DSGVO: Der Leitfaden für Anwaltskanzleien

Seit dem 25. Mai 2018 sind die Regelungen der Datenschutzgrundverordnung (DSGVO) nebst der Neufassung des Bundesdatenschutzgesetzes (BDSG) wirksam. Durch das Inkrafttreten der einheitlichen Regelung zum Datenschutz werden die Persönlichkeitsrechte der europäischen Bürger gestärkt. Bei datenverarbeitenden Stellen führt die DSGVO aber oftmals zu Unsicherheit darüber, wie den Regelungen rechtskonform entsprochen werden kann. Folgender Leitfaden bietet eine „Sofort-Hilfe" zur Einrichtung eines DSGVO-konformen Datenschutzes in der Kanzlei.

Gerade Anwaltskanzleien verarbeiten personenbezogene Daten und vor allem auch besondere personenbezogene Daten zur Erbringung ihrer Dienstleistungen. Die Anforderungen der Berufsgeheimnisträgerschaft sind zwar bereits in der Bundesrechtsanwaltsordnung geregelt, dennoch sind die Datenschutzprinzipien und etwaige Abweichungen davon bei den Verarbeitungstätigkeiten der Kanzleien genau zu prüfen und zu dokumentieren. Für Kanzleien, die besondere personenbezogene Daten, typischerweise in arbeits-, familien-, erb- und strafrechtlichen Fällen verarbeiten, sind weitergehende Schutzmaßnahmen zu erwägen.

Inhalt

25. Mai 2018, Nils Möllers (externer Datenschutzbeauftragter)

Schritt 1: Der Datenschutzbeauftragte

Jede Rechtsanwaltskanzlei muss die Regeln der DSGVO und des neuen BDSG beachten. Die Pflicht, einen Datenschutzbeauftragten zu bestellen, hängt von der Größe der Kanzlei und der Art der Datenverarbeitung ab.

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

Wann muss eine Kanzlei einen Datenschutzbeauftragten bestellen?

Eine Kanzlei muss einen Datenschutzbeauftragen bestellen, wenn sie eines oder mehrere der folgenden Kriterien erfüllt:

- Sie beschäftigt mehr als 9 Mitarbeiter und diese verarbeiten Daten automatisiert (Computer). Für die Zählung ist es unerheblich, ob es sich um Auszubildende, Teilzeit- oder Vollzeitkräfte handelt.
- Sie übermittelt geschäftsmäßig personenbezogene Daten zum Beispiel an eine Auskunft.
- Sie verarbeitet besondere personenbezogene Daten zum Beispiel zu Gesundheit, Bonität, ethnischer Herkunft, politischer Meinung, religiösen Überzeugungen, Gewerkschaftszugehörigkeit oder Sexualleben einer Person.

Der Datenschutzbeauftragte muss unabhängig und frei von Interessenkollisionen sein (Art. 38 Abs. 6 S. 2 DSGVO). Somit können folgende Personen keine Datenschutzbeauftragten sein:

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

In kleinen und mittleren Kanzleien sind nicht selten alle Rechtsanwälte auch Partner. Das bedeutet, dass keiner der Rechtsanwälte Datenschutzbeauftragter werden kann. Ein angestellter Rechtsanwalt kann hingegen zum Datenschutzbeauftragten bestellt werden. Dabei ist zu beachten, dass für Datenschutzbeauftragte ein besonderer Kündigungsschutz gilt.

Schritt 2: Organisation und Dokumentation

Wenn die Zuständigkeiten für die Überwachung der Datenschutzbestimmungen vergeben wurden, müssen alle notwendigen Informationen zur weiteren Dokumentationsarbeit gesammelt werden. Hierbei geht man im Rahmen einer Bestandsaufnahme wie folgt vor:

1. Verzeichnis der Verarbeitungstätigkeiten

Art. 30 DSGVO schreibt die Führung eines Verzeichnisses aller Verarbeitungstätigkeiten vor. Das Verzeichnis dient dem Nachweis einer DSGVO-konformen Datenverarbeitung in der Kanzlei. Im Falle fehlender Datenschutzdokumentation muss zunächst ermittelt werden, in welchen Fällen personenbezogene Daten z. B. von Mandanten, Partnern oder Beschäftigten erhoben und verarbeitet werden. Hierzu bietet es sich an, alle innerhalb der IT-Infrastruktur des Unternehmens eingesetzten Anwendungen und Tools aufzulisten, in denen personenbezogene Daten gespeichert werden. Dies hilft bei der Ermittlung der Datenflüsse im

Unternehmen und kann zugleich als Grundlage für das Verzeichnis von Verarbeitungstätigkeiten dienen.

