BUNDESRECHTSANWALTSKAMMER

Checkliste für Rechtsanwälte zur EU-Datenschutz-Grundverordnung

Hinweise des Ausschusses Datenschutzrecht – Stand: Mai 2018

Inhaltsverzeichnis

1. Beschreibung

Die EU-Datenschutz-Grundverordnung (DS-GVO)[1] und das neue Bundesdatenschutzgesetz (BDSG-neu)[2] gelten ab dem 25.05.2018. Eine übersichtliche Darstellung über deren Regelungen und Auswirkungen auch auf die Anwaltschaft finden Sie bei Herb „*Die Datenschutz-Grundverordnung der EU*“.[3] Im Folgenden werden die wesentlichen datenschutzrechtlichen Anforderungen exemplarisch und ohne Anspruch auf Vollständigkeit dargestellt. Dies geschieht bewusst in Frageform, da Rechtsanwältinnen und Rechtsanwälte sich mit dieser Thematik befassen und dabei diesen Fragestellungen stellen müssen. Zu beachten ist dabei, dass nicht jede/r verantwortliche Rechtsanwältin/Rechtsanwalt pauschal alle diese Anforderungen erfüllen muss und sich auch der Umfang, wie die einzelnen Anforderungen konkret berücksichtigt werden müssen, fallbezogen unterscheidet. Zur Erläuterung der Anforderungen wird ergänzend auf weiterführendes Material hingewiesen (z. B. auf Kurzpapiere[4] und Hinweise[5] der Datenschutzkonferenz (DSK), auf die Informationsbroschüre des BfDI[6] und Informationen der EU-Kommission[7], Praxishilfen der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD) zur DS-GVO[8] u. a.).

2. Rechtsanwalt als Verantwortlicher, Rechtmäßigkeit der Verarbeitung

Jede Rechtsanwältin und jeder Rechtsanwalt sowie jede Rechtsanwaltsgesellschaft (§59c BRAO), die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet, ist ein sog. **Verantwortlicher** (Art. 4 Nr. 7 DS-GVO). Dieser ist ggf. gemeinsam mit anderen insbesondere dafür verantwortlich, dass er die Anforderungen der DS-GVO einhält.

Die Voraussetzungen der **Rechtmäßigkeit** der Verarbeitung sind in Art. 6 DS-GVO festgelegt. Bei der Bearbeitung insbesondere der Mandantendaten liegt die Rechtsgrundlage regelmäßig im zugrundeliegenden Mandatsvertrag (Art. 6 Abs. 1b DS-GVO), bei Mitarbeiterdaten im Arbeitsvertrag. Auch nach Beendigung des Mandats bzw. der Beschäftigung können nachvertragliche Pflichten die Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten bilden. Wenn möglich sollte man es vermeiden, mit Einwilligungen zu arbeiten, da diese frei widerruflich sind und den Anforderungen von Art. 7 und/oder Art. 8 DS-GVO entsprechen müssen.

Die DS-GVO enthält an verschiedenen Stellen spezielle **Dokumentationspflichten**, beispielsweise in Art. 30 (Verarbeitungsverzeichnis), Art. 33 Abs. 5 (Dokumentation von Datenschutzvorfällen) oder Art. 28 Abs. 3 a (Dokumentation von Weisungen im Rahmen von Auftragsverarbeitungsverhältnissen).

- Gibt es ein Bewusstsein in Ihrer Kanzlei dafür, dass Datenschutz „Chefsache“ ist, beispielsweise durch Regelung der Verantwortlichkeiten, Bewusstsein über Datenschutzrisiken, Transparenz

---

[1] Die EU-Datenschutz-Grundverordnung ist am 04.05.2016 im Amtsblatt der EU (ABl. EU-Nr. L 119/1) veröffentlicht worden und findet unmittelbare Anwendung in den Mitgliedstaaten ab dem 25.05.2018.

[2] Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutzanpassung-und -Umsetzungsgesetz-EU, DSAnpUG-EU, BGBl. 2017, 2097

[3] BRAK-Mitt. 2017, 209: https://www.brak.de/w/files/01_ueber_die_brak/herb-brak-mitt.-2017-209.pdf

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

[5] https://www.bfdi.bund.de/DE/Datenschutz/DatenschutzGVO/Aktuelles/Aktuelles_Artikel/Muster_Verzeichnis_Verarbeitungstaetigkeiten.html?nn=5217040

[6] https://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/INFO6.pdf?__blob=publicationFile&v=48

[7] https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_de

[8] https://www.gdd.de/gdd-arbeitshilfen/praxishilfen-ds-gvo/praxishilfen-ds-gvo

über Zielkonflikte (z. B. zwischen den Betroffenenrechten und dem anwaltlichen Geheimnisschutz)?

