Stand: 10.04.2019

Hilfestellung zur Beauftragung von Dienstleistern

Inhalt

Stand: 10.04.2019

1. Einleitung

Mit der Auslagerung von Dienstleistungen bzw. der Beauftragung externer Dritter (Dienstleister) zur Erbringung von Leistungen in betrieblichen Prozessen und in der Administration der technischen Infrastruktur sowie mit der Einholung fachlicher Unterstützung verfolgt die WP/vBP-Praxis i.d.R. ökonomische, fachliche und ressourcengetriebene Ziele. Die Inanspruchnahme externer Dienstleistungen ist durch das am 07.11.2017 in Kraft getretene „Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen“ (nachfolgend: „Berufsgeheimnisschutzgesetz“) rechtssicher möglich geworden. Allerdings geht mit dieser Möglichkeit wiederum eine Vielzahl an Anforderungen, die an den Dienstleister zu stellen sind, einher. Vergleiche hierzu die Anlage „Anforderungen der WP/vBP-Praxis an die Auslagerung von Funktionen und Prozessen“.

Die vorliegende Hilfestellung nimmt sich ausschließlich der Erfüllung der straf- und berufsrechtlichen Anforderungen an. Insbesondere die Entscheidung hinsichtlich des Grads der Erfüllung weitergehender Anforderungen wie bspw. der Erfüllung funktionaler oder ökonomischer Anforderungen obliegen ausschließlich der WP/vBP-Praxis.

Die folgenden Ausführungen lassen zudem etwaige Vorgaben des Bundesdatenschutzgesetzes (BDSG) und der EU Datenschutz-Grundverordnung (DS-GVO)[1] unberührt.

[1] Zum Datenschutz siehe IDW Fokus: https://www.idw.de/idw/im-fokus/datenschutz.

Stand: 10.04.2019

2. Begriffstypologie der mitwirkenden Personen (Begriff des Dienstleisters in Abgrenzung zum neuen Gehilfenbegriff)

Das neue Berufsgeheimnisschutzrecht verwendet in § 203 StGB, §§ 50, 50a WPO und § 53a StPO keine einheitliche Begriffstypologie der mitwirkenden Personen. Hinzu kommt, dass mit § 50a WPO ein neuer Begriff, nämlich der des Dienstleisters, in die WPO eingeführt wurde. Außerdem ist die Einordnung von mitwirkenden Personen als „Gehilfen" i.S.v. § 50 WPO durch das Berufsgeheimnisschutzgesetz geändert worden. Nunmehr wird zwischen verschiedenen Arten der Mitwirkung differenziert, an die unterschiedliche Rechtsfolgen geknüpft sind. Die richtige Einordnung von mitwirkenden Dritten unter die verschiedenen Begriffe ist daher für die Bestimmung der strafrechtlichen, strafprozessualen und berufsrechtlichen Rechte und Pflichten von wesentlicher Bedeutung. Namentlich bestehen nach Maßgabe von § 50a WPO höhere Anforderungen bei der Beauftragung von Dienstleistern als bei der Einschaltung von Mitwirkenden i.S.v. § 50 WPO.

2.1. Berufsmäßig tätige Gehilfen

Unter den strafrechtlichen Begriff der „berufsmäßig tätigen Gehilfen" i.S. des § 203 Abs. 3 Satz 1 StGB fallen zunächst die in den Geschäftsbetrieb des WP/vBP eingegliederten Personen, die innerhalb des beruflichen Wirkungsbereichs des WP/vBP eine auf dessen Tätigkeit bezogene unterstützende Tätigkeit ausüben, mit der die Kenntnis bzw. die Möglichkeit der Kenntnisnahme fremder Geheimnisse einhergeht.

Maßgeblich für die Einordnung von mitwirkenden Personen als „Gehilfen" im berufsrechtlichen Sinne des § 50 WPO ist der Nähegrad des Mitwirkenden zum Berufsträger, also die Frage der Einbindung in den Geschäftsbetrieb des WP/vBP (Sphärentheorie). Bei der Einbeziehung in die Sphäre des Berufsträgers ist nach Auffassung der WPK insb. auf das Bestehen von Kontroll- und Weisungsrechten in Bezug auf den Umgang mit Mandantendaten abzustellen, so z.B. darauf, ob der Mitwirkende in das Qualitätssicherungssystem der WP/vBP-Praxis eingebunden ist (vgl. WPK-Praxishinweis „Mitwirkung Dritter an der Berufsausübung (§§ 50, 50a WPO)", Stand: 26.07.2018).

Mithin betreffen die Regelungen zur Verschwiegenheitspflicht des § 50 WPO Beschäftigte und andere Personen, die in der Sphäre des WP/vBP tätig sind (namentlich Angestellte von konzern- oder netzwerkangehörigen WP/vBP-Praxen und freie Mitarbeiter; siehe dazu Abschn. 2.1.1. ff.). In Abgrenzung dazu beziehen sich die in § 50a WPO kodifizierten Regelungen zur Verschwiegenheitspflicht im Wesentlichen auf Tätigkeitsbereiche, die der WP/vBP ausgelagert hat, also die Tätigkeiten, die außerhalb der Sphäre des Berufsträgers durch Dienstleister erbracht werden (siehe dazu Abschn. 2.2.). Die nachfolgenden Beispiele sollen bei der Einordnung der jeweils einbezogenen Personengruppen helfen.

2.1.1. Arbeitnehmer

Zu den berufsmäßig tätigen Gehilfen zählen zum einen die beim WP/vBP „Beschäftigten“ (§ 50 Satz 1 WPO) bzw. von diesem „angestellten Personen“ (§ 50 Satz 4 WPO), d.h. die „klassischen“ Arbeitnehmer. Diese Personen stehen in einem arbeitsrechtlichen Vertragsverhältnis und werden vom abgeleiteten Zeugnisverweigerungsrecht des § 53a Abs. 1 Satz 1 Nr. 1 StPO erfasst.

2.1.2. Auszubildende etc., berufsvorbereitende Tätigkeiten

Als weitere Gruppe von Mitwirkenden nennt § 203 Abs. 3 Satz 1 StGB die bei WP/vBP „zur Vorbereitung auf den Beruf tätigen Personen“. § 50 Satz 3 WPO bezeichnet diese Gruppe als Personen mit „berufsvorbereitenden Tätigkeiten“; diese sind vom abgeleiteten Zeugnisverweigerungsrecht des § 53a Abs. 1 Satz 1 Nr. 2 StPO erfasst. Hierzu zählen Auszubildende und Praktikanten, angehende WP/vBP und Steuerberater sowie Rechtsreferendare, die ihre Anwalts- oder Wahlstation bei einem (Syndikus-)Rechtsanwalt in der Rechts- oder Steuerrechtsabteilung einer WPG/BPG absolvieren.

2.1.3. Arbeitnehmerüberlassung

Auch Leiharbeitnehmer zählen zu den berufsmäßig tätigen Gehilfen, soweit diese innerhalb des beruflichen Wirkungsbereichs des WP/vBP eine auf dessen Tätigkeit bezogene unterstützende Tätigkeit ausüben. Auch wenn es diesen an der Arbeitnehmereigenschaft gegenüber dem Entleiher fehlt, besteht dennoch ein gesetzliches Schutzpflichtverhältnis zwischen Entleiher und Leiharbeitnehmer und gelten die arbeitsrechtlichen Schutzvorschriften. Ebenso besteht eine Einbindung in den Geschäftsbetrieb des entleihenden WP/vBP, verbunden mit umfassenden fachlichen Weisungsrechten des WP/vBP. Die in einem solchen Leiharbeitnehmerverhältnis stehenden Personen werden vom abgeleiteten Zeugnisverweigerungsrecht des § 53a Abs. 1 Satz 1 Nr. 3 StPO erfasst.

2.1.4. Mitwirkende, die sonstige Hilfstätigkeiten in der Sphäre des WP/vBP verrichten

In der Sphäre des WP/vBP können darüber hinaus weitere Personen tätig sein, die nicht auf der Grundlage eines Arbeitsvertrags bei der Berufsausübung mitwirken, sondern auf Basis eines mit dem Anstellungsverhältnis vergleichbaren, wie z.B. eines besonderen Nähe- oder eines Gefälligkeitsverhältnisses zum WP/vBP, und infolgedessen ebenfalls zu den berufsmäßig tätigen Gehilfen zu zählen sind.

2.1.4.1. Familienangehörige etc.

Zu dieser Personengruppe gehören insb. gelegentlich mithelfende nahe Familienangehörige und Bekannte oder auch Praktikanten, die nicht zu Ausbildungszwecken beim WP/vBP tätig sind. Diese Personen erbringen für den WP/vBP „sonstige Hilfstätigkeiten“ i.S.v. § 53a Abs. 1 Satz 1 Nr. 3 StPO und § 50 Satz 3 Alt. 1 WPO.

2.1.4.2. Freie Mitarbeiter

Auch freie Mitarbeiter können in der Sphäre des WP/vBP tätig sein. Sofern ein freier Mitarbeiter vergleichbaren Kontroll- und Weisungsrechten hinsichtlich des Umgangs mit vertraulichen Informationen unterliegt und insoweit in das Qualitätssicherungssystem der WPG/BPG eingebunden ist, wird er regelmäßig der Sphäre des WP/vBP zuzurechnen und berufsrechtlich wie eine beschäftigte Person i.S.v. § 50 WPO zu behandeln sein (vgl. WPK-Praxishinweis „Mitwirkung Dritter an der Berufsausübung (§§ 50, 50a WPO)“, Stand: 26.07.2018). Ist dies nicht der Fall, sind diese freien Mitarbeiter wie Dienstleister zu behandeln, für die dann die strengeren Regelungen des § 50a WPO zum Schutz der Verschwiegenheitspflicht gelten (vgl. Abschn. 2.2.1.1.).

2.1.4.3. Konzernarbeitnehmer; Netzwerk-Mitarbeiter; SDC-Mitarbeiter

Einige Besonderheiten sind bei einer mehrstufigen WPG/BPG zu beachten. Bei Arbeitnehmern, die nicht (nur) unmittelbar bei Aufträgen ihrer Arbeitgeber-WPG/BPG, sondern auch in anderen Konzernunternehmen mitwirken, kommt es entscheidend darauf an, ob sie bei der entsprechenden Tätigkeit einem fachlichen Direktionsrecht (Weisungsrecht) des Konzernunternehmens unterliegen. Wenn dies nicht der Fall ist, sind diese Personen wie nicht in die Sphäre des WP/vBP eingegliederte Dritte zu behandeln, es sei denn, sie unterliegen vergleichbaren Kontroll- und Weisungsrechten hinsichtlich des Umgangs mit vertraulichen Informationen und sind in das Qualitätssicherungssystem eingebunden. Entsprechendes gilt für Mitarbeiter einer Netzwerkgesellschaft oder eines sog. „Service Delivery Center“ (SDC) oder sog. „Shared Service Center“ (SSC). In SDC/SCC werden standardisierbare Dienstleistungsprozesse einer WP/vBP-Praxis konsolidiert und zentralisiert. Das heißt, es werden gleichartige Prozesse aus verschiedenen Bereichen einer WP/vBP-Praxis zusammengefasst und von einer zentralen Einheit (Stelle, Abteilung) erbracht. Liegen die vorgenannten Voraussetzungen (vgl. hierzu WPK-Praxishinweis „Mitwirkung Dritter an der Berufsausübung (§§ 50, 50a WPO)“, Stand: 26.07.2018) nicht vor, sind diese Mitarbeiter wie externe Dienstleister zu qualifizieren. Dann gelten die strengeren Regelungen des § 50a WPO zum Schutz der Verschwiegenheitspflicht (vgl. Abschn. 2.2.2.).

2.2. Sonstige mitwirkende und weitere Personen, die nicht in die Sphäre des Berufsgeheimnisträgers eingegliedert sind

Von den berufsmäßig tätigen Gehilfen und den in Vorbereitung auf den Beruf tätigen Personen sind die „sonstigen mitwirkenden Personen“ zu unterscheiden. Dabei handelt es sich um Personen, die zwar an der beruflichen Tätigkeit des Berufsgeheimnisträgers mitwirken, indem sie in irgendeiner Weise in diese Tätigkeit eingebunden sind und Beiträge dazu leisten, jedoch ohne dabei in die Sphäre des Berufsgeheimnisträgers eingegliedert zu sein.

Eine solche Mitwirkung an der beruflichen Tätigkeit kann nur angenommen werden, wenn die mitwirkende Person mit der beruflichen Tätigkeit der schweigepflichtigen Person, ihrer Vorbereitung, Durchführung, Auswertung und Verwaltung befasst ist. Dies kann insb. auf Basis eines Vertragsverhältnisses erfolgen, auch im Rahmen von mehrstufigen Auftragsverhältnissen.

