Christoph Schäfer, Dirk Fox

Zertifizierte Auftragsdatenverarbeitung

Das Standard-ADV-Modell

Wie lassen sich Auftragsdatenverarbeiter systematisch und kontinuierlich, zugleich aber effizient und effektiv auf die wirksame Umsetzung geeigneter organisatorischer und technischer Maßnahmen zum Schutz der verarbeiteten personenbezogenen Daten prüfen? Vielleicht haben Sie sich diese Frage selbst bereits gestellt. Denn wenn personenbezogene Daten im Auftrag verarbeitet werden, liegt die Verantwortung für die Verarbeitung beim Auftraggeber: Er muss regelmäßig prüfen, ob geeignete Maßnahmen zu deren Schutz getroffen wurden und die gesetzlichen Anforderungen erfüllt sind. Eine Zertifizierung kann aufwändige Einzelprüfungen durch ein standardisiertes Verfahren ersetzen.

1 Die Ausgangslage

Werden personenbezogene Daten von Kunden, Lieferanten, Interessenten oder Beschäftigten eines Unternehmens (Auftraggeber) durch einen Dienstleister (Auftragnehmer) erhoben oder verarbeitet, handelt es sich meist um eine Auftragsdatenverarbeitung (ADV) gemäß § 11 Bundesdatenschutzgesetz (BDSG) bzw. anderer Datenschutzvorschriften.

Das Besondere der Auftragsdatenverarbeitung ist, dass sie eine gesetzliche Fiktion darstellt. Der Auftragnehmer ist eigentlich Dritter; damit würde eine Verarbeitung personenbezogener Daten des Auftraggebers eine erlaubnispflichtige Übermittlung i. S. d. § 3 Abs. 3 Nr. 3 BDSG darstellen. Durch das Konstrukt der ADV entfällt die – unter Umständen komplizierte und bisweilen schwer zu begründende – Suche nach einer Rechtsgrundlage.

Christoph Schäfer

Security Consultant bei der Secorvo Security Consulting GmbH, zertifizierter betrieblicher Datenschutzbeauftragter (GDDcert.), Beratungsschwerpunkte: Datenschutz und Datensicherheit.
E-Mail: christoph.schaefer@secorvo.de

Dirk Fox

Geschäftsführer der Secorvo Security Consulting GmbH und Herausgeber der DuD.

E-Mail: dirk.fox@secorvo.de

Im Falle einer Auftragsdatenverarbeitung ist der Auftraggeber verpflichtet, seinen Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen (§ 11 Abs. 2 BDSG). Zudem muss er sich in der Folge regelmäßig von der Einhaltung dieser Maßnahmen überzeugen und die Ergebnisse dokumentieren. Auftragnehmer von Auftragsdatenverarbeitungen müssen umgekehrt ihren Auftraggebern regelmäßig und wiederholt die Einhaltung der von ihnen getroffenen technischen und organisatorischen Maßnahmen nachweisen.

2 Vorgaben des BDSG

§ 11 BDSG regelt die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag. Dabei ist es unerheblich, ob die Daten innerhalb eines Unternehmensverbunds bzw. Konzerns weitergegeben werden oder beispielsweise im Rahmen eines Projektes mit einem externen Dienstleister zusammengearbeitet wird. Wesentlich ist, dass die Daten durch einen Dritten – also weder den Betroffenen noch die verantwortliche Stelle – verarbeitet werden.

Sollen externe Dienstleister oder Konzerngesellschaften personenbezogene Daten im Auftrag verarbeiten, muss hierzu ein schriftlicher Vertrag geschlossen werden – eine im deutschen Recht seltene gesetzliche Beschränkung der Vertragsfreiheit. Der Auftraggeber wird dabei explizit in die Pflicht genommen. Er bleibt verantwortliche Stelle und trägt damit zunächst die alleinige Verantwortung für die korrekte Datenverarbeitung, auch wenn er die Verarbeitung an sich mit der ADV an ein anderes Unternehmen vergibt.