- Gibt es für jede Verarbeitungstätigkeit im Zusammenhang der Berufsausübung eine Dokumentation, mit der Sie die Rechtmäßigkeit Ihrer Verarbeitung (Art. 6 DS.GVO) nachweisen können (Art. 5 Abs. 2 DS-GVO)?

- Haben Sie geprüft, ob die Einwilligungen, auf die Sie ggf. eine Verarbeitung stützen, noch den Voraussetzungen der Art. 7 und/oder Art. 8 DS-GVO entsprechen? Können Sie das Vorliegen der Einwilligung nachweisen?

- Haben Sie ggf. ein Datenschutzmanagementsystem installiert, um sicherzustellen und den Nachweis erbringen zu können, dass Ihre Verarbeitung gemäß der DS-GVO erfolgt (Art. 24 Abs. 1 DS-GVO)?

- Haben Sie bei gemeinsamer Verantwortung eine Vereinbarung nach Art. 26 DS-GVO getroffen?

3. Datenschutzbeauftragter

In der Regel ist nur dann ein Datenschutzbeauftragter vom Verantwortlichen zu benennen, wenn mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind (Art. 37 DS-GVO, erweitert durch § 38 Abs. 1 BDSG-neu. Das bedeutet, dass ein Datenschutzbeauftragter bestellt werden muss, wenn mindestens zehn oder mehr Personen Zugang zur Kanzlei-EDV haben (dabei ist der Zugang zu E-Mails ausreichend), unabhängig vom Tätigkeitsumfang (auch Teilzeitkräfte). Es kann ein Angestellter der Kanzlei oder Externer bestellt werden. Für angestellte Datenschutzbeauftragte gelten besondere Kündigungsschutzregelungen. Ein Partner darf auch nicht zum Datenschutzbeauftragten bestellt werden, weil er Verantwortlicher ist.

- Muss ein Datenschutzbeauftragter vom Rechtsanwalt benannt werden?

- Wenn ja, sind dessen Kontaktdaten gem. Art. 37 Abs. 8 DS-GVO der zuständigen Aufsichtsbehörde mitgeteilt worden?

- Welche sonstigen Aufgaben hat der Datenschutzbeauftragte neben dieser Funktion in der Kanzlei? Ist er u. U. von seiner sonstigen Tätigkeit zumindest zum Teil freizustellen?

4. Verzeichnis von Verarbeitungstätigkeiten

Jeder Verantwortliche muss ein Verzeichnis seiner Verarbeitungstätigkeiten führen (Art. 30 Abs. 1 DS-GVO).

Wesentliche Verarbeitungstätigkeiten sind z. B.: Verarbeitung von Mandantendaten zur Beratung, Vertretung und Rechnungsstellung, Verarbeitung von Daten des Anspruchsgegners des Mandanten zur Beratung, Vertretung und Rechnungsstellung, Betrieb der Webseite über Dienstleister, Gehaltsabrech-

nung der Mitarbeiter. An dieser Stelle wird u.a. auf ein in der DSK abgestimmtes Muster eines Verarbeitungsverzeichnisses[9] verwiesen.

- Haben Sie ein aussagekräftiges Verarbeitungsverzeichnis aller Verarbeitungstätigkeiten erstellt, das die Angaben z. B. bezüglich Zwecken, Kategorien personenbezogener Daten, Empfängern und/oder Löschfristen enthält?

5. Datenschutz-Verpflichtung von Beschäftigten

Bei der Aufnahme der Tätigkeit sind Beschäftigte, die mit personenbezogenen Daten umgehen, zu informieren und dahingehend zu verpflichten, dass die Verarbeitung der personenbezogenen Daten auch durch sie nach den Grundsätzen der DS-GVO erfolgt (Art. 29, 32 Abs. 4 DS-GVO).

- Haben Sie alle Mitarbeiter, die mit personenbezogenen Daten umgehen, verpflichtet? Es bietet sich an, dies mit der Verpflichtung auf das Anwaltsgeheimnis zu verknüpfen.

