REthinking: Tax

1 ▪ 2022
Januar 2022
4. Jahrgang

Chefredakteur
Stefan Groß

www.rethinking-tax.com

TECHNOLOGY & INNOVATION ▪ STRATEGY ▪ LAW ▪ CHANGE & SKILLS

TITELTHEMEN

Ampel meets TaxTech

WAS DER KOALITIONSVERTRAG AUS STEUERLICHER SICHT ZU BIETEN HAT ▪ 58, 82

Das Kassengesetz und der Teufel im Detail

DIE WICHTIGSTEN ZWEIFELSFRAGEN IN DER DISKUSSION ▪ 84

FACHMEDIEN ottoschmidt
Owlit Suchen. Finden. Wissen.

Interview mit DIETER KEMPF

Das „Kassengesetz", seine Umsetzung und der Teufel im Detail

Die wichtigsten Zweifelsfragen in der Diskussion

Text — Dr. Axel-Michael Wagner

Illustration — ljubaphoto/iStock

Ende 2016 wurden mit Wirkung zum 01.01.2020 die Vorschriften des „Kassengesetzes", §§ 146a und 146b AO, erlassen, zu denen 2017 die Kassensicherungsverordnung (KassenSichV) hinzutrat. Ob dort rechtspolitisch mit Kanonen auf Spatzen geschossen wurde, weil die aufgrund statistischer Annahmen vermuteten Probleme des Kassenbetruges – also die zu bekämpfende Gefahr – nur einen (kleinen) Teil der in Deutschland betriebenen Kassen betreffen, soll hier nicht weiter vertieft werden. Man kann durchaus der Meinung sein, dass der hier gewählte „One size fits all"-Ansatz, der ja beispielsweise auch der DSGVO zugrunde liegt, die Unterschiede von Einsatzgebieten, Systemkomplexität und Implementierungsaufwand nicht ausreichend berücksichtigt. Aber auch wenn man denken möchte, dass wenigstens die Umsetzung reibungslos abläuft, weil mittlerweile auf jedem Bon kryptische Signaturwerte bzw. QR-Codes aufgedruckt sind, ist die Praxis dennoch weit davon entfernt, sämtliche (rechtlichen) Implementierungsprobleme gelöst zu haben. Möglicherweise haben sich an der Schnittstelle zwischen Steuerrecht und IT, sprich zwischen Gesetzgeber (oder besser: BMF) und dem Bundesamt für die Sicherheit in der Informationstechnik (BSI), Reibungsverluste und Missverständnisse eingeschlichen und führen so zur Rechtsunsicherheit für die Steuerpflichtigen.

Die Rahmenbedingungen

Fangen wir von hinten an: Eine Ordnungswidrigkeit nach § 379 Abs. 1 Satz 1 Nr. 4 AO liegt vor, wenn zumindest leichtfertig ein elektronisches Aufzeichnungssystem, *„das jeden aufzeichnungspflichtigen Geschäftsvorfall und anderen Vorgang einzeln, vollständig, richtig, zeitgerecht und geordnet" aufzuzeichnen hat, „nicht oder nicht richtig verwendet" wird und der Täter es „dadurch ermöglicht, Steuern zu verkürzen oder nicht gerechtfertigte Steuervorteile zu erlangen"*. Dasselbe gilt, wenn ein elektronisches Aufzeichnungssystem und dessen digitale Aufzeichnungen *„nicht oder nicht richtig"* durch eine zertifizierte technische Sicherheitseinrichtung (zTSE) geschützt werden (§ 379 Abs. 1 Satz 1 Nr. 5 AO). Der Bußgeldrahmen liegt wegen der Verweisung in § 378 Abs. 1 Satz 1 AO bei bis zu 50.000 € pro Fall (§ 378 Abs. 2 AO). Was genau ein „nicht richtiges Verwenden" oder ein „nicht richtiges Schützen" ist, erklären diese Regelungen allerdings nicht. Wir werden darauf noch zurückkommen.

Daneben besteht die „Urangst" vor der „Hinzuschätzung" durch das Finanzamt (§ 162 Abs. 2 Satz 2 AO), die nach der ständigen Rechtsprechung des BFH dann möglich ist, wenn *„die Verletzung der formellen Ordnungsmäßigkeit der Kassenführung dazu führt, dass keine Gewähr mehr für die Vollständigkeit der Erfassung der Bareinnahmen geboten wird."* Diesbezüglich hat der BFH etwa im März 2015 festgestellt, dass *„das Fehlen einer lückenlosen Dokumentation zur Kassenprogrammierung in seinen Auswirkungen auf die Beurteilung der formellen Ordnungsmäßigkeit der Buchführung und der Eröffnung der Schätzungsbefugnis dem Fehlen von Tagesendsummenbons bei einer Registrierkasse bzw. dem Fehlen täglicher Protokolle über das Auszählen einer offenen Ladenkasse gleichsteht"*. Es gibt also durchaus rein formelle Mängel, die zu einer Schätzungsbefugnis führen können.

Nach der Verordnungsermächtigung zur Kassensicherungsverordnung (§ 146a Abs. 3 AO) soll diese definieren, welche elektronischen Aufzeichnungssysteme über eine zTSE verfügen müssen und welche Anforderungen für die technischen Komponenten der zTSE, die einheitliche digitale Schnittstelle (auch als DSFinV-K bekannt), die Protokollierung und Aufbewahrung von Aufzeichnungen, den auszugebenden Beleg und die Zertifizierung (inkl. deren Kosten) selbst gelten. Die Definition der Anforderungen an das Sicherheitsmodul, das Speichermedium und die einheitliche digitale Schnittstelle – aber nicht mehr – durfte der Verordnungsgeber (BMF) dann weiter an das BSI auslagern (§ 146a Abs. 3 Satz 2 und 3 AO). Diese Weiterdelegation hat in Bezug auf das Sicherheitsmodul, das Speichermedium und *„die Anbindung der zertifizierten technischen Sicherheitseinrichtung an das elektronische Aufzeichnungssystem"* stattgefunden (§ 5 KassenSichV).

Nach dem Gesetzeswortlaut ist die einheitliche digitale Schnittstelle allerdings „nur" ein Bestandteil der zTSE selbst (§ 146 Abs. 1 Satz 3 AO) und nicht eine „frei definierbare" Anforderung an die Beschaffenheit des elektronischen Aufzeichnungssystems (Kassensystems). Genau dies wird noch wichtig werden bei der Frage, wer eigentlich auf untergesetzlicher Ebene was regeln darf.