§ 11 Abs. 2 BDSG macht detaillierte Vorgaben dazu, welche Aspekte in einer Vereinbarung zur Auftragsdatenverarbeitung schriftlich geregelt werden müssen. Die verantwortliche Stelle, also der Auftraggeber, ist zunächst verpflichtet zu prüfen, ob der

Auftragnehmer den Auftrag überhaupt ordnungsgemäß ausführen kann. Dann sind schriftlich festzuhalten:

- der Gegenstand und die Dauer des Auftrags, der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,
- die zu treffenden technischen und organisatorischen Maßnahmen,
- die Berichtigung, Löschung und Sperrung von Daten,
- die Pflichten des Auftragnehmers (Datengeheimnis, Stellung eines Datenschutzbeauftragten, Auskunftspflicht, Sanktionierung unbefugter Datenerhebung aus nicht allgemein zugänglichen Quellen und deren Verwendung, Sanktionierung solcher Daten bei Bereithaltung zum Abruf mittels automatisierter Verfahren, Sanktionierung bei Abruf oder Verschaffung einem Dritten aus automatisierten Verarbeitungen oder nicht automatisierten Dateien),
- die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,
- die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,
- mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,
- der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält und
- die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

Die Grenzen zwischen einer Verarbeitung der Daten im Auftrag und einer sogenannten „Funktionsübertragung" (datenschutzrechtlich eine Übermittlung), bei denen sich die rechtliche Zuständigkeit über die Datenbestände ändert, sind eng und oftmals nicht unumstritten. Daher muss eine Einzelfallbetrachtung erfolgen, ob es sich tatsächlich um eine Auftragsdatenverarbeitung handelt oder nicht. Als wichtigstes Abgrenzungskriterium wird in der Literatur die Entscheidungsbefugnis über die Daten aufgeführt. Mit der Änderung des BDSG vom 05.02.2009 hat der Gesetzgeber klargestellt, dass Fernwartungen („Prüfung oder Wartung automatisierter Verfahren") in jedem Fall als ADV zu verstehen sind, sofern ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann (§ 11 Abs. 5).

Unerheblich ist hingegen, in welcher Rechtsform ein Auftragsverhältnis begründet wird. In Betracht kommen sämtliche im BGB geregelten Rechtsgeschäfte (Dienstverträge, Werkverträge, Geschäftsbesorgungsverträge), aber auch verschiedene Formen der Zusammenarbeit, beispielsweise auf Konzernebene.

Werden personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt, so ist stets der Auftraggeber für die Einhaltung der Vorschriften des Bundesdatenschutzgesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Das Recht des Betroffenen auf Auskunft über die Speicherung seiner personenbezogenen Daten (§ 34 BDSG) und etwaige Schadensersatzansprüche bei missbräuchlichem Umgang mit seinen Daten richten sich dabei stets an den Auftraggeber.

Der Auftragnehmer darf die Daten nur im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen. Ist er der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Vorgaben verstößt, muss er den Auftraggeber unverzüglich darauf hinweisen.

3 Änderungen durch die EU-DS-GVO

Mit der EU-Datenschutz-Grundverordnung (EU-DS-GVO) wird die Auftragsdatenverarbeitung ab Mai 2018 europaweit einheitlich geregelt. Diese Neuregelung entspricht weitgehend der deutschen Regelung in § 11 BDSG. Einige Änderungen gilt es dennoch zu beachten.

3.1 Allgemeine Änderungen

Die bekannten Begriffe des Auftraggebers und des Auftragsdatenverarbeiters werden durch den „für die Verarbeitung Verantwortlichen" und den „Auftragsverarbeiter" ersetzt (Art. 28 EU-DS-GVO). Auch kann es künftig gemeinsam für die Verarbeitung Verantwortliche („Joint Controllership") als Auftraggeber geben. Diese legen sodann gemeinsam die Zwecke und Mittel zur Verarbeitung personenbezogener Daten fest und sind gemeinsam für die Einhaltung der Datenschutzbestimmungen verantwortlich (Art. 26 EU-DS-GVO).

Das Schriftformerfordernis für den Vertag wird durch die elektronische Form ergänzt (Art. 28 Abs. 9 EU-DS-GVO). Zudem können Auftragsverarbeitungen künftig auch außerhalb der Europäischen Union stattfinden, „soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines für die Verarbeitung Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt" (Art. 3 Abs. 1 EU-DS-GVO).

Im Gegensatz zur bisherigen maßgeblichen Haftung des Auftraggebers haften der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter gegenüber dem Betroffenen künftig gemeinsam. Der Auftragsverarbeiter haftet jedoch nur für die von ihm zu erfüllenden Pflichten – dem Inhalt des Vertrages mit dem Auftragsverarbeiter kommt damit eine weitere wichtige Bedeutung zu.

