Steuerberater-ONLINE-GmbH

Datenschutz

Online-Seminar

Dirk Munker, Datenschutz-Auditor (TÜV)

© DWS Steuerberater-Online-GmbH

Inhaltsverzeichnis

I. Vorbemerkung

Seit dem 25.05.2016 ist die **EU-Datenschutz-Grundverordnung („DS-GVO“)** in Kraft. An jenem Tag begann eine 2-jährige Übergangszeit, die den Kanzleien die Gelegenheit geben sollte, ihre Prozesse an die neuen Gegebenheiten anzupassen. Im Gegensatz zur bis dahin geltenden Datenschutz-(„DS“-) Richtlinie aus dem Jahr 1995, die erst nach der Umsetzung in nationales Recht auch national Anwendung fand, gilt die DS-GVO unmittelbar in allen EU-Mitgliedstaaten seit dem 25.05.2018.

Bereits das Bundesdatenschutzgesetz („BDSG“) in seiner bisherigen Form legt einer Steuer-(„St.“-) Kanzlei umfangreiche Pflichten im Bereich DS auf. Es gilt, das **„Grundrecht auf informationelle Selbstbestimmung“** sicherzustellen und die **Daten der Betroffenen** (Mandanten, Mitarbeiter [„MA“], Geschäftspartner etc.) **vor Missbrauch zu schützen**. Kanzleien mit > 9 MA’ern, die ständig personenbezogene Daten verarbeiten, haben deshalb die Pflicht, einen DS-Beauftragten („DSB“) zu bestellen. Dies („[…] die ständig personenbezogene Daten verarbeiten“) trifft in einer St.-Kanzlei im Grunde auf jeden MA zu. Verarbeiten in einer Kanzlei < 10 Mitarbeiter regelmäßig personenbezogene Daten, liegt die Umsetzung sämtl. DS-relevanter Themen in den Händen der Kanzlei-Leitung. An dieser Vorgabe hat sich seit dem 25.05.2018 im Grunde nichts geändert; das BDSG-NEU spricht nicht mehr von „mehr als 9“, sondern von „ab 10 MA’ern“[1].

Aus Gründen der besseren Lesbarkeit wird im folgenden Text i. d. R. von der „Kanzlei“ oder vom „Verantwortlichen“ gesprochen. Dieses Skript soll kleine und mittelgroße Kanzleien informieren, damit diese ihre Organisation und Prozesse ggf. schnellstmöglich an die neue Rechtslage anpassen können.

II. Datenschutz-relevante Themen

Die Themen im DS-Management(-„Mg’t“) der Kanzlei reichen

- vom DS-konformen Internet-Auftritt
- über die Kontrolle der Dienstleister,
- die Beschreibung und Bewertung sämtl. DS-relevanter Prozesse in der Kanzlei
- bis hin zur Sensibilisierung der MA.

Es gab und gibt viel zu tun für den DSB, denn DS wird oft vernachlässigt. Das Gefährdungs-Potenzial steigt jedoch durch die moderne Technik stetig an (jederzeitige Verfügbarkeit von Daten, leichtes Erstellen von Profilen und Quer-Verbindungen, Apps zum mobilen Zugriff auf Berufsgeheimnis-Daten etc.).

---

1 Zwecks größerer Lesefreundlichkeit sind auch die kursiv gesetzten, zitierten Texte (ggü. der jeweiligen veröffentlichten Version) rein redaktionell modifiziert wiedergegeben, u. a. durch Verwendung von Abkürzungen wie ›DS‹ oder ›MA‹.

III. Die EU-Datenschutz-Grundverordnung (DS-GVO) und das Bundesdatenschutzgesetz (BDSG)

Seit dem 25.05.2016 hat sich die DS-Welt grundlegend geändert. Die DS-GVO hat weitreichende Auswirkungen auf alle Kanzleien. Seit dem 25.05.2018 sind in Dtland sowohl deren Vorgaben als auch die Vorgaben des BDSG-NEU zu beachten. Dieses Gesetz wurde am 05.07.2017 mit dem *„Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU — DSAnpUG-EU)"* im BGBl. veröffentlicht und wird auch weiterhin die Bezeichnung „Bundesdatenschutzgesetz" (BDSG) innehaben.

Alle Entscheidungsträger sollten sich der Auswirkungen der DS-GVO bewusst sein und wissen, was diese für den Alltag in ihrer Kanzlei bedeutet.

Betrachten wir zunächst die Vorgaben seitens der EU.

Die DS-GVO …

- regelt das Recht auf **Schutz personenbezogener Daten** als **Grundrecht** innerhalb der EU,
- vereinheitlicht weitgehend die 28 nationalen Gesetze, die diesbezüglich innerhalb der EU bis dahin bestanden,
- **erhöht die Sanktionen** drastisch (bis zu 10 € / 20 Mio. € bzw. 2 % / 4 % des weltweiten Jahres-Umsatzes),
- wird durch die Aufsichtsbehörden voraussichtlich wesentlich **strenger sanktioniert** als das zuvor der Fall war,
- beinhaltet eine **Melde-Pflicht** innerhalb von **72 Stunden** („Std.") und eine **Beweislast-Umkehr**,
- setzt wesentlich mehr an Dokumentation voraus als das BDSG-ALT,
- bringt neue Aspekte wie „***privacy by design***" **und** „***privacy by default***", **Rechenschafts-Pflicht, Risiko-Bewertung,**
- **ist seit dem 25.05.2018 EU-weit in Kraft!**

Das BDSG-NEU regelt die Punkte, die die DS-GVO im Rahmen sog. Öffnungs-Klauseln den Mitgliedstaaten überlässt, u. a. die **Bestellung eines DSB,** wenn in der Kanzlei „i. d. R. **mindestens 10 Personen ständig […] personenbezogen[e] Daten [verarbeiten]**"[2]. Im Zweifel gehen stets die Regelungen der DS-GVO denen des BDSG vor.

Soweit zu einigen Eckdaten. Mit Gelten der DS-GVO gibt es jedoch noch zahlreiche weitere und teils neue Aspekte zu beachten.

- Zwar entfällt die bisherige Pflicht, ein sog. „Jedermann-Verzeichnis" vorzuhalten, doch muss die Kanzlei bei jeder Erhebung personenbezogener Daten dem Betroffenen nun umfangreiche Informationen zur Verfügung stellen.
  - Dies reicht von den Prozessen, in denen personenbezogene Daten verarbeitet werden, über Informationen zur Kanzlei-Leitung und zum DSB bis hin zum Widerspruchs-Recht und zur DS-Aufsichtsbehörde, bei der sich der Betroffene beschweren könnte, wenn er einen rechtswidrigen Umgang mit seinen Daten befürchtet.

---

2 Vgl. § 38 BDSG.

- Waren Daten-Pannen
  - bislang (nur dann) an Aufsichtsbehörde und Betroffene zu melden, wenn sensible Daten — wie z. B. Gesundheits-Daten oder Bank-/Kreditkarten-Daten — natürl. Personen betroffen waren,
  - so gilt die Melde-Pflicht an die Aufsichtsbehörde zukünftig für nahezu alle personenbezogenen Daten, wobei die Meldefrist auf 72 Std. verkürzt wurde.

Das Verfahrens-Verzeichnis, zukünftig „Verzeichnis der Verarbeitungs-Tätigkeiten“ — in dem jeder einzelne personenbezogene Daten verarbeitende Prozess in der Kanzlei beschrieben wird —, ist um eine Risiko-Bewertung zu ergänzen. Ggf. ist bei hohem Rest-Risiko zudem noch eine sog. „DS-Folgenabschätzung“ erforderlich.

Die Schulung und Sensibilisierung der MA bleibt auch weiterhin unerlässlich.