Nach dem Gesetzeswortlaut (§ 146a Abs. 3 Satz 1 Nr. 1 AO) entscheidet die KassenSichV darüber, welche elektronischen Aufzeichnungssysteme über eine zTSE verfügen müssen. Daraus ergibt sich im Umkehrschluss, dass es auch elektronische Aufzeichnungssysteme geben muss, die nicht über eine zTSE verfügen müssen, für die aber dennoch Gesetzesregelungen anwendbar sein dürften, die nicht nach zTSE- und nicht-zTSE-pflichtigen Aufzeichnungssystemen unterscheiden (wie § 146a Abs. 2 AO). Was in diesem Kontext überhaupt ein „elektronisches Aufzeichnungssystem" ist, wird weder im Gesetz (inkl. Begründung) noch in der KassenSichV definiert. Die Finanzverwaltung versteht hierunter „die zur elektronischen Datenverarbeitung eingesetzte Hardware und Software, die elektronische Aufzeichnungen zur Dokumentation von Geschäftsvorfällen und somit Grundaufzeichnungen erstellt" (Ziff. 2.1.4 der AEAO zu § 146). Das klingt nach einem sehr historischen Verständnis einer „Datenverarbeitungsanlage"; die Realität komplexer, verteilter und virtualisierter IT-Systeme – eingeschlossen die stetig zunehmenden Cloud-Lösungen – lässt sich so nicht zweckmäßig beschreiben. Auch die sich aus § 146a Abs. 1 Satz 1 AO mittelbar ergebende funktionale Beschreibung des „Erfassens" von Vorfällen oder Vorgängen führt nur bedingt weiter, da sämtliche im Ende-zu-Ende-Prozess involvierten IT-Komponenten die entsprechenden Datenströme durchschleusen und zwischenspeichern.

Es bleibt also eine Frage der wertenden Betrachtung – und damit mit erheblicher Rechtsunsicherheit behaftet –, wo ein Geschäftsvorfall „im steuerlichen Sinne aufgezeichnet" wird.

„Schützen" von Aufzeichnungen aus Sicht der Gesetzestexte

Soweit dies der AO und der KassenSichV als maßgeblichen Rechtsgrundlagen und Rahmen für konkretisierende BSI-Vorgaben zu entnehmen ist, geht es insgesamt um den Prozess der Aufzeichnung jedes aufzeichnungspflichtigen Geschäftsvorfalls und anderen Vorgangs. Was (bzw. welche Geschäftsvorfälle) generell im steuerlichen Sinne „aufzeichnungspflichtig" ist/sind, definiert der Gesetzgeber im Gesetz außerhalb von punktuellen Regelungen nicht. Die Finanzverwaltung geht im Einklang mit der Gesetzesbegründung (zu solchen „Einklängen" vgl. nachfolgend) davon aus, dass jeder Geschäftsvorfall aufzeichnungspflichtig ist (Ziff. 1.8.1 der AEAO zu § 146a), sodass es des Wörtchens „aufzeichnungspflichtigen" im Gesetz eigentlich gar nicht bedurft hätte. Ein „anderer Vorgang" ist etwa die Stornierung und nach der Gesetzesbegründung generell jeder Vorgang, der *„unmittelbar durch Betätigung der Kasse erfolgt"*. Obwohl der Gesetzgeber ausweislich der Gesetzesbegründung mit dem Begriff der „anderen Vorgänge" für „Rechtsklarheit" sorgen wollte, geht die Finanzverwaltung in einer sich nicht aus dem Gesetz ergebenden Rückausnahme in Ziff. 1.9.2 der AEAO zu § 146a davon aus, dass Vorgänge, die *„für die Erreichung der Schutzziele nicht erforderlich"* sind, nicht aufgezeichnet werden müssen. Diese Schutzziele wiederum ergeben sich nicht aus dem Gesetz oder der Gesetzesbegründung, sondern werden von der Finanzverwaltung im üblichen GoBD-Sprachgebrauch definiert (Ziff. 1.4 der AEAO zu § 146a: Integrität, Authentizität, Vollständigkeit).

Nach der Gesetzesregelung sind sowohl das Aufzeichnungssystem selbst als auch dessen Aufzeichnungen mit der zTSE zu schützen (§ 146a Abs. 1 Satz 2 AO). Man könnte dies so verstehen, dass die zTSE auch die Integrität des Aufzeichnungssystems an sich (vor nicht näher definierten Gefahren) schützen soll, also das Gesamtsystem aus Hardware und Software. Es ist aber nicht vorstellbar, wie ein solches Gesamtsystem gegen nicht näher konkretisierte IT-Gefahren durch ein „Sicherheitsmodul" geschützt werden kann (so ein Sicherheitsmodul hätte wohl jeder gerne). In der Gesetzesbegründung zur Einführung des § 146a AO wurde im Gegenteil festgehalten, dass jedenfalls Änderungen der Software oder Hardware von Kassensystemen, *„die nicht die technische Sicherheitseinrichtung betreffen"*, keine Auswirkungen auf das Zertifikat einer zTSE haben.

Es bleibt also, und dafür sprechen auch die Verordnungsermächtigung und die KassenSichV selbst, beim Schutz der Aufzeichnungen (Daten) als solcher, und es bleibt unklar, ob und was der Gesetzgeber im Hinblick auf das Aufzeichnungssystem selbst schützen lassen wollte.

Nun können Aufzeichnungen die Realität richtig oder falsch (einschließlich unvollständig) wiedergeben; sie werden vielleicht richtig „geschützt", sind aber tatsächlich unrichtig. Man sollte sich in

> **Das Hauptrisiko des „Kassenbetruges“ besteht nicht in Angriffen auf „schützende“ IT-Systeme, sondern im schlichten Unterlassen der Eingabe von Daten in das System.**