- Ist die Verwendung beruflicher Kommunikationsmittel für private Zwecke erlaubt (Telefon/Handy, Smartphone, PC/Laptop, Internet, E-Mail)? Gibt es Festlegungen zur privaten Nutzung beruflicher Kommunikationsmittel?

- Ist die Verwendung privater Kommunikationsmittel für berufliche Zwecke erlaubt (z. B. Smartphone, Laptop)? Gibt es Festlegungen zur beruflichen Nutzung privater Kommunikationsmittel?

6. Informationspflichten und Auskunftsrechte

Jeder Verantwortliche hat den betroffenen Personen schon bei der Datenerhebung bestimmte Informationen über die Verarbeitung ihrer Daten zu geben. Zumindest muss er darauf hinweisen, wo die Informationen leicht zugänglich sind (z. B. Anlage zum Anwaltsvertrag, Homepage). Die betroffenen Personen haben auch das Recht, Auskunft über die Verarbeitung ihrer Daten zu erhalten. Art. 13 Abs. 4, 14 Abs. 5 DS-GVO sowie § 29 BDSG-neu – im Hinblick auf die berufsrechtliche Geheimhaltungspflicht des Rechtsanwalts nach § 43a Abs. 2 BRAO – enthalten differenzierte Ausnahmen, die im Einzelfall zu prüfen sind.

- Haben Sie bestehende Informationspflichten, insbesondere bei Beginn des Mandats, sowie auf der Webseite in der Datenschutzerklärung geprüft?

- Haben Sie Ihre Texte zur datenschutzrechtlichen Information der betroffenen Personen bei der Datenerhebung an die Anforderungen nach Art. 13 bzw. 14 DS-GVO angepasst?

---

[9] Das Muster eines Verarbeitungsverzeichnisses als Word-Dokument finden Sie unter folgendem Link: 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

- Haben Sie geprüft, inwieweit in die Texte insbesondere folgende Informationen neu aufgenommen werden müssen? Dies betrifft ggf. folgende Informationen:

  - Kontaktdaten des Datenschutzbeauftragten;

  - Rechtsgrundlage(n) für die Verarbeitung personenbezogener Daten: Erfüllung des Mandatsvertrags (Art. 6 Abs. 1 b DS-GVO;

  - Darüber hinaus, falls Sie die Verarbeitung mit Ihren berechtigten Interessen oder berechtigten Interessen eines Dritten (Art. 6 Abs. 1 f DS-GVO) begründen: die berechtigten Interessen;

  - Dauer der Speicherung; sofern nicht möglich, die Kriterien für die Festlegung dieser Dauer:

  - Bestehen der Rechte betroffener Personen auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, auf Widerspruch aufgrund besonderer Situation einer betroffenen Person sowie auf Datenportabilität;

  - Sofern Verarbeitung auf Einwilligung beruht: das Recht zum jederzeitigen Widerruf der Einwilligung, Recht auf Beschwerde bei der Aufsichtsbehörde;

  - Ob die Bereitstellung der Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist;

  - Sofern Sie die Daten nicht bei der betroffenen Person erhoben haben: aus welcher Quelle die personenbezogenen Daten stammen und ggf. ob sie aus öffentlich zugänglichen Quellen stammen.

- Haben Sie ein Verfahren eingerichtet, um Anträge von betroffenen Personen auf Auskunft zu den eigenen Daten nach Art. 15 DS-GVO zeitnah und vollständig erfüllen zu können (Art. 12 Abs. 1 DS-GVO)?

- Haben Sie Verfahren eingerichtet, um Anträge auf Datenübertragbarkeit betroffener Personen erfüllen zu können (Art. 20 DS-GVO)?

7. Löschen von personenbezogenen Daten

Sobald keine gesetzliche Grundlage (z. B. berufsrechtliche Aufbewahrungspflicht, § 50 Abs. 1 BRAO) mehr für die Speicherung von personenbezogenen Daten besteht, sind diese zu löschen. Dies ergibt sich aus dem Grundsatz nach Art. 5 Abs. 1 e) DS-GVO („Speicherbegrenzung“) und Art. 17 DS-GVO.

- Wie haben Sie sichergestellt, dass datenschutzrechtliche Belange bei Beginn oder Änderung eines jeden Mandats in Ihrer Kanzlei in Hinblick auf die Löschung von Daten Berücksichtigung finden (datenschutzfreundliche Voreinstellungen, Art. 25 DS-GVO)?