2.2.1. Dienstleister

§ 203 Abs. 3 Satz 2 Halbsatz 1 StGB erfasst die „sonstigen Personen", die an der beruflichen Tätigkeit des WP/vBP mitwirken, ohne in die Sphäre des WP/vBP eingegliedert zu sein, aber (potenziell) Zugriff auf der Verschwiegenheitspflicht unterliegende Mandantendaten haben (vgl. Abschn. 4.2.6.1.). Gemeint sind die „Dienstleister" i.S.v. § 50a Abs. 1 WPO. Da die Mitwirkung auf Basis eines (i.d.R. Dienst- oder Werk-)Vertrags erfolgt, werden Dienstleister vom abgeleiteten Zeugnisverweigerungsrecht des § 53a Abs. 1 Satz 1 Nr. 1 StPO erfasst.

2.2.1.1. Freie Mitarbeiter

Soweit freie Mitarbeiter insb. nicht in das Qualitätssicherungssystem der WP/vBP-Praxis eingebunden und damit nicht in der Sphäre des WP/vBP tätig sind, mithin eine Zuordnung zu § 50 WPO ausscheidet (vgl. Abschn. 2.1.4.2.), sind diese Personen wie Dienstleister zu behandeln, für die § 50a WPO gilt.

2.2.1.2. Zur gemeinschaftlichen Berufsausübung vertraglich verbundener Personen

In der Gesetzesbegründung zum Berufsgeheimnisschutzgesetz werden auch Fälle der gemeinsamen Berufsausübung mit anderen freien Berufen (vgl. § 44b Abs. 1 WPO, § 59a BRAO, § 56 StBerG, § 9 BNotO) unter den Begriff „sonstige Personen" bzw. „Dienstleister" gefasst. Nicht ganz klar ist, ob hierunter alle Formen der beruflichen Zusammenarbeit fallen sollen und damit auch Mitwirkende in Konzernunternehmen, Kooperationen und Netzwerkgesellschaften i.S.v. § 319b HGB erfasst sind. Grundsätzlich ist auch dies im Einzelfall nach Maßgabe der Sphärentheorie zu prüfen (vgl. Abschn. 2.1. und 2.1.4.).

2.2.2. Angestellte eines Dienstleisters; Subunternehmer

In § 203 Abs. 3 Satz 2 Halbsatz 2 StGB werden schließlich „weitere Personen" genannt, die von „sonstigen Personen", d.h. von vom WP/vBP beauftragten Dritten, zur weiteren Mitwirkung beauftragt werden. Dieser Begriff umfasst insb. die beim Dienstleister Beschäftigten und Subunternehmer des Dienstleisters. Diese „weiteren Personen" i.S.v. § 50a Abs. 3 Satz 2 Nr. 3 WPO (Subunternehmer) werden ebenfalls regelmäßig auf Basis eines Vertragsverhältnisses tätig und sind damit vom abgeleiteten Zeugnisverweigerungsrecht des § 53a Abs. 1 Satz 1 Nr. 1 StPO erfasst.

3. Betroffene Dienstleistungen

WP/vBP können zur Unterstützung ihrer Tätigkeiten, wie dargestellt, Dienstleister in Anspruch nehmen. Dies betrifft zum einen die Auslagerung rein technischer Dienstleistungen, wie z.B. die

Nutzung fremder IT-Hardware (Rechen- oder Speicherkapazitäten), oder anderer IT-Dienstleistungen. Darüber hinaus stellt auch die Inanspruchnahme personell erbrachter Dienstleistungen eine Option für den WP/vBP dar, und zwar wiederum nicht nur bei administrativen Tätigkeiten (z.B. Call-Center-Leistungen oder Schreibarbeiten), sondern auch bei fachlichen Dienstleistungen innerhalb der Auftragsabwicklung (z.B. Mandantenumfeldanalysen, Datenanalysen).

Nachfolgend sind einige Dienstleistungen aufgeführt, die für einen WP/vBP im Rahmen eines Auftrags durch einen berufsmäßigen Gehilfen oder Dienstleister erbracht werden können. Dabei handelt es sich lediglich um eine beispielhafte und nicht abschließende Auflistung.

Zwischen den administrativen, fachlichen und technischen Dienstleistungen kann es Überschneidungen geben, da bspw. die Aktenführung und Archivierung auch mit der Einführung eines technischen Systems zur Erfassung der Akten und elektronischen Archivierung verknüpft sein kann. Die administrativen und fachlichen Leistungen können auch als technische Dienstleistungen erbracht werden.

Darüber hinaus muss bei der Auslagerung von Dienstleistungen an Dienstleister unterschieden werden, ob diese übergeordneter Natur sind oder unmittelbar einem einzelnen Mandat dienen sollen. Im letzteren Fall darf der WP/vBP die Unterbeauftragung nicht ohne Einwilligung des Mandanten in Anspruch nehmen (§ 50a Abs. 5 WPO). Zur Beurteilung der Frage, ob eine Dienstleistung unmittelbar einem einzelnen Mandat dient, vgl. Abschn. 4.2.6.

3.1. Administrative Dienstleistung

Mögliche administrative Dienstleistungen, die für einen WP/vBP durch einen berufsmäßig tätigen Gehilfen oder einen Dienstleister erbracht werden können, sind beispielsweise:

- Erstellen, Überarbeiten von Präsentationen
- Abschreiben eines Diktats und andere Schreibarbeiten, Telefondienst/Telefonzentrale
- Back-office-Tätigkeiten
- Erbringung von Post- und Druckservices
- Führung, Archivierung und Vernichtung von Akten einschließlich und Arbeitspapieren
- Bereitstellung von Programmen zur Prüfungsdokumentation und Bereitstellung der Systemumgebung zum Betrieb der Programme
- Call-Center-Leistungen
- internes Rechnungswesen, Rechnungsstellung
- Leistungserfassung und Betrieb von Nachweissystemen
- Gebäudemanagement – Gebäudesicherheit

- Catering, Organisation von Konferenzen, Empfang-Service
- Eventagenturen, Marketing

3.2. Fachliche Dienstleistung

Fachliche Dienstleistungen, die der WP/vBP auslagern bzw. inhouse durchführen kann, sind z.B.:

- Datenanalysen, Abstimmung von Massendaten
- Datenaufbereitung, Datentransfer, Datenimport
- Unterstützung bei Saldenbestätigungen
- Unterstützung bei Prüfungshandlungen (ohne prüferische Beurteilung)
- Aufbereitung von Vorjahresdaten
- Koordination von Konzernabschlussprüfungen, Prüfung von Audit Instructions, Reporting Package
- Unterstützung bei der Berichterstellung und Prüfungsdokumentation
- Mitwirkung an der Erfüllung von Buchführungs- und steuerrechtlichen Pflichten des WP/vBP
- Detektivdienste, Sachverständigenarbeit
- Übersetzungen
- Mandantenumfeldanalyse
- Qualitätssicherung und Überprüfung

3.3. Technische Dienstleistungen[2]

Das Outsourcen technischer Dienstleistungen umfasst die Auslagerung von Geschäftsprozessen einer WP/vBP-Praxis ganz oder teilweise auf einen Dienstleister. Unerheblich ist, ob die ausgelagerten Leistungen beim Auftraggeber oder Auftragnehmer zu erbringen sind. Sowohl der Betrieb eines Rechenzentrums als auch die Bereitstellung einer Anwendung oder einer Homepage sind verbreitete Services.

Die technischen Dienstleistungen können sowohl eigenständig als auch im Zusammenhang mit den administrativen und fachlichen Dienstleistungen durch einen Dienstleister erbracht werden, wie folgende Beispiele veranschaulichen:

---

[2] Vgl. hierzu insb. BSI Grundschutz, Abschnitt B1.11 sowie IDW Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung bei Auslagerung von rechnungslegungsrelevanten Prozessen und Funktionen einschließlich Cloud Computing (*IDW RS FAIT 5*) Tz. 6 ff.

- Beispiel eigenständige technische Dienstleistung: Die zum Betrieb einer IT-Anwendung (z.B. Prüfungssoftware) notwendigen Server wurden vom WP/vBP angeschafft, werden aber laut Servicevertrag vom Hersteller regelmäßig gewartet.
- Beispiel Kombination von technischer und fachlicher Dienstleistung: Der WP/vBP stellt dem Dienstleister Daten des zu prüfenden Unternehmens zur Verfügung. Dieser führt mit dem Datenbestand Datenanalysen (fachliche Dienstleistung) mithilfe seiner Datenanalyse-Software auf seinen Servern durch (technische Dienstleistung).

Die Erbringung von technischen Dienstleistungen kann wie folgt kategorisiert werden:

- Application Service Provider (ASP): Eine vom WP/vBP genutzte IT-Anwendung (z.B. E-Mail, Enterprise-Resource-Planning-Anwendungen (ERP), Archivierung) wird vom Dienstleister auf dessen IT-Systemen betrieben. Sie ist Eigentum des Dienstleisters. Der WP/vBP greift auf die IT-Anwendung über das Internet oder via Virtual Private Network (VPN) zu.
- Application Hosting: Eine vom WP/vBP genutzte IT-Anwendung (z.B. E-Mail, ERP-Anwendungen, Archivierung) wird vom Dienstleister auf dessen IT-Systemen betrieben. Sie ist aber, anders als bei einer ASP-Dienstleistung, nicht Eigentum des Dienstleisters, sondern Eigentum des WP/vBP. Der WP/vBP greift auf die IT-Anwendung über das Internet oder via VPN zu.
- Security Outsourcing und Managed Security Services: Erbringung von technischen Dienstleistungen im Zusammenhang mit der Informationssicherheit (z.B. Auslagerung des Firewall-Betriebs, die Überwachung des Netzwerks, Virenschutz oder der Betrieb eines VPN).
- Business Process Outsourcing und SSC: Der WP/vBP lagert die Erbringung von administrativen oder fachlichen Dienstleistungen auf einen Dienstleister (Business Process Outsourcing) oder auf eine Einheit innerhalb seiner Organisation (SSC) aus. Dies umfasst regelmäßig auch die Bereitstellung und den Betrieb der dafür notwendigen IT-Systeme (technische Dienstleistung).
- Offshoring: wie Business Process Outsourcing, jedoch wird die Dienstleistung in einem anderen Land erbracht.
- Cloud-Computing, Erbringung von technischen Dienstleistungen in den folgenden Servicemodellen: Bereitstellung von IT-Infrastruktur wie bspw. Speicher- oder Netzwerkserverkapazitäten (Infrastructure as a Service (IaaS)), einer informationstechnischen Umgebung zwecks Betrieb von eigener Software des Auftraggebers (Platform as a Service (PaaS)) und/oder Nutzung einer IT-Anwendung durch den Auftraggeber aus der Cloud (Software as a Service (SaaS)).

Das Outsourcen technischer Dienstleistungen und Prozesse bedingt eine unmittelbare An- und Einbindung des Auftraggebers an bzw. in die IT-Systeme bzw. die Geschäftsprozesse des

Dienstleisters. Mithin muss die Integration der durch den Dienstleister erbrachten Teilprozesse in die Prozesse des Auftraggebers gewährleistet werden. Dabei werden sowohl informationstechnische als auch personelle Integrationsmaßnahmen notwendig sein. Insbesondere bedürfen wesentliche Änderungen an dem IT-System des Dienstleisters, die die zugesagte Funktionalität des IT-Systems beeinträchtigen können, regelmäßig einer Information an den Auftraggeber. Zwar wird der Auftraggeber in der Regel kein Mitspracherecht bei etwaigen Systemänderungen haben; jedenfalls aber sollte er sich ein Sonderkündigungsrecht einräumen lassen. Mit einem Informations- und einem Sonderkündigungsrecht wird es dem WP/vBP ermöglicht, die Funktionsfähigkeit seiner Prozesse und internen Kontrollmaßnahmen zu gewährleisten.

4. Rechtliche Anforderungen an den WP/vBP bzw. die WP/vBP-Praxis

4.1. Einleitung

Vor Inkrafttreten des neuen Geheimnisschutzrechts bestand aufgrund der bislang fehlenden Kongruenz zwischen strafrechtlichen und berufsrechtlichen Anforderungen an die Verschwiegenheit (Umfang der vertraulich zu behandelnden Informationen, Gehilfenbegriff etc.) Rechtsunklarheit bei der Einbindung Dritter in die Berufsausübung. Insbesondere die Einschaltung externer (IT-)Dienstleister war vor allem im Zusammenhang mit § 203 StGB bis dato ein rechtlicher Graubereich.

Dies soll das am 09.11.2017 in Kraft getretene „Berufsgeheimnisschutzgesetz“ ändern. Die für WP/vBP und vor allem für deren Mitwirkende geltenden Neuregelungen finden sich in § 203 Abs. 3, 4 StGB, §§ 53, 53a, 97 Abs. 3, 4 StPO sowie §§ 50, 50a WPO.