diesem Zusammenhang vor Augen halten, dass das Hauptrisiko des „Kassenbetruges“ nicht in Angriffen auf aufzeichnende oder „schützende“ IT-Systeme, sondern im schlichten Unterlassen der Eingabe von Daten in das System besteht. Dem soll einerseits die Bonpflicht entgegenwirken, die – von stichprobenartigen Kontrollen durch „Inkognito-Betriebsprüfer“ abgesehen – die flächendeckende Kontrolle der Milliarden Kassentransaktionen jährlich den „wachsamen Kundenbürgern“ überlässt. Und andererseits knüpft, wie oben gesehen, die Ordnungswidrigkeit des „Nicht- oder nicht richtigen Verwendens“ des Aufzeichnungssystems u.a. genau an diesen Fall an, dass (schon) dessen Aufzeichnungsfunktion übergangen oder manipuliert wird. An dieser Stelle kann festgehalten werden, dass die richtige und vollständige Aufzeichnung als solche nicht Gegenstand des Schutzes durch die zTSE ist, sondern durch anderweitige technische und organisatorische Maßnahmen im Hinblick auf das Aufzeichnungssystem sichergestellt und prozessbezogen dokumentiert werden muss. Jeder mag selbst entscheiden, ob angesichts dieses immensen, nicht adressierbaren Restrisikos die Einführung der „Kassenfiskalisierung“ neben § 146 AO und den GoBD mit ihren weitgehenden (auch Dokumentations-) Anforderungen, die neben den Regelungen des „Kassengesetzes“ anwendbar bleiben, nicht ein Schuss „mit Kanonen auf Spatzen“ war. Politischer Stein des Anstoßes für das (damals im Gesetzgebungsverfahren als „besonders eilbedürftig“ gekennzeichnete) „Kassengesetz“ war seinerzeit, wie man hört, der „Cum-Ex-Skandal“, im Zuge dessen dem BMF vorgeworfen wurde, durch jahrelange Untätigkeit Steuerbetrug ermöglicht zu haben. Bisweilen schwingt dann das Pendel aktionistisch in die andere Richtung aus.

Doch zurück: Der Schutz durch die zTSE betrifft die – hoffentlich richtigen und vollständigen – Daten des Aufzeichnungssystems, d.h. die digitalen Grundaufzeichnungen, kurz nach ihrer Entstehung bis hin zur Archivierung und zum Datenzugriff durch die Finanzverwaltung im Rahmen von Kassen-Nachschau oder Betriebsprüfung. Nach der Vorstellung des Gesetzgebers fließen die Daten des Aufzeichnungssystems in das Sicherheitsmodul. Dieses soll digitale Grundaufzeichnungen protokollieren, um deren Integrität und Authentizität sowie die Vollständigkeit der elektronischen Aufzeichnung sicherzustellen (§ 146a Abs. 3 Satz 1 Nr. 2 lit. e AO). Die Sicherung von Integrität, Authentizität und Vollständigkeit ab diesem Zeitpunkt bezieht sich demnach auf die zum Sicherheitsmodul gelangten Daten, nicht auf die vollständige Entsprechung zu den tatsächlichen (Kassier-) Vorgängen „in der realen Welt“.

Die Protokollierung – und damit der Schutz – von digitalen Grundaufzeichnungen über Geschäftsvorfälle beginnt technisch mit dem Start einer neuen „Transaktion“ durch das elektronische Aufzeichnungssystem. Da die Transaktion bestimmte, in § 2 KassenSichV formulierte Informationen zum „Vorgang“ zu „enthalten“ hat, könnte man meinen, dass „Transaktion“ im Gesetzessinne ein Datensatz ist, der an das Sicherheitsmodul übertragen wird. Allerdings sollen Teile dieser Transaktion, insbesondere die Transaktionsnummer, *„manipulationssicher durch das Sicherheitsmodul festgelegt“* werden, und zwar so, *„dass Lücken in Transaktionsaufzeichnungen erkennbar sind“*. Darüber hinaus regeln die gesetzlichen Grundlagen im Gegensatz zum Start das Ende der Transaktion nicht, im Gegenteil: Das Wort „Transaktion“ wird außerhalb von § 2 KassenSichV gar nicht verwendet,

auch nicht im Zusammenhang mit der Definition technischer Anforderungen an „die Anbindung der zertifizierten technischen Sicherheitseinrichtung an das elektronische Aufzeichnungssystem“ (§ 5 Satz 1 Nr. 1 KassenSichV). Man kann hier festhalten, dass im Kontext der KassenSichV unklar bleibt, was die „Transaktion“ und der „Vorgang“ genau – und in Abgrenzung zu dem in der AO verwendeten Begriff des „Geschäftsvorfalls“ – ist. Auch ist bzw. wäre das BSI nicht befugt, diese Begrifflichkeiten zu definieren oder auszufüllen, weil das nicht von der Weiterdelegation an das BSI umfasst wird (§ 5 KassenSichV).

Anwendungserlass und BSI-Richtlinien

Das deutsche Steuerrecht spielt sich hauptsächlich nicht in Gesetzen und Verordnungen, sondern in (lediglich) verwaltungsbindenden Anwendungserlassen (AEAO) der Finanzverwaltung ab. Die Finanzverwaltung definiert ein „De-facto-Recht“, das zwar die Gerichte nicht formal bindet, nach dem sich aber dennoch alle richten. So ist es auch bei den AEAO zu § 146a; hier erklärt das BMF, was es sich bei der Ausarbeitung der dann parlamentarisch verabschiedeten Gesetze gedacht hat. Praktischerweise enthalten Gesetzesbegründung und Anwendungserlass zu § 146a AO sehr ähnliche, jeweils vom BMF stammende Formulierungen, sodass auch den Gerichten die rechtliche Möglichkeit gegeben wird, sich an den in der Gesetzesbegründung bereits „angelegten“ Anwendungserlassen zu orientieren. Sogar die Frage, welche elektronischen Aufzeichnungssysteme überhaupt mit einer zTSE versehen werden müssen, weil es sich um *„elektronische oder computergestützte Kassensysteme oder Registrierkassen“* handelt (§ 1 Satz 1 KassenSichV), wird vom BMF im Anwendungserlass definiert, weil die in der KassenSichV verwendete (Kurz-) Formulierung ohne weitere „Handreichung“ nur die Einordnung solcher Fälle zulässt, die von vornherein eindeutig sind. Dies soll aber hier nicht weiter vertieft werden.

Vor diesem Hintergrund bringen die Tz. 1.6 bis 1.8 AEAO zu § 146a beispielsweise Licht in das Dunkel des Verordnungstextes, was das Verhältnis zwischen Geschäftsvorfall, Vorgang und Transaktion betrifft. Ohne diese Erläuterungen wäre der Text von § 2 KassenSichV gar nicht verständlich. Hiernach ist der „Geschäftsvorfall“ der zugrunde liegende rechtliche bzw. wirtschaftliche Sachverhalt im Unternehmen, der zu einem „Vorgang“ im Aufzeichnungssystem führt, der wiederum zu einer „Transaktion“ im Sinne einzelner Absicherungsschritte innerhalb der zTSE führt. Einem Vorgang im Aufzeichnungssystem muss allerdings kein Geschäftsvorfall zugrunde liegen, sondern es kann sich auch um eine andere (durch die zTSE zu protokollierende) Nutzung oder Konfiguration des Aufzeichnungssystems handeln.

Der Anwendungserlass wiederum wird durch FAQ des BMF ergänzt, die laufenden Änderungen und Erweiterungen unterliegen.