Unabhängig vom Inhalt des Vertrages muss der Auftragsverarbeiter künftig selbst ein Verfahrensverzeichnis führen (Art. 30 Abs. 2 DSGVO) – bisher wurde die Verantwortung hierfür regelmäßig ausschließlich beim Auftraggeber gesehen.

Bei Verstößen im Rahmen der Auftragsverarbeitung drohen dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter – viel diskutierte – Geldbußen in Höhe von bis zu 10 Millionen Euro oder 2% des gesamten weltweit erzielten Jahresumsatzes, je nachdem welcher Betrag der höhere ist (Art. 83 EU-DS-GVO).

3.2 Schwerpunkt auf Zertifizierungen

Eine besondere Bedeutung kommt der Zertifizierung zu. Die EU-Datenschutz-Grundverordnung widmet ihr einen eigenen Artikel: „Die Mitgliedstaaten, die Aufsichtsbehörden, der Ausschuss und die Kommission fördern insbesondere auf Unionsebene die Einführung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und -prüfzeichen, die dazu dienen, nachzuweisen, dass diese Verordnung bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird. Den besonderen Bedürfnissen von Kleinstunterneh-

men sowie kleinen und mittleren Unternehmen wird Rechnung getragen." (Art. 42 EU-DS-GVO).

4 Nutzen einer Zertifizierung

Seit der Verschärfung der Vorgaben für die Auftragsdatenverarbeitung mit der letzten großen BDSG-Novelle hat das Thema viel Aufmerksamkeit erfahren. Auftragsdatenverarbeiter und ihre datenschutzrechtliche Kontrolle rücken immer mehr in den Fokus. Dabei ist der Trend zum Outsourcing ungebrochen.

Bei allen Beteiligten – Auftraggeber wie Auftragnehmer – verursacht die pflichtmäßige Kontrolle von Auftragsdatenverarbeitungen hohen Aufwand. Der Datenschutzbeauftragte des Auftraggebers muss überlegen, wann er welchen Dienstleister kontrolliert und die personellen und zeitlichen Ressourcen für die Kontrolle zur Verfügung stellen. Umgekehrt sieht sich der Auftragnehmer oft mit Kontrollen vieler verschiedener Auftraggeber konfrontiert, die zwar inhaltlich Ähnliches, aber nicht gemeinsam prüfen. Jede Prüfung bindet auch bei ihm erhebliche personelle und zeitliche Ressourcen.

Gerade bei einer standardisierten Dienstleistung liegt es nahe, diese Prüfungen durch einen vertrauenswürdigen Dritten durchführen zu lassen. Dies spart für alle Beteiligten der Auftragsdatenverarbeitung erhebliche Aufwände und sorgt zugleich für eine einheitliche Systematik und ein standardisiertes Prüfniveau. Entsprechend wurden in den vergangenen Jahren verschiedene Angebote für Prüfungen oder Zertifizierungen von Auftragsdatenverarbeitungen entwickelt und angeboten.[1] Gleichwohl hat sich bisher keine Lösung durchsetzen können, da jede ihre eigenen Vor- und Nachteile besitzt.

Dabei hat die Zertifizierung einer Auftragsdatenverarbeitung klare Vorteile:

- Sie belegt gegenüber dem Auftraggeber, dass geeignete Maßnahmen zum Schutz der verarbeiteten personenbezogenen Daten getroffen und wirksam umgesetzt wurden.
- Sie kann dem Auftraggeber von der Aufgabe befreien, eigene Prüfungen nach § 11 BDSG durchzuführen und
- Sie ist gleichzeitig ein wertvolles Qualitätsmerkmal für den Auftragsverarbeiter.

5 Das Standard-ADV-Modell

Doch warum hat sich bisher kein Standard etabliert? Genau mit dieser Frage haben wir uns gemeinsam mit der TÜV SÜD IT-Sec GmbH (als erfahrenem Zertifizierer) beschäftigt. Daraus ist ein Standard-ADV-Modell mit Zertifizierung entstanden, das Auftragnehmer von Auftragsdatenverarbeitungen beim Nachweis der Eignung und Angemessenheit der getroffenen technischen und organisatorischen Maßnahmen gegenüber ihren Auftraggebern mit dem Prüfzeichen und Zertifikat „Zertifizierte Auftragsdatenverarbeitung" unterstützt.