Im Berufsgeheimnisschutzgesetz im Einzelnen neu geregelt ist die Strafbarkeit des WP/vBP im Zusammenhang mit der Einschaltung von Mitwirkenden – das sind nach der Terminologie des StGB insb. „Gehilfen“, „sonstige mitwirkende Personen“ und „weitere Personen“ – sowie deren Strafbarkeit nach Maßgabe von § 203 Abs. 3, 4 StGB. Diesen Mitwirkenden wird ein eigenes strafprozessuales, vom Berufsträger abgeleitetes Zeugnisverweigerungsrecht nach § 53a StPO und ein Beschlagnahmeschutz gemäß § 97 Abs. 3, 4 StPO eingeräumt.

Trotz eines Mehrs an Rechtssicherheit durch die neuen Regelungen kann die Anwendung in der Praxis Schwierigkeiten bereiten. Denn der Rechtsanwender hat es nach wie vor mit unabhängig nebeneinanderstehenden Normen des Strafrechts einerseits und des Berufsrechts andererseits zu tun, die keine harmonisierte Terminologie gefunden haben (vgl. Abschn. 2.).

Im Zusammenspiel der Regelungen ist zu beachten, dass berufsrechtskonformes Verhalten niemals strafbar sein kann (vgl. Abschn. 6.1.4.), hingegen aber berufsrechtswidriges Verhalten nicht zwingend eine Strafbarkeit begründet.

Stand: 10.04.2019

4.2. Rechtliche Anforderungen im Einzelnen

4.2.1. Das Prinzip der „Erforderlichkeit“ (§ 203 Abs. 3 StGB und § 50a Abs. 2 WPO)

Nach der ausdrücklichen Klarstellung in § 203 Abs. 3 StGB dürfen WP/vBP nunmehr fremde Geheimnisse auch gegenüber

- „*sonstigen mitwirkenden Personen*“ (externe Dritte, d.h. Dienstleister i.S.v. § 50a Abs. 1 WPO) – § 203 Abs. 3 Satz 2 Halbsatz 1 StGB – und
- „*sonstigen mitwirkenden Personen, wenn diese sich weiterer Personen bedienen, die an der beruflichen oder dienstlichen Tätigkeit des WP/vBP mitwirken*“ (z.B. Angestellte des Dienstleisters, Subunternehmer, Unterauftragnehmer als „weitere Personen“ i.S.v. § 50a Abs. 3 Satz 2 Nr. 3 WPO) – § 203 Abs. 3 Satz 2 Halbsatz 2 StGB –

offenbaren.

Dieses tatbestandliche „Offenbaren“ gilt allerdings nur dann als nicht unbefugt und damit als nicht strafbar, wenn es „erforderlich“ i.S. des § 203 Abs. 3 StGB ist. Das Tatbestandselement der Erforderlichkeit des Offenbarens von Geheimnissen bei der Inanspruchnahme der Tätigkeit ist damit von entscheidender Bedeutung für die Frage der rechtlichen Zulässigkeit der Einbindung Dritter.

Die Erforderlichkeit ist ebenso berufsrechtliche Voraussetzung bei der Inanspruchnahme von von externen Dritten erbrachten Dienstleistungen gemäß § 50a Abs. 1 Satz 1 WPO. Der unbestimmte Rechtsbegriff der „Erforderlichkeit“, den der Gesetzgeber weder im Gesetz selbst noch in der Gesetzesbegründung weiter konkretisiert hat, muss daher ausgelegt werden.

Die Frage, ob die Einbindung sonstiger mitwirkender Personen bzw. die Inanspruchnahme der Dienstleistung erforderlich ist, bezieht sich nicht auf das „Ob“ der Auslagerung, sondern auf das „Wie“ der Inanspruchnahme, also die konkrete Art und Weise der Einbindung des Dritten im Hinblick auf den Umfang der damit einhergehenden Offenbarung von der Schweigepflicht unterliegenden Mandantendaten. Denn die unternehmerische Entscheidung über die Einbindung Dritter, also das „Ob“ der Mitwirkung Dritter, wird vom Gesetzgeber nicht hinterfragt, und steht – wie bisher auch – im pflichtgemäßen Ermessen des Berufsträgers.

Unerheblich ist also, ob die Einschaltung Dritter als solche aus organisatorischen, fachlichen oder wirtschaftlichen Gründen erforderlich ist oder nicht; dem WP/vBP steht es somit frei, sich von betriebswirtschaftlichen Erwägungen leiten zu lassen. Namentlich die Zulässigkeit der Auslagerung wichtiger Prüfungstätigkeiten bleibt hiervon unberührt, freilich nach Maßgabe der Vorgaben der § 55b Abs. 2 Satz 2 Nr. 9 WPO i.V.m. §§ 51 Nr. 14, 62 BS WP/vBP.

Hinsichtlich des „Wie“ der Mitwirkung gilt allerdings das „Need-to-know-Prinzip“. Das heißt, den mitwirkenden Personen darf nur soweit Kenntnis von fremden Geheimnissen verschafft werden, wie dies zur Vertragserfüllung erforderlich ist (§ 50a Abs. 3 Satz 2 Nr. 2 WPO). Der WP/vBP hat

die mitwirkende Person entsprechend vertraglich zu verpflichten (siehe *IDW Muster „Vereinbarung über die Einhaltung gesetzlicher Geheimhaltungspflichten“* nach § 50a WPO). Neben der Verpflichtung auf eine durch die Leistungspflicht limitierte Kenntnisnahme kann es im Einzelfall ratsam sein, weitere Absprachen zu treffen, die die Möglichkeit der Kenntnisnahme auch faktisch begrenzen bzw. dem WP/vBP eine Überwachung des Zugriffs durch die mitwirkende Person erlauben.

4.2.2. Der Einsatz von „Sub-Dienstleistern“ (§ 203 Abs. 3, 4 StGB, § 50a Abs. 3 Satz 2 Nr. 3 Halbsatz 2 WPO)

Der Einsatz von Sub-Dienstleistern durch den Dienstleister, die „weitere“ (mitwirkende) Personen i.S. des § 203 Abs. 3 Satz 2 Halbsatz 2 StGB sind, ist ebenfalls rechtssicher möglich. Verpflichtet die „sonstige mitwirkende Person“ (Dienstleister) die von ihr unterbeauftragte „weitere Person“ (Subunternehmer, „Sub-Dienstleister“) nicht zur Verschwiegenheit, macht sich der Dienstleister strafbar unter der weiteren Voraussetzung, dass die nicht zur Verschwiegenheit verpflichtete „weitere Person“ ein fremdes Geheimnis tatsächlich unbefugt offenbart hat.

Die Verpflichtung auf die Geheimhaltung ist gemäß § 203 Abs. 4 Satz 2 Nr. 2 Halbsatz 2 StGB allerdings auch in dieser Fallkonstellation entbehrlich, wenn diese „weiteren Personen“ ihrerseits bereits unmittelbar einer berufsrechtlichen oder öffentlich-rechtlichen Schweigepflicht unterliegen, wie etwa WP/vBP, RA, StB oder öffentliche Amtsträger.

Berufsrechtlich ist zu beachten, dass der entsprechende Dienstleistervertrag eine Regelung zur Zulässigkeit des Einsatzes von Sub-Unternehmern durch den Dienstleister enthalten muss (§ 50a Abs. 3 Satz 2 Nr. 3 WPO), siehe *IDW Muster „Vereinbarung über die Einhaltung gesetzlicher Geheimhaltungspflichten“* nach § 50a WPO, s.o. Abschn. 4.2.1.).

4.2.3. Sorgfältige Auswahl des Dienstleisters und Beendigung der Zusammenarbeit (§ 50a Abs. 2 WPO)

§ 50a Abs. 2 WPO verpflichtet den WP/vBP, den Dienstleister sorgfältig auszuwählen. Letztlich lässt sich das Gebot der sorgfältigen Auswahl des Dienstleisters vom Rechtsgrundsatz der im Verkehr erforderlichen Sorgfalt (§ 276 Abs. 1 Satz 2 BGB) ableiten, der wiederum seinen berufsrechtlichen Niederschlag in der in § 43 Abs. 1 Satz 1 Nr. 1 WPO kodifizierten Grundpflicht des WP/vBP zur gewissenhaften Berufsausübung gefunden hat und in der Berufssatzung vielfältig konkretisiert wird.

4.2.3.1. Sorgfaltsmaßstab und geeignete Kriterien für die Überprüfung

Als Sorgfaltsmaßstab für die Dienstleisterauswahl sind insb. die fachliche Eignung für die beauftragte Dienstleistung sowie die Zuverlässigkeit des Dienstleisters anzulegen.

Zur Orientierung hinsichtlich der Anforderungen an die Auswahl von Dienstleistern können die Regelungen zur Auftragsverarbeitung im Datenschutzrecht dienen, die ebenfalls eine Pflicht zur

sorgfältigen Auswahl durch den Auftraggeber vorsehen, die sich insb. auf die Einhaltung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten beziehen (vgl. Artikel 28 Abs. 1, 3 DS-GVO). Maßstab ist die Angemessenheit der getroffenen technischen und organisatorischen Schutzmaßnahmen im Hinblick auf den angestrebten Schutzzweck. Es gibt keine starren Kriterien der Eignung und Erforderlichkeit von Maßnahmen, sondern diese müssen im Einzelfall für den jeweiligen Zweck und die jeweilige Dienstleistung angemessen sein.

Der WP/vBP muss sich von der fachlichen Eignung und Zuverlässigkeit des Dienstleisters überzeugen. Nachgewiesene (Interne-Kontrollsystem/(IKS)-)Zertifizierungen des Dienstleisters und sonstige Qualifikationsnachweise können hierbei eine Hilfe sein. Dies gilt allerdings nur dann, wenn die entsprechenden Zertifizierungen auch alle Systeme und Bereiche beim Dienstleister abdecken, die für die konkrete Dienstleistung relevant sind.

Werden daher IKS-Zertifizierungen bei der Auswahl des Dienstleisters als Kriterium für die fachliche Eignung und Zuverlässigkeit herangezogen, sollte hierbei insb. beachtet werden:

- Die Vorlage eines Zertifikats kann regelmäßig als Nachweis genügen, wenn die Zertifizierung von einem qualifizierten Anbieter durchgeführt wurde und der Gegenstand der Zertifizierung sich unmittelbar aus dem Zertifikat ergibt. So muss aus dem Zertifikat erkennbar sein, ob die für die Dienstleistung relevanten Systeme und Bereiche des Dienstleisters überhaupt zertifiziert sind.
- Wenn Zweifel bezüglich des Gegenstands der Zertifizierung bestehen, sind schon zur eigenen Vergewisserung weitere aufschlussreichere Nachweise einzuholen (z.B. Prüfbericht).

Sind Tatsachen bekannt oder erkennbar, die Zweifel an der Zuverlässigkeit des Dienstleisters begründen, darf dieser nicht beauftragt werden.

Ein weiteres Kriterium kann der Stand der Technik der beim Dienstleister getroffenen Sicherheitsmaßnahmen sein. Der Stand der Technik und daran orientierte Kriterien sind jedoch i.d.R. Bestandteil von anerkannten Standards und Zertifizierungen.

Diese Kriterien spielen eine zentrale Rolle für IT-Dienstleistungen. Da bei fast jeder Form des Outsourcens von Dienstleistungen ein elektronischer Transfer und Speicherung von Informationen und Daten stattfindet, können die Kriterien der technischen und organisatorischen Informationssicherheit auch als Auswahlmaßstab für andere Dienstleister herangezogen werden.

4.2.3.2. Umfang und Intensität der Auswahlentscheidung, Zuverlässigkeitsprüfung [vgl. auch Abschn. 5, S. 22]

Umfang und Intensität der einer sorgfältigen Auswahl voranzustellenden Zuverlässigkeitsprüfung sind branchenabhängig. Sie hängen nicht zuletzt davon ab, inwieweit der Dienstleister bestimmungsgemäß oder potentiell Zugang zu vertraulichen Daten erhält und welche Qualität

diese Daten im konkreten Fall haben. Zu denken ist bspw. an standardisierte Background Checks und IT-Security Checks des Dienstleisters.

Die Frage, ob es sich um einen Dienstleister mit Sitz im Inland oder Ausland handelt, spielt beim anzulegenden Sorgfaltsmaßstab der Auswahlentscheidung an dieser Stelle keine eigenständige Rolle, inländische und ausländische Dienstleister unterliegen insofern demselben Prüfungsmaßstab.

Die Pflicht des WP/vBP zur sorgfältigen Auswahl des Dienstleisters gilt nach Maßgabe von § 50a Abs. 6 WPO auch im Fall der Inanspruchnahme von Dienstleistungen, in die der Mandant eingewilligt hat, sofern der Mandant nicht ausdrücklich auf die Einhaltung vorgenannter Anforderungen verzichtet hat.

