben erschlichen werden und hierbei gegen Entgelt oder in der Absicht gehandelt wird, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.

Diese Taten werden gem. § 42 Abs. 3 BDSG-neu jedoch **nur auf Antrag** verfolgt.

29. Haften Rechtsanwälte bei Datenschutz-Verstößen?

Rechtsanwälte können sich Schadensersatzforderungen ausgesetzt sehen. Jede Person, der wegen eines Verstoßes gegen die DS-GVO ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadensersatz gegen den Verantwortlichen, d. h. den Kanzleihinhaber, oder gegen den Auftragsverarbeiter. Der Kanzleihinhaber haftet somit für den Schaden, der durch eine nicht den Vorgaben der DS-GVO entsprechende Verarbeitung verursacht wurde (Art. 82 DS-GVO).

Dabei ist in Art. 82 Abs. 3 DSGVO eine **Beweislastumkehr** normiert: „Der Verantwortliche oder der Auftragsverarbeiter wird von der Haftung gemäß Absatz 2 befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.“

30. Wo findet man Informationen und praktische Hinweise zur DS-GVO?

„Checkliste für Rechtsanwälte zur EU-Datenschutz-Grundverordnung“ – Hinweise des Ausschusses Datenschutzrecht (Stand: Mai 2018): https://www.brak.de/w/files/02_fuer_anwaelte/2018-05_checkliste-rae-zur-dsgvo-final.pdf

Erläuterungen zur „Checkliste für Rechtsanwälte zur EU-Datenschutz-Grundverordnung“ (Stand: Mai 2018): https://www.brak.de/w/files/02_fuer_anwaelte/2018-05_erlaeuterungen-zur-checkliste-rae-zur-dsgvo.pdf

Herb „Die Datenschutz-Grundverordnung der EU“ in BRAK-Mitt. 2017, 209:
https://www.brak.de/w/files/01_ueber_die_brak/herb-brak-mitt.-2017-209.pdf

Dreßler/Mathis „Was bringt die Datenschutz-Grundverordnung für Anwaltskanzleien?“ in BRAKMag 2/2018, 16: https://www.brak.de/w/files/01_ueber_die_brak/dressler-mathis-brakmagazin_2018_02.pdf

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) hat sog. Kurzpapiere zu verschiedenen Themen veröffentlicht:
https://www.bfdi.bund.de/DE/Home/Kurzmeldungen/DSGVO_Kurzpapiere1-3.html

Die Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD) hat Praxishilfen zur DS-GVO veröffentlicht: <https://www.gdd.de/gdd-arbeitshilfen/praxishilfen-ds-gvo/praxishilfen-ds-gvo>

Der bitkom hat Leitfäden zur datenschutzkonformen Datenverarbeitung nach der DS-GVO veröffentlicht: <https://www.bitkom.org/Themen/Datenschutz-Sicherheit/DSGVO.html>

Die Informationsplattform der Stiftung Datenschutz ist ab dem 25.05.2018 hier zu finden:
<https://stiftungdatenschutz.org/dsgvo-info/>

Die Informationen der RAK München „Erste-Hilfe-Paket“ zum Datenschutz in Anwaltskanzleien ist hier einsehbar: <https://rak-muenchen.de/rechtsanwaelte/mitgliederservice/datenschutz-in-anwaltskanzleien.html>

* * *