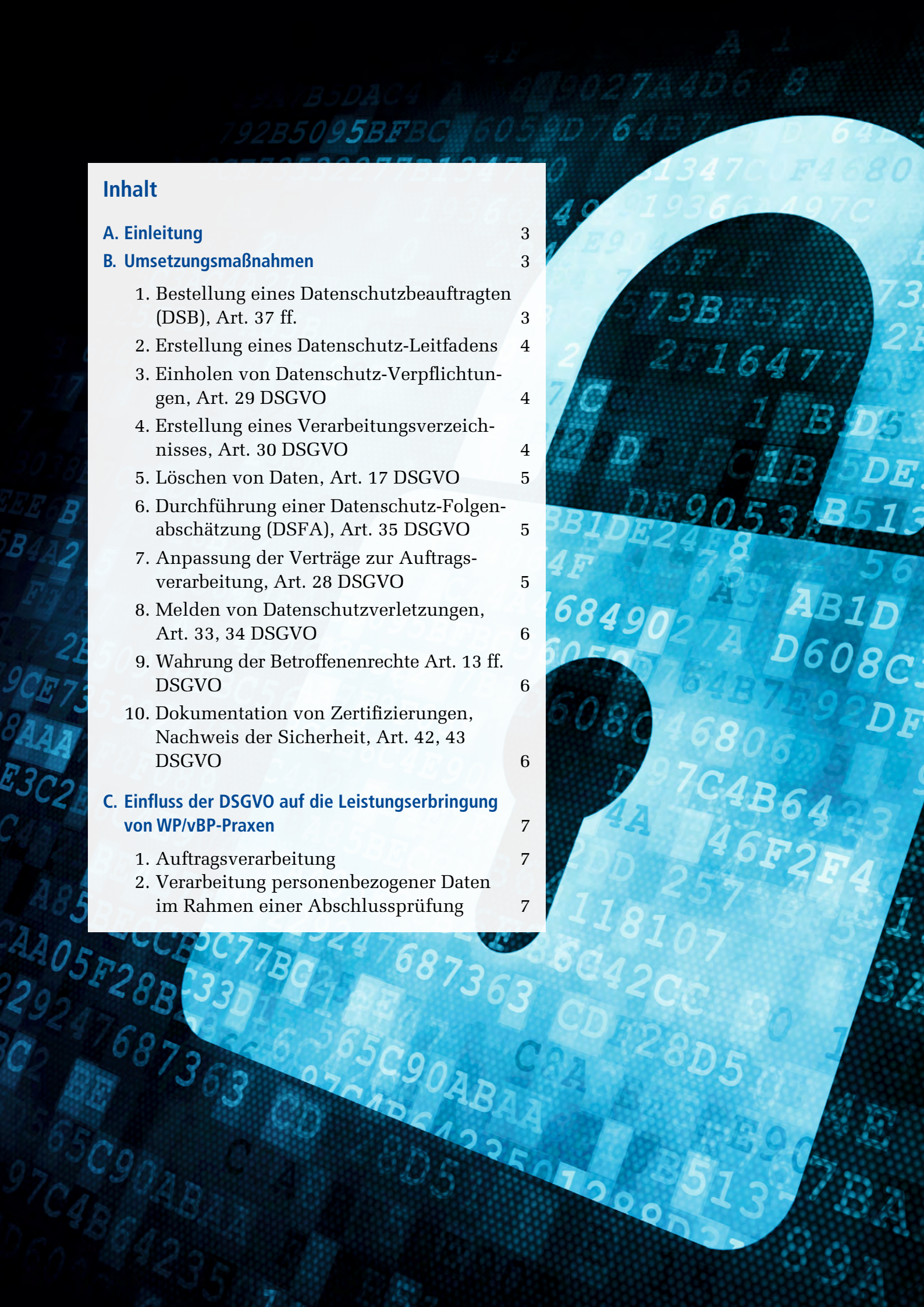
WIRTSCHAFTSPRÜFERKAMMER

Körperschaft des öffentlichen Rechts

Leitfaden der WPK zur DSGVO

Anforderungen an WP/vBP-Praxen



Inhalt

A. Einleitung

Seit dem 25. Mai 2018 sind die Datenschutz-Grundverordnung (DSGVO) und das neugefasste Bundesdatenschutzgesetz (BDSG-2018) anzuwenden. Aus beiden Gesetzen ergeben sich insbesondere erhöhte Anforderungen an den Nachweis, dass ausreichende Maßnahmen zur Sicherstellung des Datenschutzes ergriffen wurden. Die Nachweispflicht muss von dem Verantwortlichen im Sinne des Art. 4 Nr. 7 DSGVO erbracht werden. Hierbei handelt es sich regelmäßig um die WP/vBP-Praxis selbst, nicht um den Datenschutzbeauftragten der Praxis. Letztgenanntem kommt nur eine Beratungs- und Überwachungsaufgabe zu (Art. 39 Abs. 1 DSGVO).

Die geforderte Nachweisbarkeit bedeutet vor allem, dass die Maßnahmen zur Sicherstellung des Datenschutzes (siehe vor allem Art. 24 Abs. 1 und 2, Art. 32 DSGVO) so gewählt, umgesetzt, dokumentiert und auf Wirksamkeit überprüft werden, dass sie jederzeit umfassend und schnell – etwa im Rahmen einer Datenschutzprüfung – dargelegt werden können.

Die DSGVO enthält zudem weitere Pflichten, welche teilweise mit Fristen versehen sind und die in dieser Form bislang noch nicht bestanden. Als Beispiel ist hier die Pflicht zur Meldung von Datenschutzverletzungen an die Aufsichtsbehörden (Art. 33, 34 DSGVO) zu nennen, die bisher auf Fälle mit drohenden schwerwiegenden Beeinträchtigungen begrenzt war. Eine Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung (Art. 35 DSGVO) war bislang noch gar nicht vorgesehen.

Die folgenden Maßnahmen sollen daher eine Handlungshilfe für WP/vBP-Praxen sein, wie sie die Anforderungen der DSGVO umsetzen können. Sie werden ergänzt um Links auf die Webseiten der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit sowie des Bayerischen Landesamts für Datenschutzaufsicht. Hier