Auf den DSB kommt künftig eine verstärkte Überwachungs-Pflicht hinsichtlich der Einhaltung der Regelungen aus DS-GVO, BDSG-NEU und internen Richtlinien zu.

Die Kanzlei unterliegt nunmehr einer „Rechenschafts-Pflicht“ und muss im Falle einer DS- oder Datensicherheits-Panne sowie einer Kontrolle durch die Aufsichtsbehörde nachweisen können, welche Maßnahmen implementiert wurden, um Pannen zu verhindern. Hierdurch kommen auch weitere Anforderungen bzgl. der Dokumentation der IT-Infrastruktur und der IT-Sicherheitsmaßnahmen auf die Kanzlei zu. Sollte dennoch etwas passieren, sieht die DS-GVO empfindl. Bußgelder bis zu 20 Mio. € oder 4 % des weltweiten Jahres-Umsatzes vor.

Fasst man die Grundsätze der DS-GVO zusammen, so handelt es sich um:

- Rechtmäßigkeit der Daten-Verarbeitung,
- Verarbeitung nach Treu und Glauben
- Transparenz,
- Zweckbindung,
- Daten-Sparsamkeit und Speicher-Begrenzung,
- Richtigkeit und Aktualität,
- Integrität und Vertraulichkeit sowie
- unabhängige Kontrolle.

Auf die Punkte „Rechtmäßigkeit der Verarbeitung“ und „individuelle DS-Rechte“ wird an dieser Stelle besonders eingegangen.

IV. Grundsätze der DS-GVO und des BDSG-neu

1. Rechtmäßigkeit der Verarbeitung

a) Einwilligung

Die DS-GVO rückt die **Einwilligung der Betroffenen** stärker in den Fokus als dies das BDSG-ALT tat. Immer dann, wenn keine Rechts-(„R.“-)Grundlage vorhanden ist, muss der Betroffene seine Einwilligung ausdrücklich erklären. Der Betroffene muss stets in der Lage sein, seine Einwilligung zu verweigern oder zu widerrufen, ohne dabei Nachteile zu erleiden.

Auf Betreiben des Europäischen Parlaments wurde zusätzlich ein sog. **„Kopplungs-Verbot**“ mit in die DS-GVO aufgenommen. Dies soll verhindern, dass Betroffene Angebote im Internet nur dann nutzen können, wenn sie hierbei Daten von sich preisgeben, die für die Nutzung des entsprechenden Dienstes nicht erforderlich sind.

Die Wirksamkeit einer Einwilligung hängt zudem davon ab, dass der Betroffene sie **„informiert“** erteilt. Aus diesem Grund muss im Zuge der Einwilligung darüber informiert werden, wer der **Verantwortliche** ist und zu welchem **Zweck** die Einwilligung erfolgt. Werden im Zuge einer solchen Einwilligung erstmals personenbezogene Daten von Betroffenen erhoben, so gilt es, noch weitere Angaben zu machen, auf die wir unter Punkt IV. 2. a) („Information“) eingehen werden.

Die Einwilligung selbst muss in **leichter und verständlicher Sprache** verfasst sein. Die Schriftform ist im Grunde nicht gefordert, der Verantwortliche muss aber im Zuge seiner Rechenschafts-Pflicht nachweisen können, dass eine Einwilligung vorliegt. Neben dem bereits etablierten Verfahren *„Double-Opt-in“*[3] bei Einwilligungen in den Newsletter-Bezug gibt es jedoch derzeit im Grunde keine Alternativen zur Schriftform.

Für die Einwilligung von Kindern gelten spezielle Regelungen, wobei die DS-GVO hier eine Altersgrenze von 16 Jahren vorsieht. Diese Grenze kann von den Mitgliedstaaten bis auf ein Mindestalter von 13 Jahren herabgesenkt werden, wovon Dtland allerdings keinen Gebrauch gemacht hat.

- Dies bezieht sich jedoch nicht auf Einwilligungen im berufl. oder gewerbl. Bereich, sondern einzig auf Einwilligungen bei einem **Angebot von Diensten der Informations-Gesellschaft**, z. B. soziale Netzwerke, Chats oder Online-Foren.
- Es ist zu erwarten, dass sich in der Praxis diesbezüglich noch viele Fragen stellen werden.

Bereits erteilte Einwilligungen gelten fort, wenn sie DS-GVO-konform erteilt wurden.

> **▶ Praxis-Tipp** Kanzleien sind gut beraten, ihre Prozesse bzgl. des Einholens von Einwilligungen zu überprüfen.
>
> Vergessen Sie nicht, die Anmeldung zum Newsletter-Bezug DS-konform zu gestalten (*„Double-Opt-in“*-Verfahren). Beim *„Double-Opt-in“* muss die in einem ersten Schritt erfolgte Eintragung in eine Newsletter-Abonnentenliste in einem zweiten Schritt (deshalb *„double“*) bestätigt werden. Hierzu wird i. d. R. eine E-Mail-Nachricht mit Bitte um Bestätigung an die eingetragene E-Mail-Adresse gesendet. Die Registrierung erfolgt beim *„Double-Opt-in“* erst dann, wenn der Wunsch zur Registrierung mit dem Reagieren auf diese E-Mail (per Anklicken eines Buttons bzw. per Antwort) bestätigt wird. Dieses Verfahren hat sich mittlerweile im E-Mail-Marketing in Dtland durchgesetzt.
>
> Denken Sie auch an Daten-Erhebungen im Rahmen von *Tracking* der Besucher des Internet-Auftritts! Als „Tracking“ bezeichnet man die Technik, mit der das Nutzer-Verhalten im Internet analysiert werden kann. Dafür gibt es spezielle Tracking-Tools wie z. B. GOOGLE ANALYTICS. In der Regel nutzt man hierfür Cookies oder Zähl-Pixel.

3 *Näheres zu diesem Verfahren wird im Kasten „Praxis-Tipp“ auf der folgenden Seite erläutert.*

b) Weitere Verarbeitungs-Grundlagen

Die DS-GVO erlaubt Daten-Verarbeitungen, die auf der **Erfüllung eines Vertrages** oder eines **vorvertragl. Schuldverhältnisses** beruhen. Entscheidend hierbei ist, dass die Erhebung der Daten für die Erfüllung des Vertrages erforderlich ist, was bei einem St.beratungs-Vertrag zunächst grds. der Fall ist. Entscheidend ist, dass der Mandant im Rahmen der Transparenz über die Daten-Verarbeitung informiert wird (vgl. 4.2.1).

Im **Beschäftigungs-Kontext** kommen verstärkt die Regelungen des BDSG-NEU zum Tragen, da die DS-GVO hier eine Öffnungs-Klausel vorsieht. Beim Einholen von Einwilligungen im Beschäftigungs-Kontext — ein Klassiker ist die **Einwilligung in die Veröffentlichung eines MA-Fotos** auf der Homepage — ist besondere Sorgfalt geboten. Hier wird die Freiwilligkeit der Einwilligung aufgrund des **wirtschaftl. Abhängigkeits-Verhältnisses** oftmals in Frage gestellt.

- Vor diesem Hintergrund ist es wichtig, die Einwilligungen DS-konform und für den MA transparent zu gestalten und ihm ein Widerrufs-Recht einzuräumen. Gerade für die Beendigung des Arbeits-Verhältnisses sollten entsprechende Regelungen bzgl. der Entfernung der Bilder von der Homepage getroffen werden.
- Einwilligungen für die Veröffentlichung von MA-Bildern in sozialen Netzwerken sind etwas komplizierter zu gestalten, können aber durch den DSB mit Sicherheit geregelt werden. Hier müssen weitergehende Vereinbarungen getroffen werden. An dieser Stelle sei auch angemerkt, dass eine ***Social-Media Guideline*** heutzutage fast unvermeidbar ist, wenn man von den MA'ern einerseits Engagement in sozialen Netzwerken in berufl. Interesse erwartet, andererseits aber auch im Privatleben eine gewisse **„Netiquette“** einfordert.