Grundlage zur Prüfung und Bewertung der Auftragsdatenverarbeitungen ist ein Anforderungskatalog des TÜV SÜD zur Bewertung und Zertifizierung von Auftragnehmern von Auftragsdatenverarbeitungen.[2] Er beinhaltet Anforderungen aus den Bereichen

- Leistungs- und auftragsbezogene Dokumentation
- Allgemeine Maßnahmen zum Datenschutz
- Technische und organisatorische Maßnahmen zum Datenschutz

Herausfordernd sind jedoch die exakte Festlegung und Abgrenzung des Prüfgegenstands sowie die Wahl geeigneter Soll-Vorgaben.

5.1 Definition des ADV-Gegenstands

Bei der Zertifizierung einer Auftragsdatenverarbeitung ist die Definition des Zertifizierungs-Gegenstands von zentraler Bedeutung. Es muss klar sein, was genau Gegenstand der Zertifizierung und somit Prüfung der Auftragsdatenverarbeitung ist. Allzu oft wird hierbei unsauber vorgegangen. Das führt bei Zertifizierungen dazu, dass der Aufwand unnötig in die Höhe getrieben wird – oder aber für die ADV wesentliche Prozesse nicht berücksichtigt werden.

Ist beispielsweise das Durchführen von Anrufaktionen durch ein Call-Center Gegenstand der Auftragsdatenverarbeitung, müssen alle, (aber auch nur die) dafür relevanten Prozesse betrachtet werden. In diesem Fall ist der Beschäftigtendatenschutz des Auftragnehmers für die Auftragsdatenverarbeitung irrelevant. Streng genommen ist nicht einmal zu prüfen, ob beim Dienstleister ein Datenschutzbeauftragter bestellt wurde, denn verantwortliche Stelle für die Auftragsdatenverarbeitung (Call-Center-Aktivität) ist und bleibt der Auftraggeber.

5.2 Soll- und Ist-Abgleich

Bei der Prüfung und Bewertung einer Auftragsdatenverarbeitung müssen inhaltlich sowohl rechtliche als auch technisch-organisatorische Aspekte geprüft werden. Dabei ist jeweils die tatsächliche Realisierung und konkrete Umsetzung, der Ist-Zustand, mit einer Soll-Vorgabe (einem Referenz-Zustand) abzugleichen.

Kleine und mittelständische Unternehmen haben in Bezug auf ihre Datenschutz- und IT-Sicherheits-Organisation oft eines gemeinsam: Der Ist-Zustand (mit mehr oder weniger hoher Qualität) wurde „nach bestem Wissen und Gewissen" umgesetzt. Gegen welche Soll-Vorgabe ist dieser Zustand jedoch zu prüfen? Ist kein Referenz-Zustand definiert, treffen in der Praxis bei einer Prüfung die Lebenserfahrung der IT-Abteilung und die des Prüfers aufeinander – und im Zweifel muss sich erstere letzterer beugen. Vergleichbar oder wiederholbar wird ein Prüfergebnis dadurch jedoch nicht: der nächste Prüfer wird mit einer anderen Lebenserfahrung gegen abweichende „Soll-Werte" prüfen.

Daher muss für ein standardisiertes Prüfverfahren zunächst eine geeignete Soll-Vorgabe festgelegt werden. Das ist allerdings keine einfache Aufgabe: Denn je nach ADV-Dienstleistung kann ein bestimmter Schutzmechanismus – wie z. B. eine Ausweiskontrolle – oder eine Festplattenverschlüsselung angemessen sein, oder aber auch nicht.

Auch der Verweis auf einen (wie auch immer definierten) „Stand der Technik" hilft hier nicht weiter, denn der existiert nicht als einheitliche Vorgabe, und er beantwortet auch nicht die

1 Siehe z.B. http://www.dsz-audit.de

2 Siehe http://www.tuev-sued.de/fokus-themen/it-security/zertifizierte-auftragsdatenverarbeitung

Frage der Angemessenheit einer Maßnahme für eine spezifische Dienstleistung.

Die Lösung ist so einfach wie bestechend: Soll-Vorgabe der zu prüfenden technischen und organisatorischen Maßnahmen ist ein Datenschutz- und Datensicherheitskonzept des Auftragsdatenverarbeiters, bestehend aus einer genauen Verfahrensbeschreibung und einer Dokumentation der technischen und organisatorischen Maßnahmen, die der Auftragsdatenverarbeiter zum Schutz der von ihm verarbeiteten personenbezogenen Daten vorgesehen hat. Damit die Auswahl der Maßnahmen nachvollzogen werden kann, genügt hier keine stichwortartige Auflistung: Die Maßnahmen sind so zu beschreiben, das Schutzzweck und Eignung erkennbar sind.