befinden sich zu den einzelnen Themen weitergehende Informationen – teilweise auch mit Musterformulierungen –, welche von der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder erstellt worden sind. Es handelt sich bei dem vorliegenden Papier nicht um genehmigte Verhaltensregeln im Sinne von Art. 40 DSGVO.

B. Umsetzungsmaßnahmen

1. Bestellung eines Datenschutzbeauftragten (DSB), Art. 37 ff.

In einer WP/vBP-Praxis ist in der Regel ein DSB zu benennen, wenn mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten, das heißt, mit der Mandantenbetreuung beschäftigt sind. Diese zehn Personen müssen keine Angestellten sein, auch Praktikanten, Freelancer, Zeitarbeitskräfte und so weiter zählen mit. Ob der oder die Praxisinhaber/innen selbst dazuzählen, ist noch nicht abschließend geklärt.

Der DSB kann Mitarbeiter der Praxis oder ein externer Dienstleister sein. Für die Tätigkeit sollte er Fachwissen auf dem Gebiet des Datenschutzrechts sowie der Datenschutzpraxis vorweisen können. Er hat folgende Aufgaben zu erfüllen:

- Unterrichtung und Beratung des Verantwortlichen und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Datenschutzpflichten
- Überwachung der Einhaltung der Datenschutzvorschriften sowie der Strategien des Verantwortlichen für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen
- Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung nach Art. 35 DSGVO und Überwachung ihrer Durchführung

- Zusammenarbeit mit der Aufsichtsbehörde und Anlaufstelle für die Aufsichtsbehörde
- Beratung der betroffenen Personen zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte gemäß der DSGVO im Zusammenhang stehenden Fragen

Die WP/vBP-Praxis hat nach der DSGVO die Kontaktdaten des DSB zu veröffentlichen und der zuständigen Aufsichtsbehörde mitzuteilen. Ein Formular für die Mitteilung wird auf den Internetseiten der Aufsichtsbehörden zur Verfügung gestellt.