Im Grunde muss für jede Verarbeitung personenbezogener Daten eine RGrundlage vorhanden sein. Auch die DS-GVO setzt somit die Tradition des sog. **„Verbots mit Erlaubnis-Vorbehalt“** fort, sprich: Die Verarbeitung personenbezogener Daten ist grds. verboten, es sei denn, es gibt eine RGrundlage, die diese gestattet. Für eine **Weiter-Verarbeitung** von personenbezogenen Daten muss stets hinterfragt werden, ob die Verarbeitung noch für den ursprüngl. Zweck erfolgt.

▶ Praxis-Tipp Überprüfen Sie alle Prozesse, in denen personenbezogene Daten verarbeitet werden, auf die jeweilige RGrundlage. Sind weitere Einwilligungen erforderlich? Brauchen Sie eine *Social Media Guideline?*

c) Sensible Daten

Die DS-GVO sieht für bestimmte Daten besondere Regelungen vor.

Betrachten wir zunächst die „besonderen Kategorien personenbezogener Daten“, die wir noch aus dem BDSG-ALT kennen. Hierzu gehören im BDSG-NEU …

- rassische und ethnische Herkunft,
- politische Meinungen,
- religiöse oder weltanschauliche Überzeugungen,
- Gewerkschafts-Zugehörigkeit,
- biometrischen Daten zur eindeutigen Identifizierung einer natürl. Person,
- Gesundheits-Daten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürl. Person.

Auch die Verarbeitung von personenbezogenen Daten über strafrechtl. Verurteilungen und Straftaten unterliegt besonderen Auflagen. Gerade die „besonderen Kategorien personenbezogener Daten" kommen im Grunde in jeder St.-Kanzlei vor, auch wenn diese — mit Ausnahme der MA-Daten — durch das Berufsgeheimnis zusätzlichen und vorrangigen Schutz genießen.

> **▶ Praxis-Tipp** Prozesse, in denen solche Daten-Bestände vorhanden sind, sind im Verzeichnis der Verarbeitungs-Tätigkeiten eindeutig zu kennzeichnen. Diese Prozesse müssen einem besonderen Schutz unterliegen. Ggf. muss für diese Prozesse eine DS-Folgenabschätzung durchgeführt werden.

d) Risiko-Bewertung und Datenschutz-Folgenabschätzung

Jeder Prozess in der Kanzlei, in dem personenbezogene Daten verarbeitet werden, ist hinsichtlich des damit verbundenen Risikos für den Betroffenen zu bewerten. Das Risiko für die Kanzlei (Bußgeld oder Kosten für IT-Experten nach Befall mit Schad-Software) spielt dabei keine Rolle. Es geht einzig und allein darum, welche Konsequenzen für den Betroffenen zu befürchten sind, wenn seine Daten offenbart werden.

Potenzielle Schäden können physischer, materieller oder immaterieller Art sein. Die DS-GVO benennt hier beispielhaft

- Diskriminierung,
- Identitäts-Diebstahl,
- finanzielle Verluste,
- Ruf-Schädigung,
- Verlust der Vertraulichkeit

oder

- einen Verstoß gegen das Berufsgeheimnis.

Die Risiko-Bewertung betrachtet hierbei die Eintritts-Wahrscheinlichkeit sowie die Schwere des Risikos. Die ermittelten Risiken müssen dann durch geeignete Abhilfe-Maßnahmen (insbesondere durch technisch-organisatorische Maßnahmen) eingedämmt werden. Führt eine Daten-Verarbeitung dennoch weiter zu einem hohen Risiko für den Betroffenen, so hat die Kanzlei eine sog. DS-Folgenabschätzung vorzunehmen. Hierbei ist stets der Rat des DSB einzuholen, sofern ein solcher benannt wurde.

Eine solche Bewertung wird in den meisten Fällen weder die Kanzlei-Leitung noch der DSB alleine bewerkstelligen können, sondern es werden — je nach Prozess — weitere MA (EDV-Beauftragter, ggf. auch Vertreter von Dienstleistern) zu beteiligen sein. Die Verantwortung für diese Bewertung liegt jedoch bei der Kanzlei-Leitung. Die DS-GVO sieht vor, dass die DS-Aufsichtsbehörden eine Liste der Verarbeitungs-Vorgänge veröffentlichen, bei denen eine solche DS-Folgenabschätzung erforderlich ist.

> **▶ Praxis-Tipp** Verschaffen Sie sich möglichst schnell und umfassend einen Überblick über alle Prozesse in der Kanzlei, in denen personenbezogene Daten verarbeitet werden! Stellen Sie für jeden Prozess die Schutz-Maßnahmen dar. (Mehr dazu beim Punkt „Verzeichnis der Verarbeitungs-Tätigkeiten".)

2. Individuelle Datenschutz-Rechte

a) Information

Der Verantwortliche hat den Betroffenen bei jeder Daten-Verarbeitung von sich aus aktiv zu informieren. Der Betroffene muss auch wissen, was passiert, wenn er seine Daten nicht preisgibt. Zu den erforderl. Informationen gehören

- der Zweck der Daten-Verarbeitung,
- die Kontakt-Daten des Verantwortlichen,
- die Kontakt-Daten des DSB (sofern vorhanden),
- ggf. die berechtigten Interessen, auf deren Grundlage die Daten-Verarbeitung erfolgt,
- die Empfänger oder Kategorien von Empfängern

und

- — falls geplant — eine Übermittlung in Drittstaaten (außerhalb der EU / des EWR).

Hinzu kommt

- die Dauer der Daten-Speicherung,
- das Recht auf Auskunft und Widerruf

und

- das Bestehen eines Rechts zur Beschwerde bei der Aufsichtsbehörde.

Falls im Zuge der Daten-Verarbeitung eine automatisierte Entscheidungs-Findung stattfindet, so ist der Betroffene auch über die involvierte Logik und die Tragweite bzw. die Auswirkungen dieser Entscheidung zu informieren. Bei Aufnahme eines Mandats hat die Kanzlei den Mandanten diese Informationen zur Verfügung zu stellen. Darüber hinaus ist ein solcher DS-Hinweis auch im Beschäftigungs-Verhältnis und im Rahmen des Internet-Auftritts erforderlich.

> **▶ Praxis-Tipp** Prüfen Sie, an welchen Stellen in der Kanzlei personenbezogene Daten erhoben werden — Personal-Fragebogen bei Einstellung, Mandanten-Daten bei Verträgen, Gewinnspiele bei Messen, Aufnahme von Interessenten oder Tracking im Rahmen des Internet-Auftritts usw. Tragen Sie die erforderl. Informationen zusammen, um Ihre DS-Erklärungen nach den Vorgaben der DS-GVO zu gestalten!

b) Auskunft

Ein Betroffener kann jederzeit Auskunft darüber verlangen, ob eine Kanzlei Daten zu seiner Person verarbeitet.

Ist dies der Fall, so hat der Betroffene ein Recht, zu erfahren,

- welche Kategorien von Daten zu welchem Zweck verarbeitet werden,
- an wen diese weitergeleitet werden

und

- wie lange sie gespeichert werden.