Vielleicht ist das ein Ausblick auf den Gesetzgeber von morgen, der gar keine Gesetze mehr erlässt, sondern typische Fallkonstellationen und Zweifelsfragen auf seiner Website veröffentlicht und eine Lösung vorgibt, die heute anders als gestern lauten kann.

Weitere „Rechtsquelle“ des BMF ist die im Internet verfügbare *„Zusammenstellung der Beschlüsse und Bundeskonventionen zu den Standardtabellen im Bereich der Kassenbuchhaltung – Digitale Schnittstelle der Finanzverwaltung für Kassensysteme (DSFinV-K)“,* die in § 4 KassenSichV abstrakt umschrieben wird. Das ist deshalb bemerkenswert, weil die „Anforderungen an die einheitliche digitale Schnittstelle“ nach § 146a Abs. 3 Satz 1 Nr. 2 lit. c AO in der KassenSichV „bestimmt“ werden müssen und § 4 KassenSichV selbst nicht einmal konkretisiert, wer diese „Datensatzbeschreibung“ wie und wann definiert und veröffentlicht. Überraschend wird erst in § 6 Satz 4 KassenSichV – in der Vorschrift über die Anforderungen an den auszugebenden Beleg – außerhalb des dortigen Kontextes und sprachlich ungenau geregelt, dass die „digitale Schnittstelle“ (das „einheitlich“ fehlt hier) auf der Internetseite des Bundeszentralamts für Steuern in der jeweils geltenden Fassung veröffentlicht wird. Ob die Beschreibung der Komponenten der einheitlichen digitalen Schnittstelle in § 4 KassenSichV ausreicht, um, wie die AO fordert, die „Anforderungen“ an die Schnittstelle zu beschreiben, sei hier einmal dahingestellt.

Hinzu kommen die verschiedenen BSI-Richtlinien und Schutzprofile, die auf Basis von § 5 KassenSichV ergangen sind. Im Kern sind dies die TR-03153, deren Fokus die *„Definition von Mindestanforderungen an die Interoperabilität“* der zTSE ist, sowie das SMAERS-Schutzprofil

BSI-CC-PP-0105-V2-2020. Letzteres beschreibt die SMAERS-Komponente des Sicherheitsmoduls, welches neben dieser Komponente noch das eigentliche, separat definierte „Signiermodul" (CSP) umfasst. Die SMAERS-Komponente stellt eine „Applikation" dar, die Daten zwischen dem Aufzeichnungssystem und dem CSP mittelt. Der CSP selbst ist eine generische Krypto-Komponente, die mit einem asymmetrischen Verschlüsselungsalgorithmus arbeitet, d.h. mithilfe eines öffentlichen, frei verfügbaren Schlüssels kann später getestet werden, ob dem CSP der zugehörige, „geheime" private Schlüssel vorlag, mit dem ein Nutzdatensatz bzw. Hashwert verschlüsselt (signiert) wurde. Da der CSP zusätzlich zum privaten Schlüssel über einen gesicherten Zeitgeber verfügt, kann so „bewiesen" werden, dass dem CSP zu einem bestimmten Zeitpunkt bestimmte Daten vorlagen, und später die Identität vorliegender Datensätze mit den damals signierten Originaldaten festgestellt werden. SMAERS und CSP können auf derselben Hardware ablaufen (Hardware-zTSE, z.B. SmartCard) oder in unterschiedlichen Systemumgebungen verortet sein (Cloud-zTSE). Wir werden auf die einzelnen Komponenten noch zurückkommen.

Ob diese Schichtung und Verschachtelung von Rechtsquellen so überhaupt (verfassungsrechtlich) zulässig ist, wird vermutlich nie jemand infrage stellen, weil schon die sich stellenden Sachfragen beim „Zusammenlesen" der Rechtsquellen schwierig genug zu beantworten sind und weil man derartige Themen nicht in einer Betriebsprüfung diskutieren möchte. Die verschiedenen Regelungsebenen und Regelungsautoren zeigen aber, wie schwer es für Legislative und Exekutive ist, stringente Vorgaben für die (plattformneutrale) technische Ausgestaltung digitaler Prozesse über Systemgrenzen hinweg zu machen, und wie schwer es für den Rechtsanwender ist, diese Vorgaben über die Regelungsebenen (mit ihren rechtlichen „Schnittstellenproblemen") hinweg nachzuvollziehen.

In der Praxis macht man es so, wie es alle anderen machen, wie es IT-technisch vernünftig ist oder wie es das BSI oder das BMF (teils „formlos") vorgeben. Das ist verständlich, denn aus dem materiellen Gesetzesrecht kann man das, was tatsächlich passieren soll, nur höchst bruchstückhaft herauslesen.

Prozess und Datenfluss

Wenn man alle genannten „Rechtsquellen" zusammennimmt, ergibt sich für Geschäftsvorfälle wie eine Bargeldvereinnahmung ein Datenflussschema zwischen verschiedenen Komponenten, welches sich in der Praxis aber nicht „einfach so" abbilden lässt. Vielmehr sind bei der praktischen Umsetzung Details „auszufüllen", die allein anhand der Rechtsquellen nicht beantwortet werden können. Das führt natürlich zu Rechtsunsicherheit, weil in derartigen Lücken – wie immer im Steuerrecht – eine „profiskalische" Sichtweise und eine „steuerpflichtigenfreundliche" (im Bereich von Kassensystemen auch „herstellerfreundliche") Sichtweise formuliert werden kann.

Der Geschäftsvorfall wird zunächst im elektronischen Aufzeichnungssystem abgebildet, wodurch (Kassen-) Daten über den Vorgang generiert werden. Diese Daten werden in Tz. 3.4.1 des AEAO zu § 146a „Anwendungsdaten" genannt. Diese Anwendungsdaten müssen zunächst den DSFinV-K-Vorgaben (dort Anhang I) für die Schnittstelle zwischen Aufzeichnungssystem und zTSE entsprechen, um durch die zTSE „geschützt" werden zu können. Die BSI-Regularien sparen allerdings die Beschaffenheit (Datensatzdefinition) dieser sog. „Vorgangsdaten" aus. Die Übermittlung der Anwendungsdaten im Rahmen der „Fiskalisierung" an die zTSE geschieht über eine funktionale Steuerungsschnittstelle (API) der SMAERS-Komponente, die vom BSI „Einbindungsschnittstelle" genannt wird und dem Aufzeichnungssystem verschiedene Funktionen bereitstellen soll. Hier kann u.a. die Funktion zum Start von Transaktionen aufgerufen werden, wobei jede Transaktion wiederum nach der TR-03153 aus mehreren Absicherungsschritten (mindestens zwei) besteht. Bei funktionaler Betrachtung werden innerhalb des Sicherheitsmoduls die Anwendungsdaten (als „Vorgangsdaten") von der SMAERS-Komponente entgegengenommen und mittels des CSP signiert, wobei dies technisch durchaus in verteilten Systemen stattfinden kann (dazu noch unten). Die Definition dieser *„Anbindung der zertifizierten technischen Sicherheitseinrichtung an das elektronische Aufzeichnungssystem"* wird in § 5 Satz 1 Nr. 1 KassenSichV an das BSI delegiert, findet aber in § 146a Abs. 1 Satz 3, Abs. 3 Satz 1 Nr. 2 lit. c AO keine ausdrückliche Ermächtigungsgrundlage.