Weitergehende Informationen der BfDI (PDF) unter
www.wpk.de/link/mag0318b01

2. Erstellung eines Datenschutz-Leitfadens

WP/vBP-Praxen sollten einen Datenschutz-Leitfaden erstellen, welcher für alle Praxisangehörigen verbindlich ist. Der Leitfaden ist dann eine zentrale Ausprägung der Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO. Mit ihm soll die Umsetzung folgender in Art. 5 Abs. 1 DSGVO aufgeführter Datenschutzgrundsätze dokumentiert werden:

- Rechtmäßigkeit,
- Verarbeitung nach Treu und Glauben,
- Transparenz,
- Zweckbindung,
- Datenminimierung,
- Richtigkeit,
- Speicherplatzbegrenzung sowie
- Integrität und Vertraulichkeit.

3. Einholen von Datenschutz-Verpflichtungen, Art. 29 DSGVO

Da in der Regel alle Mitarbeiter einer WP/vBP-Praxis mit personenbezogenen Daten umgehen, sind diese bei der Aufnahme ihrer Tätigkeit darüber zu informieren und zu verpflichten, dass die Verarbeitung der personenbezogenen Daten nach den Grundsätzen der DSGVO erfolgt. Die Verpflichtung bezieht sich somit auf die Einhaltung der Regelungen des Datenschutz-Leitfadens.

Weitergehende Informationen des BayLDA (PDF) unter
www.wpk.de/link/mag0318b02

4. Erstellung eines Verarbeitungsverzeichnisses, Art. 30 DSGVO

Da in WP/vBP-Praxen regelmäßig personenbezogene Daten verarbeitet werden, haben sie ein Verarbeitungsverzeichnis zu führen (vgl. Art. 30 Abs. 5 DSGVO). Hierin müssen gemäß Art. 30 Abs. 1 Satz 2 DSGVO mindestens die folgenden Daten enthalten sein:

- Kontaktdaten des Verantwortlichen,
- die Zwecke der Verarbeitung,
- die Kategorien der betroffenen Personen und der erhobenen Daten,
- die Kategorien von Empfängern personenbezogener Daten,
- Übermittlungen von personenbezogenen Daten an ein Drittland,
- wenn möglich, die Fristen für die Löschung der verschiedenen Datenkategorien sowie
- wenn möglich, eine Beschreibung der technischen und organisatorischen Maßnahmen zur Sicherung der Verarbeitung

Das Verarbeitungsverzeichnis löst das bisherige Verfahrensverzeichnis ab. Dieses kann aber bei der Erstellung als Orientierung genutzt werden. Darüber hinaus haben DStV und BStBK sowie das Bayrische Landesamt für Datenschutzaufsicht Musterverzeichnisse erstellt.

Musterverzeichnis des DStV unter
www.wpk.de/link/mag0318b03

Musterverzeichnis des BayLDA unter
www.wpk.de/link/mag0318b04

Weitergehende Informationen der BfDI (PDF) unter
www.wpk.de/link/mag0318b05

5. Löschen von Daten, Art. 17 DSGVO

Grundsätzlich besteht eine Pflicht zur Löschung personenbezogener Daten auf Verlangen der betroffenen Person beziehungsweise in den in Art. 17 Abs. 1 DSGVO benannten Fällen. Für WP/vBP-Praxen wird diese Pflicht allerdings grundsätzlich dahingehend eingeschränkt, dass eine Datenlöschung erst nach Ablauf der gesetzlichen Aufbewahrungsfristen zu erfolgen hat.

Zu empfehlen ist die Erstellung eines Aufbewahrungs- und Löschkonzepts, welches die Einhaltung der Aufbewahrungsfristen und die anschließende Löschung personenbezogener Daten regelt. Auf diese Weise wird die Einhaltung der Löschpflichten dokumentiert.

Weitergehende Informationen der BfDI (PDF) unter
www.wpk.de/link/mag0318b06

6. Durchführung einer Datenschutz-Folgenabschätzung (DSFA), Art. 35 DSGVO

Bei einer besonders umfangreichen Verarbeitung „sensibler“ Datenkategorien (zum Beispiel Daten über die Religion, Gesundheit, sexuelle Orientierung etc.) muss zukünftig eine DSFA durchgeführt werden. Wobei der Begriff einer „besonders umfangreichen Verarbeitung“ momentan allerdings noch mit Rechtsunsicherheit verbunden ist. Der große Unterschied zwischen der DSFA und den auch sonst zu ergreifenden Maßnahmen liegt in dem höheren Detaillierungsgrad und der Systematik der Risikobestimmung sowie der Überprüfung der Wirksamkeit der Risikoeindämmung.