- Haben Sie ein Verfahren eingerichtet, um begründete Anträge von betroffenen Personen auf Löschung (Art. 17 DS-GVO) und Einschränkung der Verarbeitung (Art. 18 DS-GVO) erfüllen zu können?

8. Sicherheit der Verarbeitung und Organisation

Um die personenbezogenen Daten bei der Verarbeitung zu schützen, sind viele Standardmaßnahmen hilfreich. Dazu gehören u. a. aktuelle Betriebssysteme und Anwendungen, Passwortschutz, Firewall, regelmäßige Backups, Virenscanner und Benutzerrechte. Bei der Kommunikation mit Mandanten ist jedoch darauf zu achten, dass eine ausreichende Verschlüsselung eingesetzt wird.[10]

- Haben Sie Ihre bestehenden Prozesse zur Überprüfung der Sicherheit der Verarbeitung auf die neuen Anforderungen des Art. 32 DS-GVO angepasst?

- Haben Sie insbesondere bestehende Checklisten zur Auswahl von technischen und organisatorischen Maßnahmen durch eine risikoorientierte Betrachtungsweise auf Basis von Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten ersetzt?

- Wurde ein geeignetes Managementsystem zur regelmäßigen Überprüfung, Bewertung und Verbesserung der Security-Maßnahmen umgesetzt?

- Wurden Schutzmaßnahmen wie Pseudonymisierung und der Einsatz von kryptographischen Verfahren zum Schutz vor unbefugten oder unrechtmäßigen Verarbeitungen sowohl bezüglich externer als auch interner „Angreifer“ umgesetzt?

- Haben Sie die Daten z. B. bei der Verwendung mobiler Datenträger (z. B. Laptop) außerhalb der Kanzlei, z. B. durch Verschlüsselung besonders gesichert?

- Werden Altgeräte bzw. Altdatenträger (z. B. Kopierer mit Festplatte) vor der Abgabe an Dritte sicher gelöscht?

- Werden Altakten datenschutz- und berufsrechtsgerecht entsorgt?

9. Auftragsverarbeitung

Sobald Verantwortliche Dienstleistungen (z. B. IT-Wartung oder Webhosting) in Anspruch nehmen, um personenbezogene Daten in Ihrem Auftrag durch andere Unternehmen verarbeiten zu lassen, ist ein schriftlicher Vertrag zur Auftragsverarbeitung erforderlich (Art. 28 DS-GVO). Muster der DSK finden sie hier.[11] Eine Datenverarbeitung durch das besondere elektronische Anwaltspostfach (beA) beruht auf gesetzlicher Grundlage und stellt keine Auftragsdatenverarbeitung im Sinne des Art. 28 DS-GVO dar.[12]

- - Haben Sie eine Übersicht über die Auftragsverarbeiter?

---

[10] Schöttle *„Anwaltliche Kommunikation per E-Mail – nur verschlüsselt? Und wenn ja – wie?* BRAK-Mitt. 2018, erscheint in Heft 3/2018

[11] https://datenschutz.sachsen-anhalt.de/informationen/internationales/datenschutz-grundverordnung/verzeichnis-der-verarbeitungstaetigkeiten-nach-artikel-30-ds-gvo/

[12] Es ist nicht erforderlich, Vereinbarungen über die Auftragsverarbeitung im Sinne von Art. 28 DSGVO zwischen der BRAK und den das beA nutzenden Rechtsanwälten abzuschließen. Da die bereichsspezifischen Vorschriften der §§ 31a, 31c BRAO, 22 Abs. 2 Satz 1 RAVPV das Verhältnis zwischen den an der Datenverarbeitung beteiligten Stellen vorrangig regeln, liegt ein gesetzlicher Erlaubnistatbestand für die Datenübermittlung an das beA und die Datenverarbeitung durch das beA vor. Die Datenverarbeitung ist auf der Grundlage von Art. 6 Abs. 1 e), Abs. 3 DSGVO in Verbindung mit §§ 31a, 31c BRAO, 22 Abs. 2 Satz 1 RAVPV zulässig.

- Haben Sie mit allen Ihren Auftragsverarbeitern (z. B. mit. dem IT-Dienstleister für Webseite und Wartung der Kanzlei-IT) die erforderlichen Vereinbarungen mit dem Mindestinhalt nach Art. 28 Abs. 3 DS-GVO abgeschlossen?