Illustration — ljubaphoto/iStock

Dass das Sicherheitsmodul nun anlässlich der Übermittlung von Anwendungsdaten seinerseits eigene „Protokolldaten“ erzeugt, kann dem Text der KassenSichV nicht entnommen werden, obwohl die Überschrift von § 2 *„Protokollierung von digitalen Grundaufzeichnungen“* lautet und die Bestimmung der Anforderungen an die Protokollierung nach § 146a Abs. 3 Satz 1 Nr. 2 lit. e AO eine Aufgabe der KassenSichV ist. In § 2 KassenSichV ist nur unscharf bestimmt: *„Die Transaktion hat zu enthalten“* – gefolgt von einer Auflistung eines „Mindestbestandes“ von Inhalten. Erst aus Tz. 3.2.4 der AEAO zu § 146a wird ersichtlich, dass das Sicherheitsmodul der zTSE im Rahmen des Signierprozesses eigenständig Protokolldaten erzeugt sowie dann die Signatur selbst („Prüfwert“, § 2 Satz 2 Nr. 7 KassenSichV) ermittelt. Technisch wird der Hashwert eines Datenblocks signiert, der aus den Anwendungsdaten und vom Sicherheitsmodul hinzugefügten Protokolldaten (z.B. Transaktionsnummer, Signaturzähler, Uhrzeit) besteht. Jeder, der die in diesem Datenblock vorhandenen Daten ebenfalls zur Verfügung hat, kann demnach sicher nachvollziehen, dass einer bestimmten zTSE, die exklusiv über den privaten Signierschlüssel verfügt, zu einer bestimmten Uhrzeit bestimmte Daten vorlagen.

Schon um die gesetzliche Belegausgabepflicht (§§ 146a Abs. 2 AO, 6 KassenSichV) erfüllen zu können, müssen die Protokolldaten und der Prüfwert an das Aufzeichnungssystem zurückgegeben werden, denn eine zTSE selbst gibt üblicherweise keine Belege an den Kunden aus. Die SMAERS-Komponente muss also „bidirektional“ ausgestaltet werden. Die ausdrückliche Notwendigkeit des „Rückflusses“ der Daten aus der zTSE an das Aufzeichnungssystem findet sich in den gesetzlichen Vorgaben nicht, sondern lediglich in Ziff. 3.5 Nr. 3 der AEAO zu § 146a. Auch aus der TR-03153 (Ziff. 5.1) ist das Thema nur mittelbar ersichtlich, indem Funktionen der „Einbindungsschnittstelle“, die der „Integration“ der zTSE „in das Aufzeichnungssystem“ dient, die Möglichkeit des Exports der „Log-Nachrichten“ sowie „der gesicherten, zu protokollierenden Daten und den korrespondierenden Protokolldaten, der für die Verifikation der Prüfwertberechnung benötigten Zertifikate sowie den Initialisierungsdaten“ vorgeben. Auf diese Weise kann das Aufzeichnungssystem – neben dem Export der zTSE-Daten aus dessen (eigenem) Speichermedium – die (teils im Beleg anzudruckenden) Protokolldaten anfordern und extrahieren. Aber noch für einen anderen Aspekt ist der Datenrückfluss an das Aufzeichnungssystem essenziell: Die vom Aufzeichnungssystem zu erstellenden DSFinV-K-Daten beinhalten die Protokolldaten und den Prüfwert der zTSE ebenfalls in den Dateien „Stamm_TSE“ und „TSE_Transaktionen“. Im Folgenden geht es nun unter anderem darum, was im Unterschied zu den zTSE-Daten noch Bestandteil der DSFinV-K-Daten ist und wie diese entstehen bzw. abgezogen werden können/müssen.

Speicherung und Datenformate zum Datenabzug

Wie bereits angedeutet, muss in Bezug auf die Speicherung und den Export zwischen zwei

Datenströmen unterschieden werden, was in Ziff. 4.2 AEAO zu § 146a sowie in Ziff. 1.1.2 und 1.1.3 der DSFinV-K hergeleitet bzw. erläutert wird. Die Daten, die mittels der Exportschnittstelle aus der zTSE abgezogen werden können, sind *„allein nicht ausreichend, da nicht alle erforderlichen Daten in die Protokollierung durch die TSE einfließen“*. Neben die Protokoll- bzw. Log-Daten der zTSE treten die *„einzelnen, aufgezeichneten Daten in einem maschinell auswertbaren Format“* zur Erfüllung der GoBD-Vorgaben und dieses Format wird – als *„selbstständiger Bestandteil der Einheitlichen Digitalen Schnittstelle“* – durch die DSFinV-K vorgegeben. Der Export dieser Daten soll nicht aus der zTSE, sondern aus dem Aufzeichnungssystem selbst erfolgen, was aber erst nach einem durchgeführten Kassenabschluss, also zeitlich versetzt, möglich ist. Die AEAO sprechen insoweit von *„allen mit dem elektronischen Aufzeichnungssystem aufgezeichneten Daten“*. In § 146a Abs. 1 AO ist der standardisierte Abzug bestimmter Daten aus dem Aufzeichnungssystem nicht vorgesehen, was unten noch näher erläutert wird. In der Praxis gibt es in den generierten DSFinV-K-Daten noch häufig Fehler, wobei das Bestreben der Anbieter von Kassensystemen darin besteht, dass die generierten Daten die automatisierte Prüfung mit der „Prüfsoftware der Finanzverwaltung“ bestehen, einem Vorboten der „Code as law“-Zukunft.

Dieses Vorgehen führt im Ergebnis zu drei Datenströmen: Den Log-Daten aus der zTSE, den DSFinV-K-Daten aus dem Aufzeichnungssystem und „sonstigen Kassendaten“, die von einem Kassensystem generiert werden, aber in den ersten beiden Datendefinitionen nicht abgebildet werden können bzw. ohnehin in einem ganz anderen Format vorliegen (und traditionell in diesem Format z.B. an ein ERP-System übergeben werden). Auch diese sonstigen Kassendaten sind selbstverständlich steuerlich relevant und GoBD-konform zu behandeln.