Als Verarbeitungstätigkeiten gelten beispielsweise:

- Elektronische Anwaltsakten
- Kanzleisoftware wie RA-MICRO
- Elektronische Diktier- und Spracherkennungsprogramme
- Buchhaltungssoftware (Finanzbuchhaltung und Lohnbuchhaltung)
- Software zum Versenden und Verwalten von E-Mails
- Adressdatenbanken
- Software zur Terminverwaltung
- Elektronische Personalakten
- Betriebliches Intranet

Für die Erstellung des Verzeichnisses der Verarbeitungstätigkeiten ist kein Muster vorgeschrieben, allerdings müssen für jede Verarbeitungstätigkeit folgende Inhalte beschrieben werden:

- Name und Kontaktdaten der Kanzlei
- ggf. Name und Kontaktdaten des betrieblichen Datenschutzbeauftragten
- Zwecke der Datenverarbeitung
- Rechtsgrundlage der Verarbeitung
- Bezeichnung der Personen, deren Daten verarbeitet werden (z. B. Mandanten, Beschäftigte oder Lieferanten)
- Art der verarbeiteten Datenkategorien (z. B. Personenstammdaten, Personaldaten)
- Empfänger, an die Daten übermittelt werden oder worden sind
- Datenübermittlung in die USA oder in ein anderes Land außerhalb der EU (z. B. bei der Nutzung von Webmail-Diensten oder anderen Cloud-Diensten)
- Löschfristen
- Maßnahmen der Datensicherheit nach Art. 32 DSGVO
- Risikoabschätzung
- Datenschutz-Folgenabschätzung

2. Auftragsverarbeitung

Bei der Datenverarbeitung bedienen sich Kanzleien meist der Unterstützung von Dienstleistern. Dies können IT-Servicefirmen sein oder auch Cloud-Dienstleister für die Textverarbeitung, Terminverwaltung oder Spracherkennung. All diese Verfahren waren bereits nach bisherigem Recht als Auftragsdatenverarbeitung anzusehen mit der Folge, dass es entsprechender Verträge bedurfte. Hieran ändert sich nichts, allerdings müssen bestehende Verträge an das neue Recht angepasst werden. Sofern noch keine Verträge existieren, sollte ein Vertragsschluss nachgeholt werden.

Anfangs ist zu erheben, mit welchen Dienstleistern/Dritten bereits Vereinbarungen zur Verarbeitung von Daten geschlossen wurden (Auftragsdatenverarbeitungsvereinbarungen ADV nach BDSG alt). Alle Vereinbarungen sind zentral zu erfassen, einschließlich der Anlagen TOM (technische und organisatorische Maßnahmen). Falls Vereinbarungen nicht schriftlich abgeschlossen wurden, ist dies nach BDSG nachzuholen. Die Vereinbarungen heißen jetzt nach der DSGVO Auftragsvereinbarungsvertrag (AVV) und die TOM sind individualisiert abzufassen, weshalb sie zukünftig auch als Schutzmaßnahmen bezeichnet werden können. Sobald der Status erfasst ist, ist bei den Dienstleistern abzufragen, ob sie bereits DSGVO-Mustervereinbarungen für ihre Kunden vorbereitet haben, welche die Kanzlei nach Prüfung und ggf. Kontrolle der Datenverarbeitung sowie Anpassung der Beschreibung der Schutzmaßnahmen abschließen kann.