Aber auch die rechtliche Prüfung erfordert eine Soll-Vorgabe. Da das BDSG trotz detaillierter Vorgaben in § 11 Abs. 2 die exakte vertragliche Regelung bestimmter Aspekte offen lässt und die konkrete Umsetzung der vertraglichen Vereinbarungen ebenfalls zu prüfen sind, dient hier eine vom Auftragsdatenverarbeiter vorzulegende Vertragsvorlage als Soll-Vorgabe.

5.3 Vorgehen nach dem Standard-ADV-Modell

Bei der Auditierung nach dem Standard-ADV-Modell erfolgt im ersten Schritt eine klare Abgrenzung des Zertifizierungsgegenstands, nämlich die konkrete Auftragsdatenverarbeitung bei einem Dienstleister (Auftragnehmer). Dabei sind in erster Linie die auftragsspezifischen Aspekte relevant, nicht seine allgemeine (Datenschutz-) Organisation, zumindest soweit sie keine Auswirkungen auf die Auftragstätigkeit hat.

Die eigentliche Prüfung erfolgt dann systematisch in zwei Stufen: Zunächst werden die Soll-Vorgaben in Form des vom Auftragnehmer bereitgestellten (Standard-) Vertrags zur Auftragsdatenverarbeitung (ADV-Vertrag) und dessen Datenschutz- und Datensicherheitskonzept (DDSiKo) bewertet – ersterer auf seine Rechtskonformität, letzterer auf seine Eignung für den Schutz der personenbezogenen Daten bei den in der Verfahrensbeschreibung dokumentierten Prozessen.

Anschließend muss der Ist-Zustand, also die Umsetzung der sich aus den Soll-Vorgaben des ADV-Vertrags und des DDSiKo ableitenden Anforderungen an die Verarbeitung (Prozesse und technisch-organisatorische Schutzmaßnahmen) geprüft werden. Für die Auditierung ergeben sich also die folgenden Prüfbereiche:

Standard-Vertrag
Der eingesetzte ADV-Vertrag (die Standard-Vertragsvorlage des Auftragnehmers) muss den gesetzlichen Anforderungen des BDSG (zukünftig der EU-DS-GVO) genügen. Dieser Vertrag, der den Rechtsrahmen und vor allem die Rechte und Pflichten der Vertragspartner regelt, ist damit Grundlage der späteren Zertifizierung; für abweichende ADV-Verträge, die der Auftragnehmer mit einem Auftraggeber abschließt, hat das Zertifikat daher nur begrenzte Aussagekraft, da die konkrete Umsetzung von Prozessen und Maßnahmen (Ist-Zustand) die Soll-Vorgaben des Vertrags erfüllen muss.

Zwar ist das Abschließen eines ADV-Vertrags grundsätzlich Pflicht des Auftraggebers, doch erlaubt nur ein standardisierter Vertrag eine umfassende Bewertung des Auftragsgegenstandes und damit die Zertifizierung des Auftragnehmers.

Der zertifizierte Auftragnehmer wird demnach künftig seinen Auftraggebern ein zertifiziertes Gesamtpaket „zertifizierte Auftragsdatenverarbeitung“ anbieten können, welches auch den (standardisierten und im Rahmen des Auftrags auf Rechtskonformität geprüften) ADV-Vertrag umfasst.

Datenschutz- und Datensicherheitskonzept
Im Datenschutz- und Datensicherheitskonzept beschreibt der Auftragnehmer zunächst das Verarbeitungsverfahren aus einer Datenschutzperspektive. Bewährt hat sich die Verwendung eines Datenflussdiagramms, aus dem die Verarbeitungsschritte, die an der Verarbeitung beteiligten Systeme und die jeweils verarbeiteten Datentypen hervorgehen. Diese Beschreibung ist daraufhin zu prüfen, ob sie die als Zertifizierungsgegenstand festgelegte Verarbeitung vollständig beschreibt.