In der praktischen Implementierung bei Unternehmen mit etwas komplexeren Kassensystemen führt dies zu einer erheblichen Mehrbelastung, da nun mehrfache Organisations-, Transport- und Archivlogiken vorgesehen werden müssen. Es wäre wünschenswert gewesen, wenn der Gesetzgeber über derartigen Mehraufwand im Vorfeld nachgedacht und diesen zu vermeiden beigetragen hätte.

Sieht man sich zunächst den zTSE-Datenstrom genauer an, so resultiert aus der Protokollierung innerhalb der zTSE ein ständiger Strom von „Fiskaldatenpaketen“, bestehend aus (signierten) Anwendungsdaten, zugehörigen (signierten) Protokolldaten und zugehörigen Prüfwerten, die aus der zTSE ausgelesen werden können. § 3 KassenSichV gibt dann unscharf formuliert vor, dass die „Geschäftsvorfälle“ (auch) laufend auf einem „nichtflüchtigen Speichermedium“ gespeichert werden sollen – wie das (auf Basis der Definition von „Geschäftsvorfall“) wörtlich umzusetzen ist, bleibt natürlich unklar. Ob das

Speichermedium, das in der KassenSichV als Teil der zTSE genannt wird (§ 5 KassenSichV), identisch ist mit diesem in § 3 Abs. 1 KassenSichV genannten „nichtflüchtigen Speichermedium", auf dem „die laufenden Geschäftsvorfälle" zu speichern sind, ist nicht eindeutig. Das ist deshalb relevant, weil § 3 Abs. 3 KassenSichV von der Übertragung von gespeicherten digitalen Grundaufzeichnungen von einem elektronischen Aufzeichnungssystem in ein „externes elektronisches Aufbewahrungssystem" spricht, aber die zTSE kein Teil des Aufzeichnungssystems ist. Es wird also nicht klar, welche Daten nun nach der Vorstellung des Verordnungsgebers genau wo liegen. Klarheit schafft hier erst Ziff. 8.3 AEAO zu 146a: Neben der Übertragung der zTSE-Daten in ein Archiv (sodass diese in der zTSE gelöscht werden können) ist auch die Überführung der „übrigen Daten des Aufzeichnungssystems" (also der DSFinV-K-Daten) in ein Aufbewahrungssystem möglich, das dann auch den DSFinV-K-Export zur Verfügung stellen muss.

Wie oben bereits angedeutet, sucht man Anhaltspunkte für den zweiten Datenstrom – die aus dem Aufzeichnungssystem stammenden DSFinV-K-Daten – im Gesetzestext vergeblich. § 146a Abs. 3 Satz 1 Nr. 2 lit. c AO nennt zwar die „einheitliche digitale Schnittstelle" als einen Bereich, für den die KassenSichV die „Anforderungen" bestimmen kann, definiert diese aber nicht. Nach § 146a Abs. 1 Satz 3 AO ist die „einheitliche digitale Schnittstelle" neben dem Sicherheitsmodul und dem Speichermedium ein Bestandteil der zTSE. Dies legt es nahe, dass auch der Verordnungsgeber nur etwas definieren durfte, was sich direkt „in" oder „an" der zTSE abspielt. Auch nach § 146a Abs. 1 Satz 4 AO sind „die digitalen Aufzeichnungen" (des elektronischen Aufzeichnungssystems) auf dem Speichermedium (der zTSE, § 146a Abs. 1 Satz 3 AO) zu sichern und *„für Nachschauen sowie Außenprüfungen [...] verfügbar zu halten"*. Es geht also hier gerade nicht um die Daten im Aufzeichnungssystem selbst, sondern nur um die an die zTSE übertragenen (zu „protokollierenden") Daten und die daraus resultierenden, in der zTSE selbst gespeicherten Daten. Vom weiteren Schicksal der (nach § 146a Abs. 1 Satz 1 AO vorgegebenen) Aufzeichnungen außerhalb der zTSE, also den Aufzeichnungen des Aufzeichnungssystems in diesem selbst, ist in § 146a AO nicht die Rede. Damit gelten dort grundsätzlich die allgemeinen Vorschriften, insbesondere § 146 AO und die GoBD.

Es scheint, als habe der Gesetzgeber bei der Abfassung von § 146a AO keine klare Vorstellung von den als notwendig erachteten Datenflüssen gehabt.

> **Wünschenswert wäre gewesen, wenn der Gesetzgeber über den Mehraufwand im Vorfeld nachgedacht und diesen zu vermeiden beigetragen hätte.**

Vor dem Hintergrund dieser gesetzlichen Ermächtigungsgrundlage definiert nun § 4 KassenSichV, dass die einheitliche digitale Schnittstelle eine *„Datensatzbeschreibung für den standardisierten Export aus dem Speichermedium nach § 3 Absatz 1, der Anbindung an das elektronische Aufzeichnungssystem und dem elektronischen Aufbewahrungssystem zur Übergabe an den mit der Kassen-Nachschau oder Außenprüfung betrauten Amtsträger der Finanzbehörde"* ist. Grammatikalisch betrachtet geht es also um den standardisierten Export „aus" dem zTSE-Speichermedium (das Log-Daten speichert und über die zTSE-Exportschnittstelle bereitstellt), um den Export „aus" der Anbindung an das elektronische Aufzeichnungssystem und um den Export „aus" dem elektronischen Aufbewahrungssystem (das ja einen „DSFinV-K-Export" bereitstellen soll). Letzteres findet in der AO keine Stütze (s.o.), und was Zweiteres bedeuten soll, ergibt sich aus den Rechtsquellen nicht (ein „Export aus einer Anbindung" ist inhaltlich kaum möglich). Wahrscheinlicher ist diesbezüglich, dass der Verordnungsgeber die *„Datensatzbeschreibung für die Anbindung an das elektronische Aufzeich-*

nungssystem“ – die in Anhang I der DSFinV-K definiert ist – gemeint hat, was zumindest noch als „Schnittstellenthema“ zwischen zTSE und Aufzeichnungssystem gewertet werden und damit unter die „Definition“ in § 146a Abs. 1 Satz 3 AO fallen könnte.