Zum Beispiel wird Google mit Websiteanalysen beauftragt, andere Anbieter mit dem Versand von Werbemailings. Für dieses Auftragsverhältnis sieht die DSGVO nach Art. 28 Abs. 3 S. 1 den Abschluss eines AVV vor, aus dem sich, verglichen mit den Mindestanforderungen der DSGVO, deutlich höhere Anforderungen ergeben. Hierbei müssen gesetzliche Vorgaben zur Vertragsgestaltung eingehalten werden. Im Folgenden ein grober Überblick über Angaben, die ein solcher Vertrag enthalten muss:

- Auftraggeber und Auftragnehmer
- Kategorien der verarbeiteten Daten (beispielsweise E-Mail-Adressen oder Namen)
- Kategorien der Personen, deren Daten verarbeitet werden (beispielsweise Kunden)
- Zweck der Verarbeitung (beispielsweise Google Analytics)
- Verpflichtungen hinsichtlich der Befolgung von Weisungen oder der Genehmigung von Kontrollen
- Bestimmungen hinsichtlich des Zustimmungserfordernisses bei der Beauftragung von Subunternehmern und der Mitwirkung und Information
- Vertragsdauer
- Technisch-organisatorische Schutzmaßnahmen und sonstige Garantien
- Liste der Subunternehmer

3. Technische und organisatorische Maßnahmen

Technische und organisatorische Maßnahmen (TOM) sind zu ergreifen, um die Sicherheit der in der Kanzlei verarbeiteten Personendaten zu gewährleisten (Art. 32 DSGVO). Die Vorschrift konkretisiert den Grundsatz der „Integrität und Vertraulichkeit“ gem. Art. 5 Abs. 1 lit. f DSGVO. Folgende Maßnahmen sind vorgeschrieben:

- Verschlüsselung: Soweit möglich, sollen personenbezogene Daten verschlüsselt werden. Es empfiehlt sich beispielsweise, die Verschlüsselung von E-Mails mit Verschlüsselungsprogrammen zu ermöglichen.
- Stabilität: Die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme ist auf Dauer sicherzustellen. Hierzu bedarf es der Einschätzung einer IT-Fachfirma oder eines fachkundigen Mitarbeiters.
- Wiederherstellbarkeit: Verarbeitungsprozesse müssen durch eine fachgerechte Datensicherung gegen Datenverlust geschützt werden. Auch hierzu bedarf es der Unterstützung durch IT-Fachleute.
- Regelmäßige Überprüfung: Gab es bisher keine Unterstützung durch eine IT-Fachfirma, kann es ratsam sein, sich über eine zukünftige Beauftragung Gedanken zu machen.

Es sollte eine Dokumentation (TOM-Report) geben, die die Bemühungen um technische und organisatorische Maßnahmen zur Datensicherheit und deren Durchführung belegt. Der Verpflichtung, die Maßnahmen zur Datensicherheit im Verzeichnis zu beschreiben, kann Genüge getan werden, indem auf dieses Papier im Verarbeitungsverzeichnis verwiesen wird.

Checkliste für den TOM-Report

Die nachfolgend genannten Punkte sind als „Checkliste“ gedacht und sollten mit einem IT-Fachmann besprochen werden. Das Ziel der Besprechung sollte die Erstellung eines Berichts sein, der die Maßnahmen dokumentiert, die die Kanzlei zur Datensicherheit ergriffen hat.

a) Zugangskontrolle

Um zu verhindern, dass Unbefugte Zugang zu Verarbeitungsanlagen erhalten, können folgende Maßnahmen ergriffen werden:

- Installation einer Alarmanlage
- Chipkarten-/Transponder-Schließsystem
- Abschließbare Serverschränke
- Sorgfältige Auswahl des Reinigungspersonals
- Sicherheitsschlösser

b) Datenträgerkontrolle

Die Datenträgerkontrolle soll verhindern, dass Unbefugte Datenträger lesen, kopieren, verändern oder löschen können. Zum Beispiel durch:

- Sichere Aufbewahrung von Datenträgern
- Einrichtung von Standleitungen bzw. VPN-Tunneln
- Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- Verschlüsselung von (mobilen) Datenträgern
- Ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)
- Einsatz von Aktenvernichtern bzw. Dienstleistern zur Aktenvernichtung (nach Möglichkeit mit Datenschutz-Gütesiegel)
- Protokollierung der Vernichtung

c) Speicher- und Zugriffskontrolle

Die Maßnahmen der Speicher- und Zugriffskontrolle sollen sicherstellen, dass zur Benutzung eines automatisierten Verarbeitungssystems berechtige Personen ausschließlich auf die personenbezogenen Daten zugreifen können, die von ihrer Zugangsberechtigung umfasst werden. Außerdem soll verhindert werden, dass Unbefugte personenbezogene Daten einsehen, verändern oder löschen sowie neue Daten anlegen können. Hierzu zählen:

- Festlegung von Berechtigungen in den IT-Systemen
- Differenzierte Berechtigungen für das Lesen, Löschen und Ändern von Daten
- Differenzierte Berechtigungen für Daten, Anwendungen und Betriebssysteme
- Verwaltung der Rechte durch Systemadministratoren
- Reduktion der Anzahl der Administratoren auf das notwendige Minimum
- Passwortrichtlinie inkl. Passwortlänge und Passwortwechsel
- Protokollierung von Zugriffen auf Anwendungen

d) Benutzerkontrolle

Die Benutzerkontrolle soll verhindern, dass Unbefugte automatisierte Verarbeitungssysteme mit Hilfe von Datenübertragung nutzen können. Zum Beispiel durch:

- Festlegung zugangsberechtigter Mitarbeiter
- Erstellen von Benutzerprofilen
- Passwortvergabe
- Authentifikation mit Benutzername/Passwort
- Regelmäßige Kontrolle von Berechtigungen
- Sperrung von Berechtigungen ausscheidender Mitarbeiter
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Einsatz von Verschlüsselungstechnologie
- Einsatz von Antivirensoftware

e) Übertragungs- und Transportkontrolle

Die Übertragungs- und Transportkontrolle soll feststellen, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können. Zudem soll sie sicherstellen, dass bei der Übermittlung personenbezogener Daten und beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden. Zum Beispiel durch:

- Einrichtung von Standleitungen bzw. Verschlüsselungstechnologien
- Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
- Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarte Löschfristen

f) Wiederherstellbarkeit und Datenintegrität

Zur schnellen Wiederherstellung von Systemen im Störungsfall und um die Beschädigung personenbezogener Daten durch Fehlfunktionen des Systems zu verhindern, können z. B. folgende Vorbereitungen getroffen werden:

- Erstellen eines Backup- & Recoverykonzepts
- Festplattenspiegelung nach Vereinbarung mit dem Auftraggeber
- Testen von Datenwiederherstellung
- Erstellen eines Notfallplans

g) Zuverlässigkeit

Um zu gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden, bieten sich folgende Maßnahmen an:

- Unabhängig voneinander funktionierende Systeme
- Automatisierte Meldung von Fehlfunktionen
- Virenschutz

h) Verfügbarkeitskontrolle

Die Verfügbarkeitskontrolle dient dem Schutz personenbezogener Daten gegen Zerstörung oder Verlust. Hierzu zählen:

- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Feuerlöschgeräte in Serverräumen
- Aufbewahrung der Datensicherung an einem sicheren, ausgelagerten Ort
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- Erstellen eines Notfallplans

Schritt 3: Datenschutzerklärung

(Potenzielle) Mandanten müssen über alle Vorgänge aufgeklärt werden, bei denen ihre personenbezogenen Daten verarbeitet werden. Personenbezogen sind alle Angaben, die Rückschlüsse auf eine konkrete Person erlauben. Das ist beim Namen oder der E-Mail-Adresse in der Regel der Fall. Auch IP-Adressen sind personenbezogene Daten, über deren Verarbeitung aufzuklären ist.

Jede Datenschutzerklärung muss den Namen und die Kontaktdaten (Anschrift und E-Mail-Adresse) des Website-Betreibers enthalten. Wurde ein Datenschutzbeauftragter bestellt, müssen dessen Kontaktdaten (Anschrift und/oder E-Mail-Adresse) aufgeführt werden. Der Name des Datenschutzbeauftragten muss nicht genannt werden. Diese Informationen können z. B. am Anfang oder am Ende der Datenschutzerklärung eingebaut werden.