4.2.3.3. Beendigung der Zusammenarbeit [vgl. auch Abschn. 5, S. 23]

Nach § 50a Abs. 2 WPO ist der WP/vBP zur unverzüglichen Beendigung der Zusammenarbeit mit dem Dienstleister verpflichtet, wenn die Einhaltung der Vorgaben an den Inhalt eines Vertrags mit einem Dienstleister gemäß § 50 Abs. 3 WPO durch den Dienstleister nicht gewährleistet ist. Werden dem WP/vBP Umstände bekannt, aus denen sich konkrete Zweifel an der mit Blick auf die Verschwiegenheitspflicht erforderlichen Zuverlässigkeit ergeben und nach Überprüfung verbleiben, muss die Zusammenarbeit nach Auffassung des Gesetzgebers beendet werden.

Diese Beendigungstatbestände sollten Gegenstand des Dienstleistungsvertrags sein; es empfiehlt sich, ein außerordentliches Kündigungsrecht vorzusehen für den Fall, dass der Dienstleister die berufsrechtlichen Vorgaben nicht gewährleistet. Sollte ein solches außerordentliches Kündigungsrecht nicht vereinbart sein, ist jedenfalls die Zusammenarbeit faktisch zu beenden (siehe *IDW Muster „Vereinbarung über die Einhaltung gesetzlicher Geheimhaltungspflichten" nach* § 50a WPO, s.o. Abschn. 4.2.1.).

Nicht ganz klar ist, inwieweit dieser Regelung eine Überwachungspflicht des WP/vBP immanent ist. Eine ausdrückliche Überwachungspflicht wurde im Laufe des Gesetzgebungsverfahrens wieder gestrichen. Dennoch erscheint eine wirksame Sicherstellung der Pflicht zur Beendigung der Zusammenarbeit ohne Überprüfungsmöglichkeit kaum möglich. Daher könnte es für den WP/vBP ratsam sein, sich gegenüber dem Dienstleister Kontrollmöglichkeiten zu verschaffen, etwa durch regelmäßige Erneuerung des für die Auswahlentscheidung maßgeblichen Zertifikats oder aber durch eine Anzeigepflicht von Vorfällen, die für die Zuverlässigkeitsbeurteilung relevant sind, wie etwa bei Datenverlusten oder Zugriffen Dritter. Damit wird dem WP/vBP bei konkreten Zweifeln eine Überprüfung ermöglicht, ob der Dienstleister seinen Verpflichtungen aus § 50a Abs. 3 WPO noch nachkommt (siehe *IDW Muster „Vereinbarung über die Einhaltung gesetzlicher Geheimhaltungspflichten"* nach § 50a WPO, s.o. Abschn. 4.2.1.).

Jedenfalls empfiehlt es sich, den Dienstleister vertraglich zu verpflichten, dem WP/vBP unverzüglich mitzuteilen, wenn er die gemäß § 50a Abs. 3 WPO einzuhaltenden Vorgaben nicht mehr gewährleisten kann. § 50a WPO verlangt nicht explizit, dass der Dienstleister zur Errichtung eines IKS zu verpflichten ist, das spezifisch die Einhaltung der berufsrechtlichen Anforderungen überwacht. Dennoch dürfte das Vorhandensein wirksamer interner Kontrollen beim Dienstleister ein Kriterium der Dienstleisterauswahl darstellen. So sollten die getroffenen Sicherheitsmaßnahmen und insb. die technische Sicherstellung des Need-to-know-Prinzips (vgl. Abschn. 4.2.1.) regelmäßigen Kontrollen durch den Dienstleister selbst unterliegen und damit auch das Aufdecken von Verstößen ermöglichen. Zu den internen Überwachungsmaßnahmen des Dienstleisters mit Relevanz für die berufsrechtlichen Pflichten des § 50a Abs. 3 WPO gehören u.a. die regelmäßigen Überprüfungen des Zugriffsberechtigungskonzepts einschließlich der vergebenen Zugriffsberechtigungen sowie das Logging und regelmäßige Kontrolle der Zugriffe auf Systeme und auf Informationen.

Die Pflicht des WP/vBP, die Zusammenarbeit unverzüglich zu beenden, gilt nach Maßgabe von § 50a Abs. 6 WPO auch im Fall der Inanspruchnahme von Dienstleistungen, in die der Mandant eingewilligt hat, sofern der Mandant nicht ausdrücklich auf die Einhaltung der in § 50a Abs. 3 WPO genannten Anforderungen verzichtet hat.

4.2.4. Anforderungen an die Vertragsgestaltung (§ 50a Abs. 3 WPO)

§ 50a Abs. 3 WPO regelt die berufsrechtlichen Mindestinhalte für einen Vertrag mit einem Dienstleister. Das IDW hat am 27.11.2018 ein Muster für eine Vereinbarung über die Einhaltung gesetzlicher Geheimhaltungspflichten nach § 50a WPO veröffentlicht, die zusätzlich oder als Teil des Dienstleistungsvertrags getroffen werden kann.

4.2.4.1. Verschwiegenheitsverpflichtungs- und Belehrungsklausel

§ 50a Abs. 3 Satz 2 Nr. 1 WPO regelt die Pflicht des WP/vBP, den Dienstleister auf die Verschwiegenheit vertraglich zu verpflichten und über die strafrechtlichen Folgen eines Verstoßes gegen die Verschwiegenheitspflicht zu belehren. Da Rechtskundigkeit des zu Verpflichtenden nicht regelmäßig vorausgesetzt werden kann, dürfte es zumindest die Effektivität der Belehrung erhöhen (wenn auch nicht zwingend sein), den Text der in der Vereinbarung genannten Strafvorschriften ergänzend in einer Anlage beizufügen.

Der Gesetzgeber bezieht ausweislich der Gesetzesbegründung zum Berufsgeheimnisschutzgesetz in den Kreis weiterer Personen i.S. des § 50a Abs. 3 Satz 2 Nr. 1 WPO auch die Beschäftigten des jeweiligen Dienstleisters ein. Sofern der jeweilige Dienstleistungsvertrag also nicht mit einem Einzelunternehmer geschlossen wird, der über keinerlei weitere Beschäftigten verfügt, muss die Vereinbarung mithin immer auch die Verpflichtung des Auftragnehmers enthalten, seine Beschäftigten ebenfalls in Textform zur Verschwiegenheit zu verpflichten. Da dies die Gestattung der Mitwirkung der eigenen Beschäftigten des Auftragnehmers impliziert (und diese

ohnehin regelmäßig gewollt sein wird), wird daneben der Ausspruch einer ausdrücklichen Gestattung jedenfalls für eigene Beschäftigte des Auftragnehmers nicht gesondert erforderlich sein.

Eine darüberhinausgehende Verpflichtung des WP/vBP, zu überwachen, ob der Dienstleister die weiteren Personen, derer er sich bedient, tatsächlich zur Verschwiegenheit verpflichtet hat, lässt sich weder dem Gesetz noch der Gesetzesbegründung entnehmen und dürfte dem Ziel des Gesetzes, dem Berufsträger die Einschaltung externer Dritter grundsätzlich zu erleichtern, wegen des damit verbundenen unverhältnismäßigen Aufwandes zuwiderlaufen. Eine derartige Überwachungspflicht erscheint im Übrigen auch deswegen nicht geboten, weil sich der Dienstleister selbst nach § 203 Abs. 4 Satz 2 Nr. 2 StGB strafbar machen könnte, wenn er es unterließe, eingeschaltete weitere Personen seinerseits zur Verschwiegenheit zu verpflichten.

4.2.4.2. Erforderlichkeitsklausel

Darüber hinaus ist der Dienstleister gemäß § 50a Abs. 3 Satz 2 Nr. 2 WPO vertraglich zu verpflichten, sich nur insoweit Kenntnis von fremden Geheimnissen zu verschaffen, als dies zur Vertragserfüllung erforderlich ist (vgl. Abschn. 4.2.1.).

4.2.4.3. Unterbeauftragungsklausel

Schaltet der Dienstleister seinerseits weitere Personen (z.B. Subunternehmer) ein, ist dies gemäß § 50a Abs. 3 Satz 2 Nr. 3 Halbsatz 1 WPO nur zulässig, sofern der Dienstleister hierzu im Dienstleistungsvertrag befugt ist (vgl. Abschn. 4.2.2.). Erteilt der WP/vBP seinem Dienstleister die Befugnis zur Unterbeauftragung, muss der WP/vBP gemäß § 50a Abs. 3 Satz 2 Nr. 3 Halbsatz 2 WPO seinem Dienstleister im Falle einer Unterbeauftragung die Pflicht auferlegen, seinerseits diese weiteren Personen (z.B. eigene Angestellte, Subunternehmer) in Textform zur Verschwiegenheit zu verpflichten.

Praktisch muss die Lösung hier über die Unterauftragnehmer-Regelung (§ 50a Abs. 3 Satz 2 Nr. 3 WPO) im Vertrag mit dem Dienstleister erfolgen (siehe *IDW Muster „Vereinbarung über die Einhaltung gesetzlicher Geheimhaltungspflichten“* nach § 50a WPO, s.o. Abschn. 4.2.1.).

Diese Unterauftragnehmer-Klausel sollte folgende Regelungen enthalten:

- Regelung des „Ob“ und des „Wie“ des Einsatzes von Unterauftragnehmern
- ggf. das Recht des WP/vBP zur Genehmigung bzw. Ablehnung von (neuen) Unterauftragnehmern – zumindest mit Blick auf die Auslandsklausel nach § 50a WPO (vgl. Abschn. 4.2.5.) – und die korrespondierende Möglichkeit der Kenntnisnahme bzw. Information über den Stand der beauftragten Subunternehmer und etwaige Änderungen
- Verpflichtung des Dienstleisters, seinen Unterauftragnehmern vertraglich die gleichen bzw. gleichwertige Pflichten (zum Schutz von Berufsgeheimnissen) aufzuerlegen, wie im Vertrag mit dem WP/vBP vereinbart.

4.2.4.4. Form des Dienstleistungsvertrags

Hinsichtlich der Form des abzuschließenden Dienstleistungsvertrags genügt gemäß § 50a Abs. 3 Satz 1 WPO die Textform i.S.v. § 126b Satz 1 BGB, also eine lesbare Erklärung, in der die Person des Erklärenden genannt ist und die auf einem dauerhaften Datenträger i.S.v. § 126b Satz 2 BGB abgegeben wird. Mit einer E-Mail z.B. ist die Textform gewahrt.

4.2.5. Dienstleistungen, die im Ausland erbracht werden – „Auslandsklausel" (§ 50a Abs. 4 WPO)

Neben den Anforderungen der Absätze 1 bis 3 des § 50a WPO gelten für Dienstleistungen, die im Ausland erbracht werden, weitergehende Anforderungen, die in § 50a Abs. 4 WPO geregelt sind (sog. Auslandsklausel).

So darf der WP/vBP bei Dienstleistungen, die im Ausland erbracht werden, dem Dienstleister (und auch dessen etwaigen Subunternehmern, die Leistungen aus dem Ausland erbringen) nur Zugang zu fremden Geheimnissen verschaffen, wenn der dort bestehende Schutz der Geheimnisse dem Schutz im Inland vergleichbar ist. Eine Ausnahme von dem Erfordernis eines vergleichbaren Schutzniveaus besteht, wenn „der Schutz der Geheimnisse dies nicht gebietet".

Hierzu hat das IDW unter dem Datum vom 07.02.2018 eine *Auslegungshilfe „Inanspruchnahme ausländischer Dienstleistungen gem. § 50a Abs. 4 WPO"*[3] veröffentlicht, auf deren Inhalte hier verwiesen wird.

4.2.6. Besonderheiten bei der Inanspruchnahme von Dienstleistungen, die unmittelbar einem einzelnen Mandat dienen – Einwilligung (§ 50a Abs. 5 WPO) [vgl. auch Abschn. 6.3.]

Nach § 50a Abs. 5 WPO ist bei der Inanspruchnahme von Dienstleistungen, die unmittelbar einem einzelnen Mandat dienen, eine Einwilligung des Mandanten erforderlich, bevor der WP/vBP dem Dienstleister Zugang zu fremden Geheimnissen eröffnen darf (vgl. Abschn. 6.3.).

Ob eine Dienstleistung unmittelbar einem einzelnen Mandat dient, muss unter Berücksichtigung der Umstände des Einzelfalls festgestellt werden.

Nicht unmittelbar einem einzelnen Mandat dienen jedenfalls Dienstleistungen, die die allgemeine Praxisorganisation betreffen, z.B. Honorarabrechnungen (vgl. WPK-Praxishinweis „Mitwirkung Dritter an der Berufsausübung (§§ 50, 50a WPO)", Stand: 26.07.2018).

[3] https://www.idw.de/blob/106944/e8b3217638ccc181e2d152575422ed04/down-dienstleistungen-ausland-2018-data.pdf.

Stand: 10.04.2019

4.2.6.1. Fachlich-inhaltliche Befassung als Gegenstand der Dienstleistung

Praktisch wird man zunächst bei der Art der Dienstleistung ansetzen müssen und als Unterscheidungsmerkmal eine unmittelbare fachlich-inhaltliche Befassung mit dem Mandat durch den Dienstleister anlegen. Dies bedeutet, dass alle nicht inhaltsbezogenen Dienstleistungen, die der Berufsträger im Tagesgeschäft in seinem Geschäftsbetrieb einsetzt, z.B. infrastrukturelle (IT-) Dienstleistungen, nicht unter § 50a Abs. 5 WPO fallen.