IT-Komponenten und Umgebungsschutz

Aus alldem und unter Berücksichtigung der bisherigen zertifizierten Lösungen und Implementierungen („best practice“) zeichnet sich ein „gewollter“ End-to-End-Prozess ab, auch wenn dieser nur unzureichend geregelt ist. Die Daten entstehen im Aufzeichnungssystem, werden dort in ihrer „Urform“, wenn auch in einem vorgeschriebenen Format, der Finanzverwaltung zur Verfügung gestellt, gleichzeitig in einem weiteren definierten Format an die zTSE zur „Protokollierung“ übertragen und auch dort der Finanzverwaltung in einem definierten Format zur Verfügung gestellt. Für komplexere Systemumgebungen bedeutet dies zunächst umfangreiche Änderungen der Kassensoftware. Der Gesetzgeber sichert dies damit ab, dass es nach § 146a Abs. 1 Satz 5 AO verboten ist, elektronische Aufzeichnungssysteme oder Software hierfür (gewerbsmäßig) zu bewerben oder in Verkehr zu bringen, die den Vorgaben von § 146a Abs. 1 Satz 1 bis 3 AO nicht entsprechen. Dies bezieht sich (lediglich) auf die einzelne, vollständige, richtige, zeitgerechte und geordnete Aufzeichnung jedes Geschäftsvorfalls (und anderen Vorgangs) sowie auf den (als solchen nicht möglichen, s.o.) Schutz „des Aufzeichnungssystems“ und der Aufzeichnungen durch eine zTSE.

Aus den Rechtsquellen kann nicht geschlossen werden, dass der Hersteller eines Aufzeichnungssystems Anforderungen aus der einheitlichen digitalen Schnittstelle zu implementieren hat, denn diese ist nach dem Gesetzeswortlaut Teil der zTSE (s.o.). Allenfalls kann die Implementierung der Einbindungsschnittstelle als denknotwendiger Bestandteil einer Koppelung von Aufzeichnungssystem und zTSE angesehen werden, indem das Aufzeichnungssystem aus den in einem originären, internen Format vorgehaltenen Kassentransaktionsdaten die zTSE mit entsprechend formatkonvertierten Daten zur Ermittlung des Prüfwerts „bespielen“ muss. Dennoch werden in der Praxis natürlich die DSFinV-K-Vorgaben befolgt und die Aufzeichnungssysteme generieren aus den eigenen Kassentransaktionsdaten und den aus der zTSE nach der Signierung exportierten Daten DSFinV-K-Datensätze. In der Praxis werden für die dabei anfallenden Export-, Import- und Konsolidierungsprozesse Middleware-Pakete angeboten, deren Implementation einen nicht unerheblichen Aufwand darstellt. Schon bis hierhin kann die Umsetzung in verschiedene IT-Komponenten zerfallen (Endgeräte, Kassenserver, Middleware-Server etc.), die untereinander angebunden werden müssen und hinsichtlich derer sich die Frage stellt, welche Angriffsszenarien aus steuerrechtlicher Sicht bei der Konzeptionierung und Implementierung zu berücksichtigen sind.

Könnte man alleine aus der gesetzlichen Vorgabe der „richtigen“ Aufzeichnung folgern, dass das ggf. in Komponenten aufgeteilte Aufzeichnungssystem gegen Angriffe „von jeder Seite“ gehärtet werden muss und ansonsten nicht in Verkehr gebracht werden darf, was erheblichen Mehraufwand bei der Entwicklung und dem Testen eines Aufzeichnungssystems sowie erhebliche Anforderungen an die Laufzeitumgebung(en) mit sich bringt? Über die hier maßgeblichen Grenzen hat sich der Gesetzgeber offensichtlich keine Gedanken gemacht.

Der Hersteller einer zTSE kann sich mittlerweile – in den ersten Versionen der BSI-Dokumente war das gar nicht vorgesehen – zwischen einer integrierten und einer verteilten (Cloud-zTSE)-Architektur entscheiden. Es wäre interessant gewesen zu bewerten, ob die Ermächtigungsgrundlage, die dem BSI die Definition der (technischen) Anforderungen an die zTSE pauschal überlässt (§§ 146a Abs. 3 Satz 3 AO, 5 KassenSichV), den kategorischen Ausschluss einer Cloud-Architektur für zTSEs „getragen“ hätte. Allerdings kann es nicht verwundern, wenn das BSI basierend auf einer Bedrohungsanalyse (z.B. Ziff. 3.2 des SMA-ERS-Schutzprofils) anstrebt, die Anforderungen an das Sicherheitsmodul und dessen einzelne Komponenten möglichst weitreichend zu regeln. Dies schließt sowohl die „Innenarchitektur“ des Sicherheitsmoduls als auch die Laufzeitumgebung von dessen einzelnen Komponenten ein. Eine der dabei angenommenen Bedrohungen ist eine Attacke des Steuerpflichtigen selbst, der ein manipuliertes Sicherheitsmodul nutzen oder Log-Nachrichten nach deren Produktion durch die zTSE manipulieren könnte. Von dem

Zeitpunkt an, an dem Funktionen der SMAERS-Komponente aufgerufen werden, werden also „härtende" Anforderungen sowohl an das Design der Software-Komponenten als auch an deren Laufzeitumgebung (inkl. sicherer Speicherplatz) definiert. Man kann sich vorstellen, wie entsprechende BSI-Dokumente ausgesehen hätten, wenn auch die technischen Anforderungen an das Aufzeichnungssystem selbst von ihm zu definieren gewesen wären. So findet aber ein „Bruch" statt: Das Aufzeichnungssystem unterliegt – ähnlich wie Software im Bereich der „privacy by design" im Datenschutzrecht – „nur" hochabstrakten Vorgaben, während im Hinblick auf die zTSE versucht wird, alle Vorgaben bis ins Detail zu regeln. Dabei liegen die Risiken aus der Perspektive der zTSE auch und gerade – nach dem Prinzip „garbage in, garbage out" – im Aufzeichnungssystem selbst. Wie oben gezeigt, enthalten die Rechtsquellen – einschließlich der AEAO – eigentlich keine ausdrückliche Grundlage, neben den Anforderungen an das Sicherheitsmodul selbst auch die Anforderungen an dessen Laufzeitumgebung zu definieren. Man könnte zwar argumentieren, dass ein Sicherheitsmodul auf einer unsicheren Laufzeitumgebung seinen Zweck nicht erfüllen kann, andererseits aber auch, dass möglicher Folgeinvestitionsbedarf aufseiten des Steuerpflichtigen, der sich aus solchen „übergriffigen" Anforderungen ergeben kann, in einem förmlichen Gesetzgebungsverfahren definiert und entschieden hätte werden müssen.

Die aktuell in der Praxis diskutierten Themen in komplexeren Setups betreffen nicht umsonst gerade die Fragen der Trennung und der Laufzeitumgebung/Virtualisierung der einzelnen Komponenten sowie der Vorgaben für den Fall des Ausfalls einer Komponente bzw. der Verbindung zwischen Komponenten.