Er ist darüber in Kenntnis zu setzen, dass er ein Recht auf Berichtigung und Löschung bzw. Einschränkung der Verarbeitung dieser Daten hat. Des Weiteren ist er darauf hinzuweisen, dass er ein Recht zur Beschwerde bei einer Aufsichtsbehörde hat. Falls die Daten nicht beim Betroffenen selbst erhoben wurden, ist ihm Auskunft über deren Herkunft zu geben. Ebenfalls hat er wie bei der Information — vgl. Punkt IV. 2. a) — das Recht, über etwaige automatisierte Entscheidungs-Findungen informiert zu werden. Werden durch den Verantwortlichen Daten des Betroffenen in ein Drittland oder an internationale Organisationen übermittelt, so ist er über die in diesem Zusammenhang bestehenden Garantien bei der Übermittlung zu informieren. Dem Betroffenen ist auf Verlangen auch eine kostenfreie Kopie dieser Daten auszuhändigen. Die Auskunft ist dem Betroffenen unverzüglich zu erteilen, spätestens jedoch innerhalb eines Monats.

▶ Praxis-Tipp Überprüfen Sie, ob Sie in der Lage sind, in den datenverarbeitenden Prozessen in Ihrer Kanzlei die Daten einer Person schnell und umfassend zu ermitteln. Legen Sie fest, wer in der Kanzlei für Auskunfts-Anfragen von Betroffenen zuständig ist, und informieren Sie Ihre MA über diese Vorgaben, so dass diese bei Anfragen professionell reagieren.

c) Berichtigung und Löschung („Recht auf Vergessenwerden“)

Ein Betroffener hat das Recht, die Berichtigung oder Vervollständigung seiner Daten zu verlangen, wenn diese unrichtig oder unvollständig in der Kanzlei gespeichert wurden.

Wenn die Daten eines Betroffenen in der Kanzlei nicht mehr erforderlich sind und es keine weitere RGrundlage für die Speicherung mehr gibt (was z. B. bei st.relevanten Daten i. d. R. für 10 Jahre der Fall ist), so sind diese zu löschen. Dies ist auch beim Widerruf einer Einwilligung der Fall oder wenn Daten unrechtmäßig verarbeitet wurden.

Dieses Recht kann mitunter in der Umsetzung komplex sein, so etwa wenn bereits weitere Stellen auf Veröffentlichungen des Verantwortlichen verwiesen oder verlinkt haben. Auch wenn Daten-Bestände revisionssicher archiviert wurden oder in Backups enthalten sind, ist eine Löschung in der Praxis nahezu ausgeschlossen bzw. die Kosten stünden in keinem Verhältnis zum Nutzen. In diesen Situationen tritt an die Stelle der Löschung in vielen Kanzleien zunächst die Einschränkung der Verarbeitung, im BDSG-ALT als „Sperrung“ bezeichnet. Diese Lösung genügt jedoch nicht den Vorgaben der DS-GVO.

Oftmals vernachlässigt wird das Thema „Bewerbungen“. Abgelehnte Bewerber haben ein „Recht auf Vergessenwerden“, es sei denn, die Kanzlei hat eine Einwilligung für die weitere Speicherung eingeholt. Eine Speicherung von 3 – 4 Monaten erscheint vor dem Hintergrund der 2-monatigen Verjährungs-Frist im Allgemeinen Gleichbehandlungsgesetz (AGG) vertretbar.

▶ Praxis-Tipp Überprüfen Sie regelmäßig die RGrundlagen für die Speicherung personenbezogener Daten in der Kanzlei!

d) Recht auf Daten-Übertragbarkeit

Ursprünglich für soziale Netzwerke gedacht, gilt das Recht auf Daten-Übertragbarkeit nunmehr für alle Daten, die ein Verantwortlicher gespeichert hat.

Der Betroffene hat das Recht, seine Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten. Diese Daten können dann wiederum einem anderen Verantwortlichen zur Verfügung gestellt werden. Der Betroffene hat auch das Recht darauf, dass diese Übertragung unmittelbar zwischen zwei Verantwortlichen erfolgt. Fraglich ist, inwieweit dies mit den bislang marktüblichen Systemen realisierbar ist.

▶ Praxis-Tipp Fragen Sie beim Hersteller Ihrer Software-Lösungen an, ob bereits Möglichkeiten vorhanden sind, um die Personen-Stammdaten und ggf. weitere Daten der Betroffenen in einem maschinenlesbaren Format zu exportieren.

e) Widerspruch

Ein Betroffener hat das Recht, der Speicherung seiner Daten zu widersprechen.

Dies gilt jedoch nur, wenn keine anderen Gründe — wie z. B. gesetzl. Aufbewahrungs-Fristen oder Interessen Dritter — der Löschung widersprechen.

- Gerade im Bereich Marketing (Newsletter, Mandanten-Infobriefe etc.) gibt es hierzu bereits zahlreiche Regelungen, die es zu beachten gilt.
- So macht z. B. auch das „Gesetz gegen den unlauteren Wettbewerb“ (UWG) Auflagen hinsichtlich der werblichen Ansprache. Daraus resultiert u. a. die (unter Punkt IV. 1. a) bereits angesprochene Forderung, bei der Anmeldung zum Newsletter-Bezug das *„Double-Opt-in“*-Verfahren zu nutzen.

> **▶ Praxis-Tipp** Überprüfen Sie die Notwendigkeit der in Ihrem Internet-Auftritt eingebundenen Tracking-Funktionen. Werden diese Auswertungen überhaupt in der Kanzlei genutzt? Sind diese Anwendungen technisch in der Lage, ein *„Do not track“*-Signal des Nutzers umzusetzen?

V. Pflichten des Verantwortlichen

Viele der Pflichten eines Verantwortlichen ergeben sich aus den oben dargestellten individuellen Rechten. Hinzu kommen jedoch noch weitere Aspekte, u. a. die Bestellung eines DSB. Diesem Thema ist (mit Abschnitt VI.) ein eigenes Kapitel gewidmet.

1. *Privacy by design* und *privacy by default*

Mit der DS-GVO haben zwei neue Schlagworte Einzug gehalten:

- *„privacy by design“* (DS durch Technik-Gestaltung)

und

- *„privacy by default“* (DS-freundliche Vor-Einstellungen).

Die eingesetzten Lösungen müssen u. a. grds. dazu geeignet sein, mit ihnen DS-konform zu arbeiten.

Für Kanzlei-Inhaber heißt das, dass sie bei Investitionen in Lösungen und Technik, mit denen personenbezogene Daten verarbeitet werden, vom Hersteller eine Aussage dazu einfordern müssen, wie mit personenbezogenen Daten in diesen Lösungen umgegangen wird — im Grunde ein neues Kriterium als Entscheidungs-Grundlage.

Online-Angebote etwa dürfen keine überflüssigen Daten-Felder enthalten. Vor-Einstellungen müssen so getroffen werden, dass z. B. Profile nicht automatisch veröffentlicht werden oder eine Anwendung nicht automatisch Daten überträgt. Der Betroffene muss aktiv über die Nutzung der Daten bestimmen und nicht erst im Nachhinein reagieren können.

„Privacy by design“ und *„privacy by default“* waren im Grunde auch schon im BDSG-ALT verankert. Die DS-GVO verleiht dieser Forderung jedoch eine neue Qualität.

> **▶ Praxis-Tipp** Überprüfen Sie Ihre Anwendungen und Unterlagen auf die Einhaltung dieser neuen Anforderungen!
>
> Einige BEISPIELE: Werden Logins nach mehreren Fehl-Eingaben gesperrt? Wird die Komplexität der Passwörter technisch erzwungen? Gibt es bei Online-Zugriffen auf sensible Daten eine Mehrfach-Authentifizierung? Beinhalten Ihre Formulare unnötige Daten-Felder?

2. Rechenschafts-Pflicht

Seit dem 25.05.2018 ist der Verantwortliche in der Nachweis-Pflicht; die DS-GVO spricht hier von einer „Rechenschafts-Pflicht".