Die in der Gesetzesbegründung zum Berufsgeheimnisschutzgesetz aufgeführten Beispiele von Dienstleistern, die typischerweise einem einzelnen Mandat unmittelbar dienen, nämlich Sachverständige, Detektive und Übersetzer, machen ebenfalls deutlich, dass es sich beim Unmittelbarkeitskriterium um eine gezielte und umfassende inhaltlich-fachliche Auseinandersetzung des Dienstleisters mit dem Mandat im konkreten Einzelfall handeln muss, für die es einen „besonderen Bedarf“ gibt.

Entscheidend wird sein, ob ein direkter Zugriff auf die der Verschwiegenheit unterliegenden Mandantendaten für die ordnungsgemäße Erfüllung der Dienstleistung zwingend notwendig ist, weil sich der Dienstleister mit den Daten inhaltlich auseinandersetzen muss, oder ob der (potentielle) Zugriff des Dienstleisters für die ordnungsgemäße Durchführung der Dienstleistung zwar aus technischen Gründen notwendig, aber lediglich eine mittelbare Nebenfolge ist. So muss etwa der Vertrag, der vom Übersetzer übersetzt oder von einem Sachverständigen beurteilt werden soll, dem Übersetzer und Sachverständigen auch vollständig und unverschlüsselt zur Verfügung gestellt werden, damit er seine Aufgabe ordnungsgemäß erfüllen kann. Bei IT-Dienstleistungen ist dies z.B. dann nicht der Fall, wenn der (potentielle) Zugriff nur zu technischen Zwecken (z.B. Reparatur oder Wiederherstellung beschädigter Dateien) erfolgt. Die Möglichkeit, auf Klardaten des Mandanten Zugriff zu nehmen, ist in diesem Fall eine mittelbare Nebenfolge, sodass die Tätigkeit nicht unmittelbar dem einzelnen Mandanten dient, sondern über den Einzelfall hinausgeht.

4.2.6.2. Individualisierungsgrad der Dienstleistung

Auch für fachlich-inhaltliche Dienstleistungen muss zusätzlich ein gewisser Grad an Individualisierung angenommen werden, um den Anwendungsbereich des Einwilligungserfordernisses des § 50a Abs. 5 WPO sinnvoll abgrenzen zu können.

So unterfallen Dienstleistungen ebenfalls nicht dem § 50a Abs. 5 WPO, die im Zusammenhang mit zwar fachlich-inhaltlichen, jedoch standardisierten Vorgängen stehen, die für eine Vielzahl von Mandanten angewendet werden, bspw. die Einholung von Saldenbestätigungen für eine Vielzahl von Mandanten. Auch wenn diese Tätigkeiten letztlich „dem einzelnen Mandat“ dienen, handelt es sich dennoch um eine standardisierte Tätigkeit, die entsprechend der Praxisorganisation für alle Mandate gleichermaßen durchzuführen ist.

Aus dem Anwendungsbereich des § 50a Abs. 5 WPO ausgenommen werden müssen darüber hinaus alle Fälle, in denen der WP/vBP berufsrechtlich (z.B. aus Qualitätssicherungsgründen oder im Rahmen einer berufsrechtlich veranlassten Konsultation) verpflichtet ist, einen sachverständigen Dritten aufgrund dessen besonderer Fachexpertise zu einer konkreten Frage in einem konkreten Mandat einzubinden. Hier würde der WP/vBP in eine Pflichtenkollision laufen, wenn der Mandant in die Einschaltung des externen Experten nicht einwilligte.

Der jeweilige Sachverhalt oder Einzelfall sollte sorgfältig geprüft und bei sich ergebenden Zweifeln hinsichtlich der „Unmittelbarkeit" eine übliche, informierte Einwilligung eingeholt werden, die ggf. auch konkludent erfolgen kann – sofern die Möglichkeit der Einbindung unmittelbar im Mandat tätiger Dritter nicht ohnehin vertraglich vereinbart wurde.

Praxishinweis

Bei wirksamer Einbeziehung der Allgemeinen Auftragsbedingungen für WP/vBP und WPG/BPG (AAB)[4] muss die Einbindung Dritter nicht gesondert geregelt werden. Denn nach Maßgabe von Ziffer 2 Abs. 1 Satz 5 AAB ist der WP/vBP berechtigt, sich zur Durchführung des Auftrags sachverständiger Personen zu bedienen. Etwas anders gilt für die Einschaltung Dritter aus Netzwerkgesellschaften, die keinem unmittelbaren Weisungsrecht des WP/vBP unterliegen oder ihre Dienstleistung aus dem Ausland heraus erbringen (vgl. Abschn. 4.2.5. *IDW Auslegungshilfe „Inanspruchnahme ausländischer Dienstleistungen gem. § 50a Abs. 4 WPO"*). Hier sollte im Auftragsbestätigungsschreiben eine entsprechende Netzwerk- bzw. Auslandsklausel aufgenommen werden, sofern dies nicht ohnehin bereits erfolgt ist.

Die Vorgaben für den Einsatz von Dienstleistern nach § 50a Abs. 1 bis 3 WPO gelten nach Maßgabe von § 50a Abs. 6 WPO auch im Fall der Inanspruchnahme von Dienstleistungen, in die der Mandant eingewilligt hat, sofern der Mandant nicht ausdrücklich auf die Einhaltung vorgenannter Anforderungen verzichtet hat.

Daher sollte kontrolliert werden, ob es in schon vor Inkrafttreten des § 50a WPO bestehenden Vertragsverhältnissen mit Dienstleistern noch Nachbesserungsdarf gibt. Insbesondere muss eine Aufklärung der Dienstleister über die Strafbarkeit von Verstößen gegen die Verschwiegenheitsverpflichtungen erfolgen, soweit eine solche noch nicht im Vertrag erfolgt ist.

5. Technische und organisatorische Maßnahmen in der WP-Praxis

Die auslagernde WP/vBP-Praxis hat die Einhaltung der gesetzlichen Anforderungen (§§ 43 Abs. 1 WPO, 333 HGB, 203 StGB) sicherzustellen, und zwar unabhängig von der eingesetzten (Informations-)Technologie, den implementierten Geschäftsprozessen oder den angewandten

[4] Erhältlich beim IDW Verlag unter https://shop.idw-verlag.de/product.idw;jsessionid=99FFC960E26256F876296C0F76815F86?product=50261

Geschäftsmodellen bei der Verarbeitung von dem Verschwiegenheitsgrundsatz unterliegenden Daten.

Je nach Art und Umfang der eingesetzten (Informations-)Technologie sind die technischen und organisatorischen Sicherungsmaßnahmen auszugestalten. Dabei gilt, dass die technischen und organisatorischen Sicherungsmaßnahmen der WP/vBP-Praxis umso umfassender sein müssen, je höher das Risiko eines unberechtigten Zugriffs auf die vertraulichen Informationen ist. Dabei müssen die technischen und organisatorischen Maßnahmen in einem angemessenen Verhältnis zu den identifizierten Risiken stehen (Skalierung).

Dementsprechend hat die WP/vBP-Praxis ein dem Risiko angepasstes internes Qualitätssicherungssystem (QSS) einzurichten. Das QSS soll in einem angemessenen Verhältnis zum Umfang und zur Komplexität der beruflichen Tätigkeit des WP/vBP und den ausgelagerten Funktionen stehen (Skalierung des QSS).[5] Dabei muss die WP/vBP-Praxis Risiken im Zusammenhang mit der Inanspruchnahme externer Dienstleister und den geplanten Outsourcing-Projekten feststellen und beurteilen. Zur Adressierung der Risiken sind im QSS Regelungen zur Einrichtung wirksamer und angemessener Kontroll- und Sicherheitsvorkehrungen für eingesetzte Datenverarbeitungssysteme und die Inanspruchnahme Dritter in der allgemeinen Praxisorganisation einzuführen.

Daher gehört es auch zu den Aufgaben der gesetzlichen Vertreter der WP/vBP-Praxis, das (IT-)Outsourcing von Beginn an bis zur Beendigung der Auslagerung zu steuern und zu überwachen.[6] Dazu sind die mit der Auslagerung verbundenen Risiken in der Vorbereitungsphase systematisch zu analysieren und strukturieren und deren Auswirkungen auf das QSS der WP/vBP-Praxis zu ermitteln.

Zu Beginn der Vorbereitungsphase sind im Rahmen der Anforderungsdefinition der Umfang der auszulagernden Prozesse und Funktionen, die geplante Aufteilung von Aufgaben zwischen der WP/vBP-Praxis und dem Dienstleistungsunternehmen (Aktivitätensplit) und die im auslagernden Unternehmen verbleibende Organisation (Retained Organisation) und ggf. auf ein Dienstleistungsunternehmen übergehende Organisationsteile festzulegen. Auf Grundlage dieser Anforderungsdefinition der WP/vBP-Praxis sind die Risiken des geplanten (IT-)Outsourcings festzustellen und zu beurteilen. Beim Cloud Computing sind darüber hinaus die sich aus den Service- und Bereitstellungsmodellen ergebenden Risiken zu beachten.

In Bezug auf das IT-System der WP/vBP-Praxis ergeben sich bei der Inanspruchnahme von Cloud-Services Gefährdungslagen insb. aus folgenden Sachverhalten:

---

[5] Vgl. IDW Qualitätssicherungsstandard: Anforderungen an die Qualitätssicherung in der Wirtschaftsprüferpraxis *(IDW QS 1)* (Stand: 09.06.2017), Tz. 5, 6.

[6] Vgl. hierzu auch die sieben Phasen nach BSI Grundschutz im Falle des IT-Outsourcing. In Bezug auf das IT-Outsourcing einer WP/vBP-Praxis sind die Phasen in der Anlage zu Abschn. 5 (s.u.) ausführlich dargestellt.

- Ausfall des Wide Area Network (WAN) zur Anbindung an den Cloud-Dienstleister
- mangelndes Berechtigungskonzept für den lokalen IT-Zugriff
- unerlaubte Ausübung von Zugriffsrechten durch Verwendung fremder Zugangsdaten sowie ungeeigneter Umgang mit Passwörtern/Authentifikationsmechanismen
- nicht hinreichendes Administrationsmodell für die Cloud-Nutzung
- nicht hinreichende Dokumentation (insb. für den Notfallbetrieb)
- Verwendung unsicherer Protokolle in öffentlichen Netzen
- unzureichende personelle Ressourcen mit ausreichender IT-Kompetenz
- unzureichende Planung der Migration der Cloud-Nutzung
- Ausfall von Tools zur Administration der Cloud-Nutzung.

Darüber hinaus ergeben sich mittelbar Gefahren im Zusammenhang mit Cloud-Services aus folgenden Sachverhalten:

- nicht hinreichende vertragliche Regelungen mit einem externen Dienstleister, auch in Bezug auf die Behebung von Ausfällen (SLA/Service Level Agreements)
- nicht hinreichende vertragliche Regelungen für das Ende des Outsourcings bzw. der Cloud-Nutzung (Vernichtung der Informationen/Daten; Post-contract Confidentiality)
- Abhängigkeit von einem Outsourcing- oder Cloud-Dienstleister
- unzureichende Vorgaben zum Lizenzmanagement bei Cloud-Nutzung
- unzureichende Strategie für die Cloud-Nutzung
- mangelnde Überwachung der Service-Erbringung.

Dementsprechend sollte sich die auslagernde WP/vBP-Praxis bereits zum Zeitpunkt der Entscheidung über die Auslagerung von beruflichen Prozessen und Funktionen ein umfassendes Bild von dem Dienstleistungsunternehmen und dessen technischen und organisatorischen Sicherungsmaßnahmen machen. Erfahrungsgemäß wird es häufig dazu kommen, dass ein Outsourcing-Dienstleister – nicht zuletzt zur Wahrung der Informationssicherheit – einen unmittelbaren Zugriff auf die eigenen (IT-)Ressourcen nicht ermöglichen wird. In diesen Fällen ist die Überprüfung der Ausgestaltung, Wirksamkeit und Implementierung des IKS des Dienstleistungsunternehmens durch die WP/vBP-Praxis nicht unmittelbar möglich.

Um den rechtlichen Anforderungen an die WP/vBP-Praxis dennoch zu genügen, können alternative Nachweise eingeholt werden. Insbesondere die (revolvierende) Vorlage von aktuellen Berichten über eine Zertifizierung (z.B. nach dem Anforderungskatalog Cloud-Computing (C5)

des BSI) kann insoweit eigene Prüfungshandlungen der auslagernden WP/vBP-Praxis ersetzen. Dabei sind die Vorgaben zur Verwertung bzw. Verwendung der Arbeiten Dritter[7] anzuwenden.