Für jedes Tool auf der Website, das personenbezogene Daten verarbeitet, müssen separat mindestens Angaben zum Zweck und der Rechtsgrundlage der Datenverarbeitung gemacht werden. Dazu zählen:

- Facebook „Like“-Buttons oder ähnliche Social-Media-Plug-ins anderer Anbieter (Twitter, LinkedIn etc.)
- Webformulare (Kontaktformulare, Newsletter etc.),
- Cookies (Informationen zu Zweck, Empfänger der Daten etc.)
- Analyse-Tools wie Google Analytics oder etracker
- Retargeting- bzw. Audience Optimisation Tools (z. B. AddThis, Facebook-Pixel)

Datenschutzerklärungen sollten von jeder Seite der Website aus abrufbar sein. Dazu wird z. B. am Ende der Website (Footer) ein mit „Datenschutz“ betitelter Link zur Unterseite mit der Datenschutzerklärung platziert.

Die Texte der Datenschutzerklärung müssen so formuliert sein, dass alle relevanten Informationen mitgeteilt werden und gleichzeitig die Formulierungen leicht verständlich sind. Dies stellt eine Herausforderung an die Formulierungskunst der Website-Betreiber dar.

Checkliste für die Datenschutzerklärung nach der DSGVO

Diese Inhalte müssen, sofern sie auf der Kanzlei-Homepage zur Verfügung stehen, in der Datenschutzerklärung enthalten sein:

- Verantwortliche Stelle
- Datenschutzbeauftragter/Datenschutzansprechpartner
- Rechtsgrundlage der Verarbeitung
- Erstellung der Cookies
- Erstellung von Log-Files
- Registrierung auf der Website
- Kontaktformular
- Newsletter
- Online-Shop
- Blog
- Rechte der betroffenen Personen
- Widerspruchsrecht
- Weitergabe an Dritte (Google Analytics, Fonts, Maps etc.)
- Schlussbestimmungen

Schritt 4: Rechenschaftspflichten nach Art. 5 Abs. 2 DSGVO

In der DSGVO findet sich keine dem alten § 5 BDSG entsprechende Regelung und damit auch keine Verpflichtung auf das Datengeheimnis. Nach den Vorgaben der DSGVO sind Unternehmen jedoch verpflichtet, jederzeit den Nachweis erbringen zu können, dass sie die Grundsätze für die Verarbeitung personenbezogener Daten einhalten. Hierzu gehört der Grundsatz der „Integrität und Vertraulichkeit“ (Art. 5 Abs. 1 lit. f DSGVO), also der Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, vor Verlust, unbeabsichtigter Zerstörung oder Schädigung personenbezogener Daten. Daneben sehen auch die Vorgaben zu den technisch-organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit im Unternehmen nach Art. 32 Abs. 4 DSGVO vor, dass Unternehmen als Verantwortliche sicherzustellen haben, dass die ihnen unterstellten Personen mit Zugang zu personenbezogenen Daten nur auf entsprechende Weisung hin tätig werden.

Durch eine Verpflichtung der Mitarbeiter auf Vertraulichkeit können Unternehmen ihren Rechenschafts- und Nachweispflichten nachkommen. Dies sollte vor Aufnahme der datenverarbeitenden Tätigkeit erfolgen und ein Merkblatt zur Datenschutzrichtlinie sowie zu den einschlägigen datenschutzrechtlichen Bestimmungen beinhalten.

Schritt 5: Mitarbeiterschulung

Datenschutzschulungen stärken das Problembewusstsein der Mitarbeiter für datenschutzrelevante Fragestellungen. Die DSGVO sieht daher die Überwachung der Sensibilisierung und die Schulung von Mitarbeitern als Aufgabe des Datenschutzbeauftragten vor (Art. 39 Abs. 1 lit. b DSGVO). Bei den Datenschutzschulungen für Mitarbeiter stehen drei Ziele im Vordergrund:

- Bewusstsein für datenschutzrechtliche Probleme schaffen
- Mitarbeiter zu datenschutzkonformem Verhalten befähigen
- Bereitschaft zu datenschutzkonformem Verhalten fördern

Datenschutzschulungen werden mitunter wenig ernst genommen. Eine gewisse Sensibilität kommt häufig erst auf, wenn es zu einem schwerwiegenden Datenschutzvorfall kommt. Dabei müssen Datenschutzschulungen nicht langweilig sein. Diese können durch webbasierte E-Learning ressourcenschonend und unterhaltsam abgehalten werden.