Das Bayrische Landesamt für Datenschutzaufsicht geht für Steuerberater davon aus, dass keine DSFA durchzuführen ist, da hier kein hohes Risiko bei der Datenverarbeitung besteht. Es ist daher davon auszugehen, dass die Durchführung einer DSFA auch für WP/vBP-Praxen weniger relevant sein sollte.

Weitergehende Informationen der BfDI (PDF) unter
www.wpk.de/link/mag0318b07

7. Anpassung der Verträge zur Auftragsverarbeitung, Art. 28 DSGVO

Nehmen WP/vBP-Praxen Dienstleistungen von Dritten in Anspruch, um personenbezogene Daten auf Weisung verarbeiten zu lassen (das heißt ohne Entscheidungsbefugnisse des Dienstleisters), ist ein schriftlicher Vertrag zur Auftragsverarbeitung abzuschließen. Bestehende Verträge können fortgelten, wenn sie den Anforderungen der DSGVO entsprechen oder darüber hinausgehen. Ist dies nicht der Fall, muss eine Anpassung erfolgen. Wie von allen Dienstleistern, die mit personenbezogenen Daten in der Praxis in Berührung kommen können, muss auch

von Auftragsverarbeitern eine Verschwiegenheitserklärung eingeholt werden.

Beispiele einer Auftragsverarbeitung, welche für eine WP/vBP-Praxis erbracht werden können, sind:

- Rechenzentren
- IT- und TK-Dienstleistungen
- Aktenvernichtung
- Druckerei- und Kopierdienste
- Datenerfassung

Weitergehende Informationen der BfDI (PDF) unter
www.wpk.de/link/mag0318b08

8. Melden von Datenschutzverletzungen, Art. 33, 34 DSGVO

Die DSGVO sieht in Art. 33 die Pflicht vor, eine Schutzverletzung personenbezogener Daten unverzüglich (das heißt binnen 72 Stunden) an die zuständige Aufsichtsbehörde zu melden. Bislang waren nur Datenpannen meldepflichtig, bei denen sensible personenbezogene Daten betroffen waren und wodurch dem Betroffenen schwerwiegende Beeinträchtigungen drohten. Nunmehr sind alle Datenpannen zu melden, welche voraussichtlich zu einem Risiko des Betroffenen führen. Alle Datenschutzverletzungen und ihre Behandlung müssen zudem entsprechend dokumentiert werden.

Auf Grund der bestehenden Unbestimmtheit dieser Regelung ist zu hoffen, dass die Aufsichtsbehörden die Kriterien einer solchen Risikobewertung noch näher bestimmen.

Nach Art. 34 Abs. 1 DSGVO hat der Verantwortliche die Betroffenen unverzüglich von einer Verletzung des Schutzes ihrer personenbezogenen Daten zu benachrichtigen, wenn diese voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten dieser Personen zur Folge hat.

Diese Benachrichtigung ist nicht erforderlich nach Art. 34 Abs. 3 DSGVO, wenn:

- die Daten mittels geeigneter technisch-organisatorische Maßnahmen (zum Beispiel Verschlüsselung) vor unbefugter Kenntnisnahme geschützt sind (Buchstabe a),
- mit geeigneten nachlaufenden Maßnahmen sichergestellt ist, dass das in Absatz 1 genannte hohe Risiko aller Wahrscheinlichkeit nach nicht mehr besteht (Buchstabe b) oder
- eine individuelle Benachrichtigung unzumutbar ist (Buchstabe c). Allerdings schreibt die DSGVO in diesem Fall eine öffentliche Bekanntmachung oder eine vergleichbare Maßnahme vor.