Anschließend sind darin die Maßnahmen zum Schutz der im Auftrag verarbeiteten personenbezogenen Daten zu dokumentieren. Dabei sind vom Auftragnehmer sowohl die Erfüllung allgemeiner Datenschutzanforderungen als auch die konkret eingesetzten technischen und organisatorischen Maßnahmen zu beschreiben, die im Rahmen der Auftragsdatenverarbeitung Bestandteil des Vertragswerkes werden. Die Beschreibung der Maßnahmen muss

- den jeweiligen Schutzzweck und die grundsätzliche Eignung jeder Maßnahme für diesen Zweck erlauben und
- auf einem Detaillierungsgrad erfolgen, der es ermöglicht, diese Soll-Vorgaben einer Umsetzungsprüfung zu Grunde zu legen.

Das Datenschutz- und Datensicherheitskonzept muss auf Vollständigkeit, Eignung, Plausibilität, Datenschutzkonformität und Aktualität unter Berücksichtigung des Standes der Technik geprüft werden. Dabei sind sowohl das spezifische Leistungsangebot (die im Rahmen der Auftragsdatenverarbeitung betroffene Verarbeitung personenbezogener Daten zu den im ADV-Vertrag definierten Zwecken) als auch Vertragsspezifika zu berücksichtigen.

Prozesse
Nach der Bewertung des ADV-Vertrags muss dessen praktische Umsetzung in konkrete Prozesse, Abläufe und Arbeitsanweisungen geprüft werden (beispielsweise die Datenschutzverpflichtung der an der Verarbeitung beteiligten Mitarbeiter, Schulungsnachweise oder Anweisungen für den Umgang mit Datenschutzvorfällen). Die Prozesse müssen geeignet sein, die Erfüllung der Vereinbarungen des ADV-Vertrags zuverlässig sicherzustellen. Hierbei sind nur für das Auftragsverhältnis relevante Prozesse prüfungs- und zertifizierungsrelevant.

Technische und organisatorische Maßnahmen
Weiter muss die Umsetzung der im Datenschutz- und Datensicherheitskonzept des Auftragnehmers beschrieben organisatorischen und technischen Maßnahmen zum Schutz der verarbeiteten personenbezogenen Daten mindestens stichprobenartig und durch Einsichtnahme in die Dokumentation (beispielsweise Schlüsselausgabeliste, interne Datenschutzrichtlinie, Berechtigungskonzepte) geprüft werden.

Auch hier sind nur für das Auftragsverhältnis relevante Maßnahmen prüfungs- und zertifizierungsrelevant.

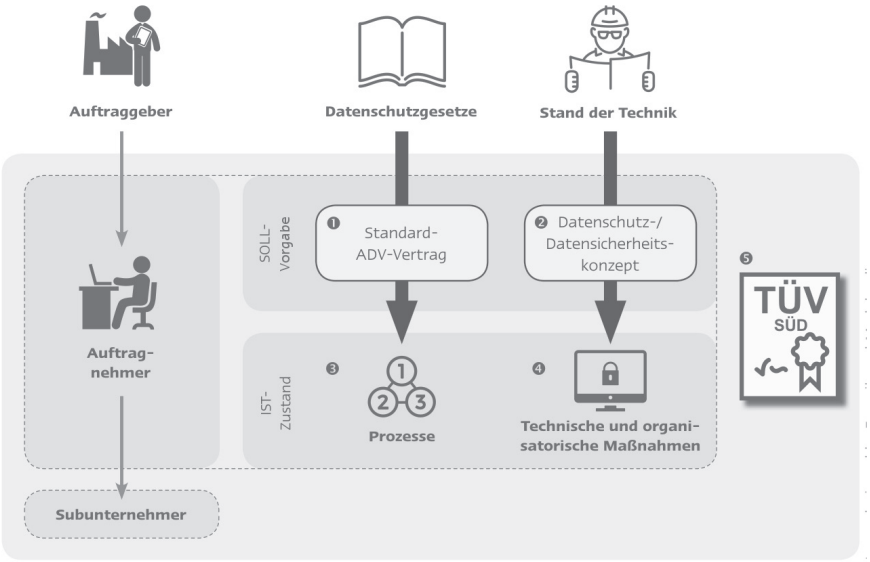
Prüfung von Unterauftragnehmern
Grundsätzlich sollte die ADV-Zertifizierung ausschließlich für den direkten ADV-Auftragnehmer erfolgen. In der Praxis werden allerdings oft Teile der Datenverarbeitung in unterschiedli-

cher Form von weiteren Unterauftragnehmern erbracht.