10. Datenschutzverletzungen/Meldepflichten

Kommt es bei der Verarbeitung personenbezogener Daten zu Sicherheitsvorfällen (z. B. Diebstahl, Hacking, Fehlversendung, Verlust von Geräten mit unverschlüsselten Mandantendaten), so bestehen gesetzliche Meldepflichten: Im Ausnahmefall kann die Aufsichtsbehörde unter Wahrung der Verschwiegenheit in Kenntnis zu setzen sein.

- Haben Sie gem. Art. 33 DS-GVO sichergestellt, dass eine Meldung von Verletzungen des Schutzes personenbezogener Daten innerhalb von 72 Stunden möglich ist?

- Haben Sie insbesondere sichergestellt, dass Datenschutzverletzungen in Ihrer Kanzlei erkannt werden können?

- Haben Sie dazu eine geeignete Methode zur Ermittlung eines Risikos bzw. eines hohen Risikos in Ihrer Kanzlei eingeführt?

- Haben Sie einen Prozess aufgesetzt, wie mit potentiellen Verletzungen kanzleiintern umzugehen ist?

- Haben Sie festgelegt, wer, wann und wie mit der für Sie zuständigen Datenschutzaufsichtsbehörde kommuniziert?

- Haben Sie Verfahren eingerichtet, um Ihrer Benachrichtigungspflicht gegenüber betroffenen Personen erfüllen zu können z. B. beim Verlust von Mitarbeiterdaten (Art. 34 DS-GVO, § 29 BDSG-neu)?

11. Datenschutz-Folgeabschätzung

Hat eine Verarbeitung personenbezogener Daten ein hohes Risiko für die betroffenen Personen, so muss das spezielle Instrument der Datenschutz-Folgenabschätzung durchgeführt werden (Art. 35 DS-GVO). Ein solch hohes Risiko für die Rechte und Freiheiten natürlicher Personen ist bei Rechtsanwältinnen und Rechtsanwälten häufig gegeben. Erwägungsgrund 91, S. 4 und 5 zur DS-GVO sieht unter bestimmten Umständen eine Ausnahme für Einzelanwälte vor. [13]

Wenn eine Datenverarbeitung vorliegt, die eine Datenschutz-Folgenabschätzung gem. Art. 35 DS-GVO erfordert, muss gem. § 38 Abs. 1 Satz 2 BDSG-neu ein Datenschutzbeauftragter benannt werden, unabhängig von der Anzahl der mit der Datenverarbeitung beschäftigten Personen.

Bei Rechtsanwälten mit umfangreicher Tätigkeit insbesondere in den Bereichen der Art. 9 und 10 DS-GVO (z. B. Daten zur Religion, zur Gesundheit, zu Straftaten) sollte die Verpflichtung zur Datenschutz-Folgenabschätzung (auch bei Unterschreitung der „10er-Grenze“) im Einzelfall geprüft werden.

---

[13] „(91) …Die Verarbeitung personenbezogener Daten sollte nicht als umfangreich gelten, wenn die Verarbeitung personenbezogene Daten von Patienten oder von Mandanten betrifft und durch einen einzelnen Arzt, sonstigen Angehörigen eines Gesundheitsberufes oder Rechtsanwalt erfolgt. In diesen Fällen sollte eine Datenschutz-Folgenabschätzung nicht zwingend vorgeschrieben sein.“

- Haben Sie als Rechtsanwalt eine Datenschutz-Folgenabschätzung durchzuführen?

- Verarbeiten Sie besondere Kategorien von personenbezogenen Daten i. S. v. Art. 9 und 10 DS-GVO z. B. Gesundheitsdaten in umfangreicher Weise?

- Haben Sie sich auf die evtl. Notwendigkeit der Durchführung einer Datenschutz-Folgenabschätzung vorbereitet?

- Haben Sie eine geeignete Methode zur Bestimmung der Frage, ob eine Datenschutz-Folgenabschätzung durchzuführen ist, in Ihrer Kanzlei eingeführt?

- Haben Sie eine geeignete Risikomethode zur Durchführung einer Datenschutz-Folgenabschätzung in Ihrer Kanzlei eingeführt?

- Haben Sie sich für einen Prozess der Datenschutz-Folgenabschätzung entschieden; haben Sie diesen schon einmal getestet?

* * *