Es gilt zu dokumentieren, welche Maßnahmen unternommen wurden, um den Anforderungen der DS-GVO gerecht zu werden. Erleidet ein Betroffener einen Schaden, so ist es Sache der Kanzlei, nachzuweisen, dass sie alle (wirtschaftlich vertretbaren) Anstrengungen unternommen hat, um diesen Schaden zu verhindern. Im Zusammenhang mit der durch die DS-GVO vorgegebenen Beweislast-Umkehr führt dies in der Kanzlei zu einem erhöhten Dokumentations-Aufwand.

3. Meldung von Daten-Pannen

Schon bisher waren DS-Pannen unter bestimmten Umständen an die Aufsichtsbehörde zu melden und den Betroffenen mitzuteilen. In der Regel war dies der Fall, wenn besondere Arten personenbezogener Daten, Berufsgeheimnis-Daten oder Bank-/Kreditkarten-Daten natürl. Personen betroffenen waren und ein schwerwiegender Schaden für die Betroffenen drohte. In der Vergangenheit führte dies in manchen Fällen gar zur Veröffentlichung in der Presse.

Die DS-GVO senkt diese Schwelle jedoch ab. Seitdem sind **alle** DS-Pannen an die Aufsichtsbehörde zu melden — es sei denn, diese Panne führt voraussichtlich nicht zu einem Risiko für den Betroffenen. Eine Benachrichtigung der betroffenen Personen muss dagegen nur dann erfolgen, wenn ein hohes Risiko für deren Rechte und Freiheiten besteht.

Während die Meldung bislang „unverzüglich" (sprich: „ohne schuldhaftes Zögern") zu erfolgen hatte — was durchaus 2 Wochen dauern konnte —, verkürzt die DS-GVO die maximale Zeitspanne extrem. **Die Meldung hat seit dem 25.05.2018 innerhalb von 72 Std. nach Bekanntwerden der Panne zu erfolgen!**

> **► Praxis-Tipp** Stellen Sie sicher, dass die Melde-Wege in Ihrer Kanzlei funktionieren! Die Kanzlei-Leitung und der DSB müssen über DS- und Datensicherheits-Pannen umgehend informiert werden!

4. Verstöße — Bußgeld

Während das BDSG-ALT bislang maximale Bußgeld-Beträge von 50.000 € / 300.000 € vorsah, sind Verstöße gegen die Vorgaben der DS-GVO mit Bußgeldern bis zu 10 Mio. € / 20 Mio. € oder 2 % bzw. 4 % des weltweiten Jahres-Umsatzes bewehrt. Auch die Bußgeld-Tatbestände wurden erweitert. Diese sind zu umfangreich, um sie an dieser Stelle alle aufzuführen (siehe Artikel 83 und 84 DS-GVO).

Nahezu alle in diesem Skript angesprochenen Vorgaben sind bußgeldbewehrt, d. h. ein Verstoß gegen die Vorgaben kann mit einem Bußgeld geahndet werden.

Eines sollte zudem herausgestellt werden: Nach der DS-GVO stellt der Verstoß gegen die Pflicht zur Ergreifung geeigneter und angemessener technischer und organisatorischer Maßnahmen zum Schutz personenbezogener Daten eine Ordnungswidrigkeit dar, was im BDSG-ALT nicht explizit der Fall war.

Diese Bußgeld-Tatbestände stellen zwar ein Risiko für die Kanzlei dar, spielen aber keine Rolle für die Bewertung der Prozess-Risiken in der Kanzlei. Hierfür ist allein die Frage ausschlaggebend, welches Risiko bzw. welcher Schaden für den Betroffenen entstehen könnte.

VI. Der Datenschutz-Beauftragte („DSB“)

1. Überblick

Nach der DS-GVO sind Kanzleien dann zur Bestellung eines DSB verpflichtet, wenn

- eine Kern-Tätigkeit mit umfangreicher oder systematischer Überwachung von Personen

oder

- eine Kern-Tätigkeit mit umfangreicher Verarbeitung besonderer Kategorien von Daten vorliegt.

Das BDSG-NEU behält jedoch — aufgrund einer Öffnungs-Klausel in der DS-GVO — die bisherige Regelung bei, so dass diese o.g. Fallgruppen in Dtland kaum eine Rolle spielen werden.

> **▶ Hinweis** Kanzleien, in denen ≥ 10 Personen regelmäßig personenbezogene Daten verarbeiten, haben die Pflicht, einen DSB zu bestellen! Bei der Ermittlung der Anzahl der „i. d. R. mindestens 10 Personen, [die] ständig […] personenbezogen[e] Daten [verarbeiten]“, sind alle ‚Köpfe‘ zu zählen: Kanzlei-Leitung, Beschäftigte, freie MA, Praktikanten, Auszubildende.

Gelingen kann die Einführung und Umsetzung eines DS-Mg’t-Systems jedoch nur, wenn dieser DSB auch über die entsprechenden Kompetenzen verfügt. Diese machen sich immer an den Anforderungen in der Kanzlei und der Komplexität der kanzleiinternen Organisation fest. Der Berufsverband der Datenschutzbeauftragten Deutschlands („BvD“) e.V. hat hierzu das *„berufliche Leitbild der Datenschutzbeauftragten“* entwickelt, auf das im Folgenden kurz eingegangen wird.

2. Fach-Kompetenz

Hierzu gehört eine qualifizierte Ausbildung in zumindest einer der Kategorien

- Organisation und Prozesse,
- Informations- und Kommunikationstechnologie (IuK)

oder

- Recht,

dazu solide Grund-Kompetenzen in den beiden anderen Kategorien.

Neben einer mindestens 2-jährigen Berufs-Erfahrung in den genannten Bereichen muss diese Person eine anerkannte Qualifikation zum DSB nachweisen.

3. Datenschutzrechtliche Grund-Kompetenzen

Im Zuge seiner Ausbildung erhält ein angehender DSB Grund-Kompetenzen im DS-Recht. Darüber hinaus benötigt er Kenntnis der DS-relevanten Vorschriften in der St.-Beratung, was bei einer Person aus der Kanzlei gegeben sein sollte. Auch Kenntnis des allg. Persönlichkeits-Rechts und der Grundrechte-Charta der EU mit DS-Bezug gehören zu seiner Ausbildung, ebenso Grundlagen des europ. und des dt. DS-Rechts, RGrundlagen der Verarbeitung personenbezogener Daten und DS-rechtl. Anforderungen beim Einsatz von IuK.

4. Informations- und Kommunikations-Technologie („IuK“)-Grundkompetenzen

Um den DS-rechtl. Anforderungen beim Einsatz der IuK zu genügen, muss ein DSB technisches Verständnis (Sachverhalte der Informations-Technologien) mitbringen. Die Organisation der IuK sowie die Strukturen von IT-Systemen, IT-Applikationen und IT-Prozessen sollten ihm bekannt sein. Ebenso sollte er über Kenntnisse im Informationssicherheits-Mg’t verfügen. Nur mit diesen Fähigkeiten wird er in der Lage sein, Risiken für betroffene Personen zu erkennen, die aus IT-Systemen, IT-Applikationen und IT-Prozessen resultieren.

5. Weitere Kompetenzen

Ein DSB versteht die Kanzlei-Prozesse und Mg’t-Systeme, kennt Methoden zur Risiko-Analyse sowie zu Audit- und Prüf-Verfahren. Er verfügt über persönl. Integrität, Beratungs-Kompetenz, methodische und didaktische Kompetenz und kann seinen eigenen Status durchsetzen.

6. externer vs. interner DSB

Die Funktion des DSB kann sowohl von kanzleiinternen als auch von externen Personen übernommen werden.