Zur Bewältigung der Risiken des (IT-)Outsourcings während der Nutzungsphase haben die gesetzlichen Vertreter das QSS um Grundsätze, Verfahren und Maßnahmen (Regelungen) zu ergänzen bzw. zu erweitern, die zur Steuerung des (IT-)Outsourcings dienen und die Überwachung der Einhaltung dieser Regelungen sicherstellen.

Daneben bieten sich für eine Überwachung der Angemessenheit und Wirksamkeit des (IT-)Kontrollsystems beim Outsourcing-Dienstleister regelmäßige Berichterstattungen durch diesen an. Hierdurch kann die WP/vBP-Praxis regelmäßig beurteilen, ob die ursprünglich mit dem Dienstleister vereinbarten Regelungen weiterhin eingehalten werden. Dabei erscheint eine jährliche Überprüfung durch die WP/vBP-Praxis i.d.R. angemessen. Eine kontinuierliche Überwachung im Sinne einer vollständigen Integration der WP/vBP-Praxis in Regelprozesse des Dienstleisters zu dessen Überwachung ist hingegen nicht notwendig.

In Einzelfällen mag es sinnvoll und möglich sein, automatische Überwachungsprogramme (Scanning) zu implementieren oder programmgestützte Angriffssimulationen (Penetration-Test-Verfahren), bspw. nach dem Open Source Security Testing Methodology Manual (OSSTMM), in Abstimmung mit dem Dienstleistungsunternehmen durchzuführen. Damit können die eingerichteten (IT-)Kontrollmaßnahmen unter Echtzeitbedingungen auf ihre Angemessenheit und Wirksamkeit überprüft werden („Attack and Penetration“). Sofern die Durchführung solcher IT-Sicherheitstests durch die WP/vBP-Praxis nicht unmittelbar möglich ist, können auch hier anerkannte Zertifizierungen, z.B. nach *IDW PS 860* i.V.m. BSI-C5, ISO 27001, OSSTMM, diese ersetzen. Die WP/vBP-Praxis hat sich hierzu die entsprechenden Nachweise vorlegen zu lassen und dabei die Grundsätze zur Verwertung bzw. Verwendung der Arbeiten Dritter zu beachten.

Korrespondierende generelle Kontrollen können darüber hinaus in Einzelfällen für das IT-Outsourcing die Durchsicht folgender Unterlagen vorsehen:

- Nachweise über kritische Systemberechtigungen sowie deren Nutzung
- Protokolle über nicht erfolgreiche Systemzugriffe
- Protokolle über unerwartete Ereignisse (Systemabstürze und -neustarts etc.)
- Nachweise über Systemänderungen (Einspielen neuer oder geänderter Software wie Releasewechsel und Fehlerbereinigungen, Veränderungen von Parametern und Steuerungsdaten)
- Nachweise der vom Dienstleistungsunternehmen vorgenommenen Tests.

---

[7] Vgl. *IDW Prüfungsstandard: IT-Prüfung außerhalb der Abschlussprüfung (IDW PS 860)* (Stand: 02.03.2018), Tz. 63 ff.

Auch für den Zeitpunkt der Beendigung des Outsourcings ist eine Risikoanalyse durchzuführen und hat das QSS der auslagernden WP/vBP-Praxis angemessene und wirksame Kontrollen vorzusehen, um die straf- und berufsrechtlichen Anforderungen an die Verschwiegenheit sicherzustellen. Insbesondere die vollständige Herausgabe der durch den Dienstleister verwalteten Informationen und Daten sollte bereits zu Beginn des Outsourcing-Projekts vertraglich zwischen den Parteien vereinbart werden. Sofern Informationen durch das Dienstleistungsunternehmen zu vernichten sind (z.B. Kopien von Datenbeständen), sind angemessene und wirksame Kontrollen bei dem Dienstleistungsunternehmen zu vereinbaren, die dies gewährleisten. So mag die Vereinbarung einer Datenvernichtung nach DIN 66399 Schutzklasse 2 mit einer Sicherheitsstufe 4 (analog Datenschutz) sinnvoll sein, sofern der WP/vBP-Praxis entsprechende Vernichtungsbestätigungen des Dienstleistungsunternehmens vorgelegt werden.

6. Umsetzung der rechtlichen Anforderungen in praktischen Anwendungsfällen

Nachfolgend werden einige typische Anwendungsfälle und Themen aus der Praxis dargestellt. Inhalt und Maß der an externe Dienstleister zu stellenden konkreten Anforderungen sind nicht in jeder Hinsicht und nicht in allen Fällen identisch, sondern können nach Größe und Organisationstiefe des eingeschalteten Dienstleisters wie auch nach Art der jeweils beauftragten ausgelagerten Dienstleistung variieren.

6.1. Beauftragung von IT-Dienstleistungen

6.1.1. Speicherung von Daten

Wird die bloße Speicherung von Daten beauftragt oder bewirkt – sei es durch Anmietung von Servern, sei es durch das Verschieben von Daten „in die Cloud“ –, ist eine Kenntnis des Beauftragten bzw. eingeschalteten Dritten vom Inhalt der Daten grundsätzlich nicht erforderlich. Mit einer Verschlüsselung kann in diesem Fall die Möglichkeit der Kenntnisnahme von diesen Daten ausgeschlossen werden. Benötigt der jeweilige Dienstleister dagegen für Notsituationen (Gefährdung des Datenbestands) oder für notwendige Wartungen Administratorenrechte für einzelne seiner Mitarbeiter, die eine Zugriffsmöglichkeit auch auf den Dateninhalt bedingen, muss die Gewährung derartiger Rechte zulässig sein, da ansonsten die übertragene Speicheraufgabe nicht ordnungsgemäß erbracht werden kann. Da es dann erforderlich ist, den Dienstleister auch zur Verschwiegenheit zu verpflichten (und ihm aufzuerlegen, diese Verpflichtung an die betreffenden Administratoren weiterzugeben, vgl. Abschn. 4.2.4.1.), und den Dienstleister selbst die Strafandrohung des § 203 Abs. 4 Satz 1 StGB trifft, erscheint die Einschaltung eines außerhalb des Dienstleistungsvertrags stehenden, „neutralen“ Dritten zur Aufbewahrung des Datenschlüssels (sog. „Treuhandlösung“) nach der gesetzlichen Neuregelung des § 203 StGB nicht mehr zwingend erforderlich; es muss mithin ebenso möglich sein, den Datenschlüssel später ad hoc oder sogleich bei der Begründung des Vertragsverhältnisses – zur ausschließlichen Verwendung durch die Administratoren des Dienstleisters – zur Verfügung zu stellen.

6.1.2. Sonstige (spezielle) EDV-Dienstleistungen

Der Gesetzgeber spricht in seiner Begründung zu § 203 Abs. 3 StGB davon, dass gegenüber eingeschalteten IT-Spezialisten das Offenbaren im Sinne der Ermöglichung der Kenntnisnahme erforderlich sei, damit deren Tätigkeit wie z.B. Wartung oder Einrichtung der IT-Anlagen überhaupt sinnvoll in Anspruch genommen werden könne. Gleichwohl kann es geboten sein, diesbezüglich auch hier im Einzelfall zu reflektieren und ggf. entsprechende tatsächliche Schutzmaßnahmen zu ergreifen. So wird z.B. bei der Ermöglichung des „Aufschaltens“ auf Computern von Mitarbeitern des WP/vBP auch aus datenschutzrechtlichen Gründen anzuraten sein, eine solche Aufschaltung vorher anzukündigen, um lediglich einen „datenfreien“ Bildschirm für die jeweiligen Arbeiten zur Verfügung zu stellen (anders wiederum, wenn gerade dieses aufgrund eines technischen Defektes nicht mehr möglich sein sollte). Die Gewährung von Administratorenrechten wird aber regelmäßig nicht möglich sein, ohne dass damit auch Zugriffsmöglichkeiten des Administrators auf geschützte Daten bestehen.

6.1.3. IT-Administratoren

Für den praktisch wichtigen Fall der Beauftragung von IT-Dienstleistern gilt, dass hinsichtlich des „Ob“ der Einschaltung zu prüfen ist, ob der WP/vBP alternativ eine hauseigene IT mit bei ihm angestellten IT-Experten vorhalten könnte. Hinsichtlich des „Wie“ ist zu beachten, dass der Umstand, dass ein IT-Dienstleister zur Erfüllung seiner Aufgaben Administratorenrechte eingeräumt bekommt und damit potenziellen Zugriff auf Mandantendaten haben kann, insoweit unschädlich ist, als die dem IT-Dienstleister eingeräumten Administratorenrechte erforderlich sind für Zwecke der ordnungsgemäßen Einrichtung, Betrieb und Wartung des IT-Dienstes.

6.1.4. Verpflichtung auf „need to know“ bei IT-Dienstleistern

§ 50a Abs. 3 Satz 2 Nr. 2 WPO verpflichtet den WP/vBP, dem Dienstleister die Verpflichtung aufzuerlegen, sich nur insoweit Kenntnis von fremden Geheimnissen zu verschaffen, als dies zur Vertragserfüllung erforderlich ist (vgl. Abschn. 4.2.1. und 4.2.4.2.). Die Umsetzung dieser berufsrechtlichen Regelung ist gerade bei der Einschaltung von IT-Dienstleistern sehr hilfreich. Dem WP/vBP wird es häufig nicht möglich sein, ohne Weiteres zuverlässig zu beurteilen, wie weit es erforderlich ist, dem eingeschalteten IT-Dienstleister den Zugang zu vertraulichen Daten und Informationen zu ermöglichen bzw. inwieweit es möglich ist, eine solche Zugangsmöglichkeit zu begrenzen. Hier bietet die vorgenannte Verpflichtung des IT-Dienstleisters auf das „Need-to-know-Prinzip“ bzw. der dadurch bewirkte Apell zusätzlichen tatsächlichen Schutz.

Daneben trägt sie auch zum strafrechtlichen Schutz des WP/vBP bei, weil nach der eindeutigen Positionierung in der Gesetzesbegründung zum Berufsgeheimnisschutzgesetz die Einhaltung der Regeln der WPO zum Geheimnisschutz eine Strafbarkeit bereits wegen fehlender Unbefugtheit (§ 203 Abs. 1 am Anfang StGB) einer Offenbarung ausschließt.

6.1.5. Anwendungsfall Cloud

Die Inanspruchnahme von Cloud-Diensten richtet sich nach den vorstehend dargelegten allgemeinen berufsrechtlichen Anforderungen und stellt insofern keinen Sonderfall dar. Besonderheiten müssen beachtet werden, wenn sie – wie häufig – im Ausland erbracht werden; insofern kann ergänzend auf die – inhaltlich auch von der WPK geteilte – *IDW Auslegungshilfe zur „Inanspruchnahme ausländischer Dienstleistungen gemäß § 50a Abs. 4 WPO“* verwiesen werden (vgl. Abschn. 4.2.5.).

6.2. Beauftragung sonstiger Dienstleistungen

6.2.1. Aktenauslagerung und Aktenvernichtung

Bei Lichte betrachtet, wird sich die Möglichkeit der Kenntnisnahme von Mandatsgeheimnissen bei der Übergabe von materialisierten (Papier-)Akten an einen Dritten nicht ausschließen lassen. Gleichwohl wird man dem Need-to-know-Prinzip hier insoweit Rechnung tragen können, als dass der unbemerkte unzulässige Zugriff auf die konkreten Akteninhalte jedenfalls erschwert werden kann. Hierzu bietet es sich an, die jeweiligen Akten in verschlossenen, sichtgeschützten Behältnissen zu übergeben oder einzelne Akten mit einem Aufkleber zu „versiegeln“, sodass jedenfalls die „Hemmschwelle“ für eine unbefugte Einsichtnahme erhöht wird.

Ob solche und weitere Maßnahmen ergriffen werden sollten, kann sich daran bemessen, welche Aufgaben der WP/vBP dem Dienstleister überträgt. Soll der Dienstleister nur die Lagerung der Akten vornehmen und verbleibt die Listenführung über die archivierten Akten beim WP/vBP, sollten die Informationen auf dem Aktenrücken – da sie selbst ebenfalls bereits geschützte Daten darstellen – ausschließlich in anonymisierter Form (mittels Strichcode o.ä.) aufgenommen werden, um dem Need-to-know-Prinzip zu genügen. Die sog. chaotische Lagerhaltung beim Dienstleister mag eine weitere Hemmschwelle für eine unbefugte Einsichtnahme bewirken und deshalb hilfreich, im Ergebnis allerdings für den WP/vBP kein strafrechtlich oder berufsrechtlich zwingendes Erfordernis sein. Soll der Dienstleister dagegen auch die Listenführung übernehmen, ist eine Kenntnis der grundsätzlichen Inhalte für die Leistungserbringung erforderlich. Auch hier kann es sich aus übergeordneten Sicherheitsaspekten heraus anbieten, die Aktenrücken nur mit anonymisierten Daten zu versehen und eine chaotische Lagerhaltung vorzusehen; eine straf- oder berufsrechtliche Verpflichtung hierzu besteht aber wiederum nicht.