Zusätzlich zu diesen Fällen schließt § 29 Abs. 1 Satz 3 BDSG-neu die Benachrichtigungspflicht auch dann aus, soweit durch die Benachrichtigung Informationen offenbart würden, die nach einer Rechtsvorschrift (zum Beispiel berufsrechtliche Verschwiegenheitspflicht) oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen. Die betroffene Person ist jedoch zu benachrichtigen, wenn ihre Interessen, insbesondere unter Berücksichtigung drohender Schäden, gegenüber dem Geheimhaltungsinteresse überwiegen (§ 29 Abs. 1 Satz 4 BDSG-neu).

Damit hat der deutsche Gesetzgeber hinsichtlich der Information betroffener Dritter zwar grundsätzlich einen Vorrang der beruflichen Verschwiegenheit geregelt. Der WP/vBP hat allerdings in allen Fällen eine Güterabwägung im Sinne von § 29 Abs. 1 Satz 4 BDSG-neu vorzunehmen, um beurteilen zu können, ob die Verschwiegenheitspflicht wegen überwiegender Interessen des betroffenen Dritten zurücktritt.

Weitergehende Informationen des BayLDA (PDF) unter
www.wpk.de/link/mag0318b09

9. Wahrung der Betroffenenrechte Art. 13 ff. DSGVO

Die Art. 13 ff. DSGVO normieren eine Reihe von Rechten betroffener Personen im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten. Als Verantwortlicher ist die WP/vBP-Praxis verpflichtet, diese Rechte zu erfüllen. Dabei sind auch die form- und verfahrensbezogenen Vorgaben des Art. 12 DSGVO zu beachten.

In WP/vBP-Praxen sollten Regelungen geschaffen werden, wie mit anlassunabhängigen Informationspflichten der WP/vBP-Praxis sowie mit Anfragen und Ansprüchen Betroffener umgegangen werden soll. Dabei ist insbesondere zu beachten, dass die Verschwiegenheitspflicht des WP/vBP und seiner Mitarbeiter grundsätzlich Vorrang vor der DSGVO hat (vergleiche die Ausnahmeregelungen in Art. 14 Abs. 5 Buchstabe d DSGVO, § 29 Abs. 1 BDSG, hierzu WPK Magazin 1/2018, S. 21). Die Bearbeitung des Auskunftsersuchens sollte dokumentiert werden.

Artikel im WPK Magazin 1/2018, S. 21 ist abrufbar unter
www.wpk.de/link/mag0318b10

Weitergehende Informationen der BfDI (PDF) unter
www.wpk.de/link/mag0318b11
www.wpk.de/link/mag0318b12

Weitergehende Informationen des IDW unter
www.wpk.de/link/mag0318b13

10. Dokumentation von Zertifizierungen, Nachweis der Sicherheit, Art. 42, 43 DSGVO

Zukünftig soll es auch möglich sein, den Nachweis der Verarbeitung personenbezogener Daten im Einklang mit der Datenschutz-Grundverordnung über Zertifizierungen zu führen (Art. 42 und 43 DSGVO). Wurden Zertifizierungen durchgeführt oder werden zertifizierte Produkte/Verfahren eingesetzt, so sollte dies entsprechend dokumentiert werden. Auch hier sollte eine schnelle und umfassende Auskunft jederzeit möglich sein.

C. Einfluss der DSGVO auf die Leistungserbringung von WP/vBP-Praxen

1. Auftragsverarbeitung

Unter Auftragsverarbeitung wird gem. Art. 29 DSGVO die weisungsgebundene Datenverarbeitung verstanden. Der Auftraggeber ist hierbei weiterhin Verantwortlicher nach Art. 4 Nr. 7 DSGVO. Beispiele für eine Auftragsverarbeitung sind:

- Rechenzentren
- IT- und TK-Dienstleistungen
- Aktenvernichtung
- Druckerei- und Kopierdienste
- Datenerfassung

Die Tätigkeiten von WP/vBP sind aufgrund der nach § 43 Abs. 1 WPO geforderten Eigenverantwortlichkeit der Berufsangehörigen in der Regel keine Auftragsverarbeitung. Insofern muss kein schriftlicher Vertrag zur Auftragsverarbeitung zwischen WP/vBP und Mandant abgeschlossen werden. Der Berufsangehörige ist selbst Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO.