Der Vorteil des internen DSB ist, dass dieser die Kanzlei kennt und in den internen Ablauf eingebunden ist. Nachteilig kann sich jedoch auswirken, dass neben der Unkündbarkeit des bestellten (mittlerweile „benannten“) DSB dessen Tätigkeit nicht zeitlich begrenzt werden kann, da er weisungsfrei ist und sein Zeit-Aufwand zulasten seiner eigentl. Tätigkeit geht. Ganz nebenbei besteht zudem die Gefahr der „Betriebs-Blindheit“. Es gilt darüber hinaus, Interessen-Kollisionen zu vermeiden. So darf die Funktion des DSB nicht durch den EDV-Leiter, den Personal-Leiter oder die Kanzlei-Leitung wahrgenommen werden. Als zusätzl. Kosten-Aufwand gilt es, auch erforderl. Schulungen, Weiterbildungen, ein eigenes Büro, einen eigenen PC etc. einzukalkulieren.

Ein externer DSB hingegen hat eine neutrale Stellung und Unabhängigkeit, wodurch Interessen-Konflikte vermieden werden. Er verfügt bereits über entsprechende Fach-Kenntnisse. Die Nachteile, dass der externe DSB anfangs die Kanzlei nicht kennt und nicht ohne weiteres in den internen Ablauf eingebunden ist, sind durch entsprechende Branchen-Kenntnisse gut zu kompensieren.

Ganz gleich jedoch, ob sich ein interner oder ein externer DSB oder (in kleinen Kanzleien) die Kanzlei-Leitung selbst um das Thema kümmert — wer es noch nicht getan hat, für den ist es allerhöchste Zeit, sich mit den neuen Anforderungen zu befassen.

7. Die Rolle des DSB

Der DSB ist bei der Erfüllung seiner Aufgaben weisungsfrei; er darf deswegen weder abberufen noch benachteiligt werden. Er berichtet unmittelbar der Kanzlei-Leitung. Den Betroffenen ggü. ist er allerdings zur Geheimhaltung verpflichtet.

Der DSB hat folgende Aufgaben:

- Unterrichtung und Beratung des Verantwortlichen und der Beschäftigten,
- Überwachung der Einhaltung der DS-Vorschriften und Überwachung der Sensibilisierung und Schulung der MA und der diesbezügl. Überprüfungen,
- Beratung im Zusammenhang mit der DS-Folgenabschätzung und Überwachung ihrer Durchführung,
- Zusammenarbeit mit der Aufsichtsbehörde;
- zur Verfügung stehen als Anlaufstelle für die Aufsichtsbehörde.

Hinzu kommt noch die Beratung der betroffenen Personen zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte gemäß DS-GVO im Zusammenhang stehenden Fragen.

So ausgeprägt die Überwachungs-Funktion des DSB jedoch auch sein mag, die Umsetzung der Anforderungen der DS-GVO und des BDSG-NEU liegt in der Verantwortung der Kanzlei-Leitung.

Im Vergleich zum alten Recht verschieben sich hier die Zuständigkeiten in Richtung Kanzlei-Leitung — DS ist Chef-Sache! Dem DSB kommt zunehmend eine Überwachungs- und eine Beratungsfunktion zu.

► Praxis-Tipp Überprüfen Sie, ob Ihr DSB über die erforderl. zugewiesenen Kompetenzen verfügt! Sollte noch kein DSB bestellt sein, überprüfen Sie die Notwendigkeit einer Bestellung! Bewerten Sie Vor- und Nachteile einer externen vs. einer internen Lösung!

Bei der Ermittlung der Anzahl der „i. d. R. mindestens 10 Personen, [die] ständig […] personenbezogen[e] Daten [verarbeiten]“, sind alle ‚Köpfe‘ zu zählen: Geschäfts-Leitung, Beschäftigte, freie MA, Praktikanten, Auszubildende.

8. Meldung an die Aufsichtsbehörde

Seit dem 25.05.2018 ist jede Kanzlei verpflichtet, die Kontakt-Daten ihres DSB an die zuständige DS-Aufsichtsbehörde zu melden.

Erste Aufsichtsbehörden haben bereits kundgetan, dass sie hierzu Online-Meldeverfahren einrichten wollen. Aufgrund der föderalen Struktur der DS-Aufsicht in Dtland ist die hierfür zuständige Behörde im nicht-öffentl. Bereich der jeweilige Landesbeauftragte für den DS bzw. in Bayern das Bayerische Landesamt für Datenschutzaufsicht.

VII. Auftrags-Verarbeitung

Von „Auftrags-Datenverarbeitung“ spricht man, wenn sich die Kanzlei einer Stelle bedient, die für sie im Auftrag und weisungsabhängig personenbezogene Daten erhebt, verarbeitet oder nutzt (z. B. Rechenzentrum, IT-Dienstleister oder Aktenvernichtungs-Unternehmen[-„U’en“]). Die Verantwortung und Haftung für den Umgang mit den personenbezogenen Daten bleibt weiterhin beim Auftraggeber, sprich: bei der Kanzlei.

Das BDSG-ALT sah vor, dass im Falle einer Auftrags-Datenverarbeitung nach § 11 BDSG der Auftragnehmer sorgfältig auszuwählen und der Auftrag schriftlich zu erteilen sei. Hierbei war im Einzelnen schriftlich festzulegen:

- der Gegenstand und die Dauer des Auftrags,
- der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,
- die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen,
- die Berichtigung, Löschung und Sperrung von Daten,
- die Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,
- die etwaige Berechtigung zur Begründung von Unter-Auftragsverhältnissen,
- die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,

- mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,
- der Umfang der Weisungsbefugnisse, die sich der Auftraggeber ggü. dem Auftragnehmer vorbehält,
- die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

Zur sorgfältigen Auswahl gehörte u. a. die Überprüfung der technisch-organisatorischen Maßnahmen beim Auftragnehmer. Dies konnte durch ein Vor-Ort-Audit, durch Vorlage von Audit-Berichten / Zertifizierungen oder durch Selbst-Auskunft erfolgen.

Mit der DS-GVO hat sich zunächst die Begrifflichkeit geändert: Man spricht seit dem 25.05.2018 von „Auftrags-Verarbeitung“ und „Auftrags-Verarbeitern“.

Neu ist, dass der Auftrags-Verarbeiter bei Vertragsschluss die beauftragten Sub-Unternehmer explizit benennen muss. Gerade im Online-Bereich und bei Service- und Wartungs-Arbeiten geben viele Dienstleister Aufträge an Sub-Dienstleister weiter. Hier ist bis zum letzten Glied der Kette eine vertragl. Regelung erforderlich. Der Wechsel eines Sub-Unternehmers ist durch den Auftraggeber schriftlich zu genehmigen. In der Praxis werden sich vermutlich Lösungen etablieren, in denen der Auftrags-Verarbeiter einen Wechsel schriftlich anzeigt und dem Auftraggeber ein Sonder-Kündigungsrecht einräumt.

Aufgrund der jüngsten Änderung des § 203 StGB ist es nunmehr möglich, auch Auftrags-Verarbeiter und deren Sub-U’en als Mitwirkende auf die berufl. Verschwiegenheit zu verpflichten. Sofern im Zusammenhang mit der Beauftragung also personenbezogene Daten verarbeitet werden, die der berufl. Verschwiegenheit unterliegen, ist eine Ergänzung bzgl. der Verpflichtung des Auftrags-Verarbeiters und dessen Sub-Unternehmers um § 203 StGB erforderlich.

Für den Abschluss des Vertrages sowie eventueller Änderungen/Ergänzungen kommt neben der Schriftform auch die elektron. Form in Frage. Die elektron. Form muss aber dokumentiert werden.

Das BDSG-ALT sah auch die Fernwartung von EDV-Systemen als Auftrags-Verarbeitung. Hierzu lässt sich die DS-GVO nicht explizit aus. Es ist aber davon auszugehen, dass dieser Umstand im Falle der Fernwartung von EDV-Systemen, in denen personenbezogene Daten verarbeitet werden, auch weiterhin als Auftrags-Verarbeitung angesehen wird.