6.2.2. Klassische Bürohilfsdienste (Telefondienstleister, Schreibservice)

Bei Telefondienstleistern wird nach Art des jeweils in Anspruch genommenen Dienstes zu differenzieren sein. Geht es um die bloße Anrufentgegennahme bzw. die Notierung von Rückrufbitten, wird zu verlangen sein, dass der WP/vBP schon in der Leistungsbeschreibung für den betreffenden Auftrag die zu erbringende Leistung ausdrücklich auf das Vorgenannte beschränkt; zu ergänzen ist dieses natürlich – wie auch bei sämtlichen anderen in Anspruch genommenen

Dienstleistungen – um eine entsprechende Verpflichtung des Telefondienstleisters. Darüberhinausgehende tatsächliche Beschränkungen werden dem WP/vBP nicht möglich sein, da sie sich naturgemäß seiner Eingriffsmöglichkeit entziehen. Dies gilt auch für die Inanspruchnahme von Schreibdiensten. Würde man hier vom WP/vBP verlangen, das Diktierte selbst, also dessen Inhalt im diktierten Text, zu anonymisieren, würde eine ordnungsgemäße Vertragserfüllung kaum möglich sein bzw. deren Zweck vereitelt, sodass man hier allenfalls eine äußerliche Anonymisierung bei der Verbringung von Diktaten zum Schreibdienst wird verlangen können.

6.3. Praxisfälle der unmittelbaren Mitwirkung am Mandat [vgl. auch Abschn. 4.2.6.]

Für Dienstleistungen, die unmittelbar einem einzelnen Mandat dienen, darf dem Dienstleister der Zugang zu den betreffenden fallbezogenen Mandantendaten nur mit Einwilligung des Mandanten eröffnet werden (§ 50a Abs. 5 WPO). Allerdings wird der Anwendungsbereich des § 50a Abs. 5 WPO insofern als begrenzt anzusehen sein, als Dienstleistungen, die allgemeine Fragen der Praxisorganisation betreffen, keiner Einwilligung bedürfen (vgl. Abschn. 4.2.6. und WPK-Praxishinweis „Mitwirkung Dritter an der Berufsausübung (§§ 50, 50a WPO)“, Stand: 26.07.2018).

Beispiele für derartige Dienstleistungen, für die kein „besonderer Bedarf im einzelnen Mandat besteht“ und die typischerweise auch von Shared Service Centern erbracht werden können, sind:

- Auslagerung der Honorarabrechnung
- Einholung von Saldenbestätigungen für eine Vielzahl von Mandaten (vgl. Abschn. 4.2.6.2.)
- Erstellen/Überarbeiten von Standard-Präsentationen
- Druckerei
- (Cyber) Security Services
- Telefondienst/Telefonzentrale
- Aktenarchivierung und -vernichtung.

7. Technische und organisatorische Maßnahmen bei dem Dienstleistungsunternehmen

Je nach Art und Umfang der technisch realisierbaren Sicherungsmaßnahmen beim (Cloud-) Dienstleister sind die organisatorischen Sicherungsmaßnahmen durch diesen und die auslagernde WP/vBP-Praxis auszugestalten. Dabei gilt, dass die organisatorischen Sicherungsmaßnahmen der WP/vBP-Praxis und des Dienstleisters umso umfassender sein müssen, je höher das Risiko eines unberechtigten Zugriffs auf die vertraulichen Informationen ist. Dabei müssen die technischen und organisatorischen Maßnahmen in einem angemessenen Verhältnis zu den identifizierten Risiken stehen (Skalierung), vgl. Abschn. 5.

Mit technischen Maßnahmen sind alle Vorkehrungen gemeint, die sich bspw. auf den Vorgang der Datenverarbeitung erstrecken, wie z.B. das Wegschließen von Datenträgern, bauliche Maßnahmen, die den Zutritt Unbefugter verhindern sollen, oder Steuerungen des Software- oder Hardwareprozesses der Verarbeitung, wie etwa Zugriffs- oder Weitergabekontrolle durch z.B. Verschlüsselungen oder Passwortsicherung. Weitere Maßnahmen können u.a. sein: Pseudonymisierung, Anonymisierung, Datenaggregation, Datensynthese, Nutzerauthentifizierung.

Organisatorische Maßnahmen richten sich auf die äußeren Rahmenbedingungen zur Gestaltung des technischen Verarbeitungsprozesses, wie z.B. Vier-Augen-Prinzip, Protokollierung von Tätigkeiten und Stichprobenroutinen oder aber auch Mitarbeiterschulungen.

Durch organisatorische Maßnahmen hat das Dienstleistungsunternehmen zu gewährleisten, dass die straf- und berufsrechtlichen Anforderungen, die unmittelbar an die WP/vBP-Praxis gestellt werden, erfüllt werden, soweit dies in den Herrschaftsbereich des Dienstleisters fällt. Zu diesem Zweck hat das Dienstleistungsunternehmen ein diesbezüglich angemessenes und wirksam ausgestaltetes IKS einzurichten.

Verantwortlichkeiten, auch in Bezug auf die Einrichtung eines angemessenen, ggf. übergreifenden IKS zwischen der auslagernden WP/vBP-Praxis und dem Dienstleistungsunternehmen sind eindeutig und lückenlos festzulegen, zu dokumentieren und in der IT-Infrastruktur, den IT-Anwendungen und den IT-gestützten Geschäftsprozessen abzubilden.

Insbesondere im laufenden Betrieb ist die Einhaltung der organisatorischen Sicherungsmaßnahmen innerhalb der Aufbau- und Ablauforganisation des Dienstleisters laufend zu gewährleisten.

Wenn die WP/vBP-Praxis einen Datenschutzbeauftragten oder Informationssicherheitsbeauftragten hat, empfiehlt es sich, ihn regelmäßig in die Prüfung bzw. das Audit des Dienstleisters einzubeziehen.

Neben organisatorischen Anforderungen an das IKS des Dienstleistungsunternehmens zur Gewährleistung der Einhaltung der straf- und berufsrechtlichen Vorgaben werden technische Maßnahmen durch den Dienstleister zu ergreifen sein. Dabei lassen sich Anforderungen an den Dienstleister aus etablierten Rahmenwerken wie dem C5-Katalog des BSI, *IDW RS FAIT 1* oder ISE/IEC 27001 ableiten. Hiernach können bspw. folgende technische Anforderungen genannt werden:

- Absicherung der Kommunikation zwischen der WP/vBP-Praxis und dem Dienstleistungsunternehmen
- Absicherung des Datenaustauschs (VPN)

- Verschlüsselung der E-Mail-Kommunikation (Secure Socket Layer (SSL)/Transport Layer Security (TLS)/Transportverschlüsselung; Pretty Good Privacy (PGP)/Multipurpose Internet Mail Extensions (MIME)/Ende-zu-Ende-Verschlüsselung; elektronische Signatur)
- Härtung von weiteren Kommunikationswegen (z.B. Telefonie)
- Verschlüsselung der Inanspruchnahme von Web-Applikationen (Hypertext Transfer Protocol Secure (https))
- Sichere IT-Systeme des Dienstleistungsunternehmens
- gehärtete Betriebssysteme mit automatisiertem Patch-Service
- Intrusion-Detection-Systeme (IDS)/Security Operation Centre (SOC)
- Datei-Integrität-Prüfungssysteme
- Syslog- und Timeserver
- kaskadierte Firewall-Systeme
- physische Sicherungsmaßnahmen in Rechenzentren (z.B. Zugangskontrollen, Vier-Augen-Prinzip)
- Verschlüsselung gespeicherter Daten
- Berechtigungskonzept für die Administration der IT-Systeme des Cloud-Dienstleisters
- Löschung von Daten nach Nutzungsbeendigung.

Die an den Dienstleister zu stellenden Anforderungen sind entsprechend den tatsächlichen Verhältnissen im Einzelfall angemessen auszugestalten. So mag bspw. die Verschlüsselung von beim Dienstleister gespeicherten Daten sinnvoll erscheinen, sofern diese nicht in Verarbeitungsprozesse einbezogen werden, sondern ausschließlich für Zwecke der Archivierung (Datenspeicherung) ausgelagert wurden (z.B. Inanspruchnahme von Festplattenkapazitäten im Rahmen einer IaaS-Strategie); vgl. auch Abschn. 6.1.1. Hingegen ist bei der Inanspruchnahme von SaaS-Dienstleistungen mitunter eine Verschlüsselung von Daten auszuschließen, sofern diese sodann einer Verarbeitung nicht mehr zugänglich wären.

Auf Ebene der Netzwerkumgebung sind vertrauenswürdige Netzwerke (z.B. im Rahmen einer Private Cloud) von nicht vertrauenswürdigen Netzwerken (z.B. im Rahmen einer Public Cloud) sicher und zuverlässig zu trennen. Dabei ist zu beachten, dass der Zugriff auf Netzwerke zur Verwaltung der Dienstleistung getrennt von den übrigen Zugriffen erfolgt.

Sofern administrative und privilegierte Berechtigungen für die IT-Infrastruktur und die IT-Anwendungen seitens des Dienstleistungsunternehmens zu verwalten und vor unberechtigter Nutzung zu schützen sind – z.B. bei Cloud Computing betrifft dies die Berechtigungen für Hypervisor- und Storage-Systeme –, sollten diese Berechtigungen restriktiv vergeben werden.

Dabei gilt, dass Veränderungen an der IT-Infrastruktur über einen geordneten Veränderungsmanagementprozess durch das Dienstleistungsunternehmen ggf. unter Einbeziehung der auslagernden WP/vBP-Praxis geplant, getestet, umgesetzt und dokumentiert werden sollten. Dabei ist durch die WP/vBP-Praxis zu gewährleisten, dass im Kontext der Infrastrukturänderungen durch diese oder den externen Dienstleister hinreichende Datensicherungen durchgeführt werden.

Sowohl beim Wechsel der Speichermedien zu Wartungszwecken als auch bei Nutzungsbeendigung sollte das auslagernde Unternehmen dafür Sorge tragen, dass vertragsgemäß technische Maßnahmen zur Anwendung kommen, um eine vollständige Löschung von Daten auf allen Speichermedien durch das Dienstleistungsunternehmen zu gewährleisten und eine Wiederherstellung zu verhindern.

Im Bereich des Cloud-Computing haben sich folgende Standard-Zertifizierungen im Zusammenhang mit Informationssicherheit herausgebildet:

- BSI C5
- *IDW PS 860* i.V.m. BSI Grundschutz/ISO 27001
- *IDW PS 860* i.V.m. *IDW RS FAIT 1* und *IDW RS FAIT 5*
- TCDP (Schutz-b/a-Klasse 3).

Auf Basis von BSI Grundschutz unterscheidet BSI C5 folgende technische und organisatorische Anforderungsbereiche[8] den Outsourcing-Dienstleister betreffend:

- Organisation der Informationssicherheit
- Sicherheitsrichtlinien und Arbeitsanweisungen
- Anforderungen an das Personal
- Asset Management
- physische Sicherheit
- Maßnahmen für den Regelbetrieb
- Identitäts- und Berechtigungsmanagement
- Kryptographie und Schlüsselmanagement

[8] Vgl. für detaillierte Ausführungen zu den einzelnen Anforderungsbereichen den Anforderungskatalog, abrufbar im Internet unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CloudComputing/Anforderungskatalog/Anforderungskatalog_Tabellen_bearbeitbares_Format.xls;jsessionid=CD666410A6074E3F34BF8EE57AE9FCC3.2_cid360?__blob=publicationFile&v=3 (Abruf vom 07.02.2019).

- Kommunikationssicherheit
- Portabilität und Interoperabilität
- Beschaffung, Entwicklung und Änderung von Informationssystemen
- Steuerung und Überwachung von Dienstleistern und Lieferanten
- Security Incident Management
- Sicherstellung des Geschäftsbetriebs und Notfallmanagement
- Sicherheitsprüfung und -nachweis
- Compliance und Datenschutz
- Mobile Device Management.

Allerdings muss beachtet werden, dass die vorgenannten Zertifizierungen nicht unmittelbar auf die hier behandelten straf- und berufsrechtlichen Vorgaben ausgerichtet sind. Aufgrund von Art und Umfang der in den jeweiligen Standards erarbeiteten Anforderungen an den Outsourcing-Dienstleister sind jedoch zusätzliche technische und organisatorische Anforderungen aufgrund von straf- und berufsrechtlichen Vorgaben für die WP/vBP-Praxis nicht zu erkennen. Mithin wird die WP/vBP-Praxis bei (regelmäßigem) Vorlegen aktueller Zertifizierungsnachweise (vgl. Abschn. 3.2.) durch das Dienstleistungsunternehmen von der Art und dem Umfang nach angemessenen technischen und organisatorischen Maßnahmen ausgehen können.