Weitergehende Informationen der BfDI (insbesondere Anhang B) (PDF) unter
www.wpk.de/link/mag0318b14

2. Verarbeitung personenbezogener Daten im Rahmen einer Abschlussprüfung

Im Rahmen der Abschlussprüfung werden unter anderem auch personenbezogene Daten des Mandanten oder Dritter erhoben und verarbeitet. Vor dem

Hintergrund der neuen datenschutzrechtlichen Regeln stellt sich die Frage, auf welche Rechtsgrundlage diese Verarbeitung personenbezogener Daten gestützt werden kann.

Die Verarbeitung personenbezogener Daten kann auf Art. 6 Abs. 1 Buchstabe c, Abs. 3 Buchstabe b DSGVO in Verbindung mit §§ 316, 320 HGB Abs. 2 HGB gestützt werden. Das zu prüfende Unternehmen unterliegt, wenn es mittelgroß oder groß ist, der gesetzlichen Prüfungspflicht nach § 316 HGB, sodass es eine „rechtliche Verpflichtung" zu erfüllen hat. Der Abschlussprüfer ist im Rahmen der Erfüllung dieser gesetzlichen Verpflichtung gesetzlich eingebunden und hat nach § 320 Abs. 2 HGB ein Auskunftsrecht und kann Nachweise anfordern. Damit geht naturgemäß einher, dass diese Auskünfte und Nachweise auch verarbeitet werden müssen.

Die Verarbeitung personenbezogener Daten kann des Weiteren auch auf Art. 6 Abs. 1 Buchstabe f DSGVO gestützt werden. Demnach ist die Verarbeitung personenbezogener Daten rechtmäßig, die „zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten", also des Mandanten, „erforderlich" ist, „sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen …". Die gesetzliche Jahresabschlussprüfung nach § 316 Abs. 1 Satz 1 HGB stellt für den Mandanten eine gesetzliche Verpflichtung dar. In der Abwägung mit den Interessen anderer Dritter, wie zum Beispiel Arbeitnehmern bezüglich ihrer personenbezogener Daten, geht die Abwägung zugunsten der gesetzlichen Pflicht zur Abschlussprüfung aus. Für die Dauer der gesetzlichen Aufbewahrungsfristen können entsprechende Daten auch gespeichert werden (§ 51b Abs. 1 WPO als speziellere Norm geht dem BDSG vor).

Bei einer freiwilligen Abschlussprüfung und anderen Leistungen, bei denen personenbezogene Daten verarbeitet werden, liegt hingegen keine gesetzliche Verpflichtung vor. Auch hier kann allerdings auf den oben genanntenTatbestand des Art. 6 Abs. 1 f DSGVO zurückgegriffen werden. Das berechtigte Interesse des Mandanten folgt aus der Pflicht zur Rechenschaftslegung der Geschäftsführung des Mandanten gegenüber den Gesellschaftern. Die Interessen der betroffenen Personen, zum Beispiel der Angestellten des Mandanten, überwiegen in diesem Kontext nicht. Die Verschwiegenheitspflicht des WP/vBP, die straf- und berufsrechtlich verankert ist (StGB, WPO und Berufssatzung WP/vBP) stellt sicher, dass der WP/vBP entsprechende Daten lediglich zweckentsprechend erhebt und verarbeitet und die Interessen der von der Datenverarbeitung betroffenen Personen (zum Beispiel Arbeitnehmer) gewahrt bleiben.

Vgl. hierzu auch die Hinweise des Fachausschusses Recht des IDW zur Datenschutznovelle 2018 (PDF) unter
www.wpk.de/link/mag0318b15

Ansprechpartner Referat Berufsrecht

Wenn Sie Fragen haben, wenden Sie sich bitte an
(Telefon +49 30 726161-Durchwahl)
Herr Ass. jur. Dr. Goltz -145
Herr Ass. jur. Kamm -147
Frau Kosterka LL.M. -258
Herr Ass. jur. Dr. Thormann -144
Leiter: Herr RA Geithner -311

E-Mail berufsrecht@wpk.de

www.wpk.de/mitglieder/praxishinweise/datenschutz/
Stand September 2018