Haftete bislang alleine der Auftraggeber für Verstöße des Auftrags-Verarbeiters, so weitet die DS-GVO die Haftung in bestimmten Situationen auch auf den Auftrags-Verarbeiter aus.

> **▶ Praxis-Tipp** Überprüfen Sie, ob mit allen Dienstleistern, die personenbezogene Daten verarbeiten, entsprechende Verträge geschlossen wurden! Passen Sie Ihre Verträge auf die neue Rechtslage an!

VIII. Technisch-organisatorische Maßnahmen

Im BDSG-ALT waren die technisch-organisatorischen Maßnahmen in sog. „8 Gebote“ gegliedert:

- Zutritts-Kontrolle,
- Zugangs-Kontrolle,
- Zugriffs-Kontrolle,
- Weitergabe-Kontrolle,
- Eingabe-Kontrolle,
- Auftrags-Kontrolle,
- Verfügbarkeits-Kontrolle

und

- Trennungs-Kontrolle.

Ergänzend waren Vorgaben zur Verschlüsselung zu beachten.

Die DS-GVO spricht in diesem Zusammenhang von „Sicherheit der Verarbeitung“ und benennt u. a. die klassischen Schutzziele der IT-Sicherheit. Neu ist der Begriff der „Belastbarkeit“ der Dienste und Systeme. Im Vordergrund steht die Risiko-Bewertung. Die DS-GVO fordert, dass die Maßnahmen, die zum Schutz von personenbezogenen Daten getroffen werden, unter Berücksichtigung des Risikos ausgewählt werden. Hierbei ist zu beachten, dass die Betroffenen bei der Risiko-Bewertung in den Mittelpunkt zu stellen sind.

Auch für die technisch-organisatorischen Maßnahmen besteht eine „Rechenschafts-Pflicht“. Der Verantwortliche muss nachweisen können, dass die Sicherheit der Verarbeitung gewährleistet ist. Damit werden interne Richtlinien und externe Zertifizierungen noch weiter an Bedeutung gewinnen. In diesem Zusammenhang gilt es, noch weitere Informationen der Aufsichtsbehörden abzuwarten, da gemäß DS-GVO zukünftig nur noch akkreditierte Zertifizierungsstellen externe Zertifizierungen vornehmen dürfen.

> **▶ Praxis-Tipp** Etablieren Sie ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technisch-organisatorischen Maßnahmen! Legen Sie konkrete Vorgaben für die Risiko-Bewertung Ihrer Prozesse fest!

IX. Verzeichnis der Verarbeitungs-Tätigkeiten

1. Überblick

Das BDSG-ALT forderte vom U'en ein Verzeichnis aller Prozesse, in denen personenbezogene Daten verarbeitet werden.

Die DS-GVO fordert dies grds. nur von U'en, die > 250 MA beschäftigen, es sei denn,

- eine von ihnen vorgenommene Verarbeitung birgt ein Risiko für die Rechte und Freiheiten der betroffenen Personen,
- die Verarbeitung erfolgt nicht nur gelegentlich

oder

- es erfolgt eine Verarbeitung besonderer Daten-Kategorien bzw. die Verarbeitung von personenbezogenen Daten über strafrechtl. Verurteilungen und Straftaten.

Das Verzeichnis ist nach DS-GVO also zu erstellen, wenn besondere Arten personenbezogener Daten verarbeitet werden. Dies ist im Grunde in einer Personal-Abteilung immer der Fall, so dass in der Praxis nahezu keine Kanzlei umhinkommen wird, dieses Verzeichnis zu erstellen.

Um das „Recht auf Vergessenwerden" umzusetzen, muss die Kanzlei wissen, welche Daten in welchen Prozessen vorhanden sind. Auch dies wird ohne das Verzeichnis nur schwerlich gelingen.

Hinzu kommt die Forderung, die Risiken der Prozesse zu bewerten. Auch dies setzt die Kenntnis aller Prozesse voraus.

Steuerberater-ONLINE-GmbH

2. MUSTER: Verzeichnis der Verarbeitungs-Tätigkeiten

Name, Firma	Kanzlei Mustermann & Partner
Vorstände, Geschäftsführer, Inhaber	Herbert Mustermann, Sabine Müller
Anschrift, Telefon, E-Mail	Hauptstraße 15, 98765 Musterhausen Tel.: 01234/56789-0 E-Mail: info@mustermann.de
Datenschutzbeauftragter	Karl Schutzheimer
Anschrift, Telefon, E-Mail	Hauptstraße 15, 98765 Musterhausen Tel.: 01234/56789-12 E-Mail: dsb@mustermann.de

***Hinweis**: Die nachfolgenden Angaben sind lediglich als Beispiele zu sehen und sind nicht allgemeingültig auf die Verfahren Ihrer Kanzlei zu übertragen!*

Auflistung: Verfahren / Anwendungen / Programme	01 Finanzbuchhaltung	02 Mandanteninfoabend
Zwecke der Datenverarbeitung	Erfassung aller ein und ausgehenden Zahlungen des Unternehmens. (siehe § 238 Abs. 1 HGB)	Führen einer Gästeliste/Einladungsliste zur Vorbereitung und Durchführung eines Mandanten-Infoabends.
Kategorien betroffener Personen	Mandanten, Lieferanten, Dienstleister.	Mandanten, Interessenten und Daten weiterer Gäste.
Kategorien personenbezogener Daten	Mandantenstammdaten und Rechnungsdaten von Debitoren und Kreditoren.	Kontaktdaten im Zuge der Anmeldung und zur Erstellung des Namensschildes.
Besondere Arten personenbezogener Daten (Ja/Nein)	Ja	Nein
Kategorien von internen und externen Empfängern (einschließlich Drittland oder internationale Organisation)	Beschäftigte, Mandanten, Finanzbehörden und ggf. weitere Behörden.	Beschäftigte
Übermittlung in ein Drittland, Name des Drittlandes. Übermittlung an eine internationale Organisation, Name der internationalen Organisation.	nicht vorgesehen	nicht vorgesehen
Dokumentierung geeigneter Garantien im Drittland, bzw. bei der internationalen Organisation.	nicht relevant	nicht relevant
Fristen für die Löschung der Daten	10 Jahre	Nach Durchführung der Veranstaltung.
allgemeine Beschreibung der technischen und organisatorischen Maßnahmen	Siehe gesonderte Beschreibung der technisch-organisatorischen Maßnahmen.	Siehe gesonderte Beschreibung der technisch-organisatorischen Maßnahmen.

© DWS Steuerberater-Online-GmbH

Im Verzeichnis der Verarbeitungs-Tätigkeiten sind zahlreiche Angaben aufzunehmen, die auch bislang gefordert waren. Neu hinzu kommt die Angabe des DSB; es entfällt die Angabe des Leiters der Daten-Verarbeitung.

Neu ist, dass Auftrags-Verarbeiter ebenfalls ein Verzeichnis zu führen haben. In diesem sind Name und Kontakt-Daten des Auftrags-Verarbeiters und jedes Verantwortlichen, in dessen Auftrag er tätig ist, aufzuführen. Der DSB des Auftraggebers ist ebenso zu nennen wie die Kategorien von Verarbeitungen, die im Auftrag jedes Auftraggebers durchgeführt werden. Hinzu kommen ggf. Angaben zu Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation.

▶ Praxis-Tipp Überprüfen Sie, ob Sie alle Prozesse erfasst haben, in denen personenbezogene Daten verarbeitet werden!

X. Sonderfall Video-Überwachung

Das BDSG-ALT machte — im Gegensatz zur DS-GVO — konkrete Vorgaben zur Video-Überwachung. Das BDSG-NEU hat in Teilen die Regelungen des BDSG-ALT übernommen, aber die Zulässigkeit der Video-Überwachung gerade für den Bereich öffentl. Plätze und des öffentl. Personen-Nahverkehrs ausgeweitet.