Bei der Kalkulation des Prüf- und Zertifizierungsaufwands sollte eine vollständige Erfassung der beteiligten Unterauftragnehmer erfolgen. Dabei wird im Einzelfall zu entscheiden sein, inwieweit und in welchem Umfang diese in die Prüfung einzubeziehen sind. Bei einigen Arten von Dienstleistungen, beispielsweise einem Housing in einem Rechenzentrum als Unterauftragnehmer, ist denkbar, sich mit einer Dokumentenprüfung vorhandener aktueller Zertifizierungen und Verträge zu begnügen (beispielsweise ISO 27001).

Gegebenenfalls können Unterauftragnehmer gleicher Art auch zusammengefasst, Anforderungen an sie gestellt und anschließend stichprobenartig im ersten und in jedem weiteren Folgeaudit geprüft werden (beispielsweise bei einer größeren Zahl von Druckereien, die als Unterauftragnehmer zum Einsatz kommen).

Abbildung 1 | Standard-ADV-Modell



Generell abzugrenzen sind „echte" Unterauftragsverhältnisse von solchen, die lediglich für „Hilfsdienstleistungen" geschlossen werden (beispielsweise Aktenvernichtung, Raumreinigung, allgemeine Wartungsdienstleistungen). Letztere sind nicht Gegenstand der Zertifizierung, wenngleich der Auftragnehmer vertraglich verpflichtet werden muss, auch solche Dienstleister sorgfältig auszuwählen und datenschutzrechtlich korrekt anzubinden.

Standard-ADV-Modell im Überblick

Nach diesem Standard-ADV-Modell ist eine Auditierung mit anschließender ADV-Zertifizierung effizient und effektiv gestaltbar. Für die Durchführung des Zertifizierungsaudits („Zertifizierungsreife") sind vom Auftragsdatenverarbeiter die folgenden Vorbereitungen zu treffen:

1. Erstellung einer auf die zu zertifizierende ADV-Dienstleistung zugeschnittenen ADV-Vertragsvorlage, die alle datenschutzrechtlichen Anforderungen erfüllt.
2. Entwicklung eines ausführlichen Datenschutz- und Datensicherheitskonzepts (Soll-Vorgabe), das eine Verfahrensbeschreibung (Datenflussdiagramm) und die Beschreibung aller relevanten technischen und organisatorischen Schutzmaßnahmen sowie deren Schutzzwecke umfasst.
3. Umsetzung der Vertragspflichten der ADV-Vertragsvorlage in konkrete Prozesse, Abläufe und Arbeitsanweisungen.
4. Interne Prüfung der Umsetzung der im Datenschutz- und Datensicherheitskonzept beschriebenen organisatorischen und technischen Schutzmaßnahmen („Vor-Audit").
5. Anschließend erfolgt die Auditierung und Zertifizierung durch den TÜV SÜD.

Fazit

Die Zertifizierung einer Auftragsdatenverarbeitung, die ein Auftragnehmer für mehrere Auftraggeber erbringt, birgt für alle Beteiligten erhebliche Vorteile:

Der Auftraggeber erfüllt seine gesetzlichen Prüfpflichten und spart gleichzeitig eigene Prüfaufwände. Durch den veröffentlichten Anforderungskatalog und das vom Auftragnehmer zu erstellende Datenschutz- und Datensicherheitskonzept entsteht zudem Transparenz, die weit über die verabeiteten „TOM-Stichwortlisten" hinaus geht. Dokumentation und Umsetzung der technischen und organisatorischen Maßnahmen beim Auftragnehmer werden durch erfahrene Prüfer bewertet; die kontinuierliche Weiterentwicklung des erreichten Schutzniveaus wird durch jährliche Folgeaudits gewährleistet.

Der Auftragnehmer kann außerdem in der Regel den Abschluss individueller ADV-Verträge vermeiden, die ihrerseits ein erhebliches Rechtsrisiko und Auftraggeber spezifische Umsetzungsprozesse bewirken können. Er spart interne Aufwände für Auftraggeber-Audits und gewinnt mit dem Zertifikat einen Datenschutz-Nachweis für Ausschreibungen und gegebenenfalls sogar einen Wettbewerbsvorteil. Die jährliche Re-Zertifizierung sorgt für einen kontinuierlichen Verbesserungsprozess. Mit mehreren in der ersten Jahreshälfte 2016 durchgeführten Zertifizierungen konnten die praktische Umsetzbarkeit und die erwarteten Wirkungen der Zertifizierung nachgewiesen werden.