Stand: 10.04.2019

Anlage
Anforderungen der WP/vBP-Praxis an die Auslagerung von Funktionen und Prozessen

Ziel des Outsourcings		**Erläuterung**
1	Funktionale Anforderungen	Der Dienstleister übernimmt die (bislang) durch die WP/vBP-Praxis gewährleisteten Funktionen und muss sicherstellen, dass diese (auch künftig) erreicht werden (Funktionsfortführung). Darüber hinaus kann eine Ausweitung von Funktionen und Funktionalitäten angestrebt werden (Funktionsausweitung).
2	Betriebs-Anforderung (vgl. *IDW RS FAIT 1*, Tz. 23)	Im Rahmen z.B. des IT-Outsourcing muss gewährleistet sein, dass die ausgelagerten Funktionen verfügbar sind (Verfügbarkeit), die Integrität gewährleistet wird und die Authentizität der IT-Systeme gegeben ist. Darüber hinaus wird regelmäßig die Gewährleistung der Verbindlichkeit der IT-Systeme gefordert sein.
3	Ökonomische Anforderungen	Durch die Auslagerung sollen ökonomische Ziele, z.B. Kostenreduktion, realisiert werden.
4	Know-how-Anforderungen	Insbesondere technische Dienstleistungen erfordern ein spezielles Know-how, das üblicherweise nicht in WP/vBP-Praxen vorhanden ist. Durch das Outsourcing soll erreicht werden, dass dieses spezifische Know-how nicht mehr in der WP/vBP-Praxis vorgehalten werden muss.
5	Ressourcen-Anforderungen	WP/vBP-Praxen sehen sich sowohl bei Bereithaltung personeller als auch technischer Ressourcen mit erheblichen Herausforderungen konfrontiert. Das Outsourcing kann insoweit auch dazu dienen dem Fachkräftemangel (Knappheit personeller Ressourcen) zu begegnen. Gerade aufgrund der Skalierbarkeit von Cloud-Ressourcen (technische Ressourcen) haben diese gegenüber der internen Vorhaltung von Ressourcen (z.B. Speicherkapazitäten, Rechnerleistung) Vorteile für die auslagernde WP/vBP-Praxis.

6	Innovations-Anforderungen	Aufgrund der berufsfachlichen Ausrichtung von WP/vBP-Praxen liegt deren Innovationsfokus regelmäßig außerhalb technischer Innovationen. Durch die Inanspruchnahme externer Dienstleister können technische Innovationen (z.B. Kommunikationsplattformen) auch durch WP/vBP-Praxen erschlossen werden.
7	Informationssicherheitsanforderungen	Aufgrund der zunehmenden Cyber-Kriminalität und dem zunehmenden IT-Sicherheitsrisiko sehen sich auch WP/vBP-Praxen mit nachhaltig steigenden Sicherheitsanforderungen (technisch und organisatorisch) konfrontiert. Insbesondere aufgrund des finanziellen Aufwands in Kombination mit dem spezifischen Know-how sind mitunter (notwendige/sinnvolle) Lösungen (z.B. Security Operation Center) für die einzelne WP/vBP-Praxis nicht realisierbar. Durch die Inanspruchnahme professionalisierter IT-Sicherheits-Dienstleistungen und die bei ihnen realisierbaren Skaleneffekte kann die IT-Sicherheit signifikant ausgebaut werden.
7a	Anforderung zur Wahrung von Geschäftsgeheimnissen der WP/vBP-Praxis (z.B. Know-how, Templates, eigene Geschäftsdaten) sowie der Unternehmensfortführung (z.B. Vermeidung von Einschränkung der Verfügbarkeit, Integrität, Authentizität sowie der Verbindlichkeit aufgrund unberechtigter Zugriffe)	Aus ökonomischen Gründen (z.B. Wahrung von Wettbewerbsvorteilen, USP) werden WP/vBP-Praxen die Anforderung haben, dass eigene Geschäftsgeheimnisse vor dem Zugriff unberechtigter Dritter geschützt werden.
7b	Straf-/berufsrechtliche Anforderungen (Geheimniswahrung)	Auch im Rahmen des Outsourcings sind die straf- und berufsrechtlichen Vorgaben, insb. die Kenntnisnahme ausschließlich berechtigter Personen, zu wahren. Hier besteht ein gewisser Trade-off mit den vorgenannten Zielen.

7c	Datenschutzrechtliche Anforderungen	Ebenso sind die datenschutzrechtlichen Vorgaben (BDSG, DS-GVO) auch im Rahmen des Outsourcings zu gewährleisten. In diesem Zusammenhang ist ebenfalls ein Trade-off im vorgenannten Sinne zu verzeichnen.

Anlage zu Abschn. 5. *Technische/organisatorische Maßnahmen in der WP/vBP-Praxis*

Um auf die in Abschn. 5. beschriebenen Gefährdungslagen zu reagieren, müssen im Rahmen des Outsourcing-Projekts die technischen Anforderungen beachtet werden. Nach BSI Grundschutz können im Falle von IT-Outsourcing-Projekten folgende Phasen eines Outsourcing-Vorhabens unterschieden werden:

Phase 1: Strategische Planung des Outsourcing-Vorhabens

Bereits im Rahmen der strategischen Entscheidungsfindung sind sicherheitsrelevante Gesichtspunkte herauszuarbeiten. Insbesondere hat die WP/vBP-Praxis eine Erhebung der Schutzbedarfe aufgrund der Erhebung der Risiken durch das QSS durchzuführen. Konkret sind folgende qualitätssichernde Handlungen in Phase 1 vorzunehmen:

- Abgrenzung der auszulagernden Funktionen
- Abgrenzung der damit verbundenen Bestandteile des IT-Systems
- Aufnahme der technischen Bestandsmaßnahmen des betroffenen IT-Systems, insb. der IT-Infrastruktur und der IT-Anwendungen
- Aufnahme der inhärenten Risiken des geplanten Outsourcings, wie bspw. potentielle (technische) Sicherheitslücken, Bedrohung durch Malware
- Aufnahme der damit verbundenen technischen Maßnahmen in der WP/vBP-Praxis und bei dem Dienstleister zur Gewährleistung der gesetzlichen Anforderungen an die Geheimniswahrung (Kontrollrisiken und Kontrollmaßnahmen), wie bspw. technische IT-Sicherheitsmaßnahmen (IT-Sicherheitskonzept) sowie technische Maßnahmen zur Sicherung der Verfügbarkeit des IT-Systems.

Phase 2: Definition der wesentlichen (Sicherheits-)Anforderungen (Pflichten-/Lastenheft)

Auf der Grundlage der Analyse in Phase 1 sind sodann technische Maßnahmen zu definieren, die den identifizierten Bedarfen Rechnung tragen und die mit dem Outsourcing-Dienstleister zu vereinbaren sind. Art und Umfang der zu stellenden Sicherheitsanforderungen sind dabei in Bezug auf den Einzelfall mit dem Dienstleister zu vereinbaren. Weder ist es sinnvoll noch notwendig, in allen Fällen gleichgelagerte Sicherheitsanforderungen zu stellen. Unangemessen hohe

Sicherheitsanforderungen werden prohibitiv auf die Durchführung von Outsourcing-Projekten wirken. Mithin gilt bei der Ableitung der Anforderungen in einem Pflichten-/Lastenheft:

- hinreichende Definition der zu übernehmenden Funktionen
- hinreichende Definition der geforderten technischen Kontrollmaßnahmen als angemessene Reaktion auf identifizierte inhärente Risiken gemäß Phase 1
- Darstellung der geforderten Kontrollrechte durch die auslagernde WP/vBP-Praxis bzw. alternativer Nachweis, z.B. anhand von Zertifizierungen.

Auf Seiten der WP/vBP-Praxis sind folgende technische Sicherungsmaßnahmen denkbar:

- physische Sicherungsmaßnahmen in lokalen IT-Ressourcen (z.B. Zugangskontrollen Serverraum)
- lokales IT-System (z.B. Betriebssystem sog. Fat-Clients)
- gehärtete Betriebssysteme mit automatisiertem Patch-Service
- Datei-Integrität-Prüfungssysteme
- Härtung von lokalen Kommunikationswegen (z.B. Telefonie)
- Verschlüsselung lokal gespeicherter Daten
- Berechtigungskonzept für die Administration der IT-Systeme der WP/vBP-Praxis
- Mobile Device Management.

Bei den durch die WP/vBP-Praxis zu ergreifenden Sicherheitsmaßnahmen ist immer die Kompatibilität zu den IT-Systemen des (noch auszuwählenden) Cloud-Dienstleisters zu beachten und vor Abschluss der Phase 3 zu untersuchen.

Phase 3: Auswahl des Outsourcing-Dienstleisters

Der Auswahl des Outsourcing-Dienstleisters kommt eine besondere Bedeutung zu. Insbesondere ist die Fähigkeit zur Einhaltung der gestellten Sicherheitsanforderungen zu prüfen durch den Abgleich der Angebote der Dienstleister mit den Anforderungen gemäß Pflichten-/Lastenheft. In diesem Zusammenhang sind auch Kontrolllücken beim Dienstleister abzuleiten und die Klärung der Schließung dieser zu gewährleisten.

Mithin kommt es zur Auswahl eines Dienstleisters oder zur Verwerfung des Outsourcing-Projekts.

Phase 4: Vertragsgestaltung

Auf Basis des erarbeiteten Pflichtenheftes ist ein Vertrag mit dem Outsourcing-Dienstleister auszuhandeln (Service Level Agreements/SLA).

Die SLA umfassen auch die genauen Modalitäten der Zusammenarbeit wie bspw. die Benennung der Ansprechpartner des Dienstleisters, die Abgrenzung der Reaktionszeiten, die Definition der IT-Anbindung, die Möglichkeiten der Kontrolle der Outsourcing-Leistungen, die Prüfung der Ausgestaltung der Sicherheitsvorkehrungen, die Behandlung vertraulicher Informationen, den Ausschluss von Verwertungsrechten sowie das Verbot der unerlaubten Weitergabe von Information an Dritte. Insbesondere ist aber durch die WP/vBP-Praxis die vertragliche Vereinbarung der Vorgaben nach §§ 203 StGB, 50a WPO (vgl. Abschn. 4.2.4.) zu gewährleisten.

Phase 5: Erstellung eines Sicherheitskonzepts für den ausgelagerten Informationsverbund

Die WP/vBP-Praxis und der Outsourcing-Dienstleister müssen gemeinsam in Phase 5 ein detailliertes Sicherheitskonzept erstellen, das auch ein Notfallvorsorgekonzept umfasst.

Dabei ist zu berücksichtigen, dass Phase 5 regelmäßig erst nach der erfolgreichen Migration abgeschlossen werden kann, da während der Migration der IT-Systeme und Anwendungen ergänzende und neue Erkenntnisse zu verzeichnen sein werden, die ebenfalls in das Sicherheitskonzept einzuarbeiten sind.

Phase 6: Migrationsphase

Während der Migrationsphase sind auf Seiten der WP/vBP-Praxis folgende Maßnahmen zu ergreifen, um den Sicherheitsanforderungen gerecht zu werden:

- Gewährleistung der Existenz, Implementierung und Wirksamkeit eines Sicherheitskonzepts für die Migrationsphase
- ausschließliche Verwendung von Testdaten für Migrationstests
- Gewährleistung einer hinreichenden fachlichen Vorbereitung der Mitarbeiter des Auftraggebers sowie Schaffung hinreichender zeitlicher Freiräume.

Auch für die im Rahmen der Migrationsplanung vereinbarten Migrationsschritte ist die Vertraulichkeit der Informationen zu gewährleisten (z.B. Verwendung ausschließlich verschlüsselter Kommunikationswege im Rahmen des Datentransports).

Phase 7: Planung und Sicherstellen des laufenden Betriebs

Sobald die Cloud-Services implementiert wurden bzw. der Outsourcing-Dienstleister die Geschäftsprozesse übernommen hat, ist im Regelbetrieb die Funktionsfähigkeit der getroffenen technischen Maßnahmen regelmäßig zu überprüfen. Dazu gehört insb. auch die permanente Prüfung der Aktualität der bei Projektbeginn beschlossenen technischen und organisatorischen Maßnahmen. Nicht zuletzt die erhebliche Änderungsgeschwindigkeit informationstechnischer Installationen (siehe hierzu bspw. Moore’s Law) macht dies zwingend erforderlich. Sofern ein unmittelbarer Nachweis bei dem IT-Dienstleister nicht möglich ist und die WP/vBP-Praxis daher

auf Zertifikate und andere Signale zurückgreifen musste, sind die betreffenden Nachweise regelmäßig, üblicherweise einmal jährlich, oder bei Bekanntwerden entsprechender Anlässe erneut bei dem Dienstleister anzufordern. Sollten die entsprechenden Nachweise nicht erbracht werden können, hat die WP/vBP-Praxis im Zweifel eine Beendigung des Outsourcing-Vertrags zu prüfen.