Auf die Tatsache der Video-Überwachung ist mit Hinweis-Schildern — Logo „Video-Überwachung“ und Angaben zum Verantwortlichen: Name und Adresse — aufmerksam zu machen. Der Prozess der Video-Überwachung ist zu dokumentieren (Kamera-Typen, Blickwinkel, Reichweite, Speicher-Dauer). In der Regel geht man bei der Speicher-Dauer von 1 – 2 Arbeitstagen aus, eine Frist von bis zu 10 Wochentagen kann aber noch als angemessen betrachtet werden.

Für die Kanzlei ändert sich somit im Grunde nicht viel. Ist die Überprüfung der Video-Überwachung bislang durch den DSB vorab durchzuführen, so sollte auch weiterhin der DSB zu Rate gezogen werden. In vielen Fällen dürfte dies aufgrund der Notwendigkeit einer DS-Folgenabschätzung ohnehin erforderlich sein. Es ist davon auszugehen, dass hier noch weitere Konkretisierungen durch den EU-Datenschutz-Ausschuss erfolgen werden.

▶ Praxis-Tipp Überprüfen Sie den Prozess der Video-Überwachung!

Sind alle Beobachtungs-Bereiche ausgeschildert? Sind die Schilder zu erkennen, bevor der Beobachtungs-Bereich betreten wird? Ist auf den Schildern der Verantwortliche für die Video-Überwachung benannt?

© DWS Steuerberater-Online-GmbH

XI. Datenschutz-Managementsystem

Das DS-Mg't-System hat durch neue Anforderungen eine andere Qualität erhalten. Wir haben mehrere Themen — wie Rechenschafts-Pflicht, Meldung von Daten-Pannen, Risiko-Bewertung oder DS-Folgenabschätzung — bereits angesprochen. Dokumentation und Versionierung spielen eine wesentlich stärkere Rolle als zuvor.

Im Folgenden werden stichpunktartig einige Punkte und Unterlagen angeführt, die in einer Kanzlei auf jeden Fall vorhanden sein sollten:

- Bestellung eines DSB (Bestellungs-Urkunde, falls erforderlich)
- DS-Leitlinie und DS-Handbuch/DS-Konzept
  - Verantwortlichkeiten in der Kanzlei
  - Stellenbeschreibung DSB
  - Kategorisierung personenbezogener Daten
  - Risiko-Bewertung und DS-Folgenabschätzung
  - Verhalten am Telefon
  - *Clean-Desk Policy*

  etc.
- Richtlinie zur Nutzung der EDV, ggf. IT-Sicherheitskonzept
- Checklisten zur Auswahl von technischen und organisatorischen Maßnahmen
- Regelung der Privat-Nutzung von dienstl. oder büroeigenem Internet, E-Mail-System und Telefon durch die MA
- Liste der Dienstleister und Verträge zur Auftrags-Verarbeitung
- Verzeichnis der Verarbeitungs-Tätigkeiten
- Protokollierungs-, Archivierungs- und Lösch-Konzept
- Datensicherungs-Konzept
- Notfall-Plan
- Nachweis der Schulung der MA
- Dokumentation interner und externer Audits, ggf. Zertifizierungen
- DS-Hinweise für sämtl. Daten-Erhebungen (auch Internet-Auftritt!)

XII. Fazit

Der Umfang dieses Skripts erlaubt es nicht, auf spezielle Fragestellungen einzugehen — wie …

- Auftragsverarbeitung außerhalb der EU,
- *Binding Corporate Rules*,
- *Codes of Conduct*

u. v. m.

Auch mussten viele Aspekte im Detail offenbleiben. Dies war jedoch auch nicht die Zielstellung. Fazit ist, dass die Anforderungen an das DS-Mg't-System einer Kanzlei bereits in den vergangenen Jahren aufgrund zunehmender technischer Komplexität und zahlreicher neuer Anforderungen gestiegen sind.

Seit dem 25.05.2018 haben sich die rechtlich-organisatorischen Anforderungen verschärft, und die Bußgeld-Beträge sind drastisch erhöht worden. DS wird aber auch mehr und mehr zum Image- und Compliance-Thema. Eine Zertifizierung nach ISO 9001/2015 ohne Umsetzung der DS-rechtl. Anforderungen ist künftig kaum noch möglich.

Gehen Sie das Thema Datenschutz jetzt aktiv an!

XIII. Checkliste

Prüfen Sie Ihr Datenschutz-Management auf der Grundlage der folgenden Checkliste:

Lfd. Nr.	
1.	**Datenschutz ist Chefsache! — Gibt es eine Leitlinie zum Datenschutz?** • Gibt es ein Datenschutz-Handbuch? • Gibt es darüber hinaus Regelungen zum Umgang mit der IT und zur Privat-Nutzung von dienstl. oder büroeigenem Internet, E-Mail-System und Telefon durch die Mitarbeiter? • Finden regelmäßige Schulungen/Sensibilisierungen der Mitarbeiter statt?
2.	**Datenschutz-Beauftragte(r)** • Ist die Benennung eines Datenschutz-Beauftragten erforderlich? (Es sind alle Köpfe zu zählen!) • Falls ja, gibt es eine schriftliche Benennung, in der auch das Aufgaben-Gebiet klar umrissen ist? • Ist der zeitliche Umfang der Tätigkeit festgelegt?
3.	**Verzeichnis der Verarbeitungs-Tätigkeiten** • Gibt es ein Verzeichnis der Verarbeitungs-Tätigkeiten? • Wurden die Risiken der Verarbeitung bewertet? • Gibt es für jede Verarbeitung eine Rechtsgrundlage? • Sind klare Aufbewahrungs- und Lösch-Fristen festgelegt? • Sind alle Stellen bekannt, an denen personenbezogene Daten erhoben und gespeichert werden? • Ist sichergestellt, dass datenschutzrechtliche Belange bei Beginn oder Änderung eines jeden Prozesses Berücksichtigung finden?
4.	**Einwilligungen** • Sind alle Einwilligungen DS-GVO-konform? • Wird insbesondere das Kopplungs-Verbot beachtet? • Wird auf die Rechte in Zusammenhang mit der Einwilligung verwiesen?
5.	**Auftrags-Verarbeitung** • Sind alle „Verträge zur Auftrags-Verarbeitung“ vorhanden? • Gibt es eine Übersicht über alle Dienstleister und freie Mitarbeiter? • Wurden die Verträge zur Auftrags-Verarbeitung an die DS-GVO angepasst?
6.	**Information** • Gibt es einen Datenschutz-Hinweis für den Internet-Auftitt? • Gibt es Datenschutz-Hinweise für Kunden? • Gibt es Datenschutz-Hinweise für Mitarbeiter?

7.	**Weitere Betroffenen-Rechte** • Gibt es ein Verfahren zur Beantwortung von Auskunfts-Ersuchen? • Wird das Recht auf Berichtigung und Löschung sichergestellt? • Kann das Recht auf Daten-Übertragbarkeit sichergestellt werden? • Wird das Recht auf Widerspruch sichergestellt?
8.	**Datenschutz-Verletzungen — Werden Datenschutz-Pannen durch die Mitarbeiter erkannt?** • Ist sichergestellt, dass Datenschutz-Pannen innerhalb von 72 Stunden an die Aufsichtsbehörde gemeldet werden können? • Gibt es ein Verfahren zur Benachrichtigung der betroffenen Personen?
9.	**Internet-Auftritt** • Wurde der Internet-Auftritt auf Datenschutz-Konformität überprüft?
10.	**Video-Überwachung** *(falls vorhanden)* • Wurde die Video-Überwachung auf Datenschutz-Konformität überprüft?