Feinsinnig wird darüber diskutiert, in welcher Laufzeitumgebung die SMAERS-Komponente eingesetzt werden darf, ob die SMAERS-Komponente im selben Systemumfeld wie das Aufzeichnungssystem betrieben werden muss, welche Sicherheitsanforderungen an eine „Umbettung" der steuerlich relevanten Daten in ein Langzeitarchiv zu stellen sind etc. Man kann durchaus den Standpunkt vertreten, dass der Gesetzgeber und der Verordnungsgeber für eine Regelung dieser Themen „unterhalb" ihrer selbst keine Ermächtigungsgrundlage geschaffen haben, da diese Themen nicht die Anforderungen an das Sicherheitsmodul als solches betreffen (§ 5 Satz 1 Nr. 2 KassenSichV). Der Gesetzgeber hätte in § 146a Abs. 3 Satz 1 Nr. 2 lit. a AO dann besser sinngemäß die Anforderungen „an das Sicherheitsmodul, dessen Laufzeitumgebung beim Steuerpflichtigen oder einem Dritten und die Anbindung an das Aufzeichnungssystem" delegiert und damit hoffentlich im Vorfeld eine Diskussion über den damit verbundenen, enormen Folgeaufwand ausgelöst, wenn hier den Steuerpflichtigen untergesetzlich weitreichende Vorgaben gemacht werden. Auch wenn beispielsweise die steuerliche Aufbewahrungsfrist (§ 147 AO) pauschal auf 50 Jahre verlängert werden sollte, würde dies wohl im Gesetzgebungsverfahren zu einer erheblichen Diskussion über die damit verbundenen Kosten bei den Steuerpflichtigen führen.

Was lediglich in Ziff. 7 der AEAO zu § 146a „geregelt" wird, ist die Frage des temporären Ausfalls der zTSE. Dies muss keine Cloud-zTSE sein, sondern kann auch eine zTSE in Dongle- bzw. Token-Form betreffen (Hardware-Defekt etc.). Die übrigen Rechtsquellen reflektieren diese Frage nicht. Unklar ist auch, ob ein „Ausfall" dann vorliegt, wenn lediglich die Netz- bzw. Internetverbindung zum Sicherheitsmodul (oder zwischen dessen Komponenten) temporär ausfällt, nicht aber das Sicherheitsmodul selbst. Ausgehend vom rechtlichen Grundsatz, dass Unmögliches nicht gefordert werden kann, und da das Gesetz an keiner Stelle eine bestimmte Technologie oder Art der Implementierung vorschreibt (was auch verfassungsrechtlich problematisch wäre), wird man aus der abstrakten Möglichkeit solcher Verbindungsprobleme in keinem Fall die Unzulässigkeit einer Aufspaltung, Verteilung und Netzanbindung der einzelnen Komponenten der zTSE folgern können, solange die üblichen IT-Sicherheitsanforderungen an die Implementierung derartiger komplexer Systeme und ihrer Verbindungen untereinander beachtet werden. Für das Aufzeichnungssystem selbst – was immer das ist – könnten solche Vorgaben erst recht nicht gemacht werden, weil das Gesetz keine Anforderungen an dessen technische Beschaffenheit formuliert oder deren Definition delegiert.

Was bleibt

Gesetze für die „digitale Welt“ zu schreiben ist nicht einfach, zumal wenn dies im Rahmen von Steuergesetzen erfolgen soll, die letztlich von der Finanzverwaltung verfasst und von Parlamentariern verabschiedet werden, deren Kernkompetenz nicht in digitalen Datenflüssen und IT-Zusammenhängen besteht. Zudem ist das „Vorausberechnen“ von Folgen gesetzlicher Regelungen insbesondere in der „digitalen Welt“ schwierig, weil diese sich besonders komplex, schnelllebig und schlecht vorhersehbar entwickelt. Simulationen möglicher Gesetzesänderungen im Vorfeld („Planspiele“), die beispielsweise in den 2000er-Jahren im Bereich der Umsatzsteuer (Reverse Charge) durchgeführt wurden, sind aufgrund ihrer Kosten und ihres Zeitaufwands wenig geschätzt, wenn ein Vorhaben „schnell, schnell“ umgesetzt werden soll. So werden die unbekannten Folgekosten der Umsetzung stattdessen auf den Steuerpflichtigen externalisiert.

Der Implementationsaufwand des „Kassengesetzes“ für die gesamte deutsche Wirtschaft wurde in der Gesetzesbegründung mit einmalig „rund 470 Mio. Euro“ und jährlich mit „rund 106 Mio. Euro“ beziffert. Ein deutscher Parlamentarier würde bei solchen Zahlen den Gesetzesentwurf vermutlich schnell beiseitelegen, weil das pro Unternehmen eine vernachlässigbare Größenordnung bedeutet. Eine Nachschau solcher „gegriffener“ Zahlen aus der Retrospektive findet nicht statt, weil sie viel zu viel Aufwand erfordern würde, und auch die Herleitung der ursprünglichen Schätzung ist nicht transparent. Jeder, der mit dem Thema befasst ist, mag sich selbst eine Meinung darüber bilden, ob deutschlandweit der bisherige – und noch kommende – Aufwand annähernd mit dieser Schätzung korreliert, zumal, wenn man die unzähligen Gesprächsrunden zu diesem Thema in Unternehmen und Verbänden und mit Beratern als „Opportunitätskosten“ hinzuzählt. Umgekehrt, so muss man konzedieren, hat das Kassengesetz ganz neue Anbieter und Geschäftsmodelle befördert. Des einen Freud, des anderen Leid.

Wann nun – im Sinne der steuerrechtlichen Ordnungswidrigkeiten – Kassendaten präzise ausreichend „geschützt“ und Systeme „richtig verwendet“ werden, kann auch eine intensive Analyse der Rechtsquellen nicht erschöpfend beantworten. Prozesse, Datenflüsse, Komponenten und Rahmenbedingungen (wie die Laufzeitumgebung für die verschiedenen Komponenten) kann man den Rechtsquellen nicht hinreichend entnehmen.

Die für die Praxis wichtigen Strukturfragen, also wie ein verteiltes Aufzeichnungs- und Absicherungssystem aussehen darf, werden vom Gesetz- und Verordnungsgeber nicht gelöst, obwohl doch der Trend zu „verteilten Systemen“ seit Langem unübersehbar ist und die IT-Realität sich in größeren Unternehmen in gewachsenen, heterogenen Systemlandschaften unter zunehmendem (punktuellem oder flächendeckendem) Einsatz von Cloud-Diensten abspielt.

Zur Lückenfüllung legt dann das BSI notgedrungen seine Ermächtigungsgrundlagen anhand der vom BSI selbst, also aus IT-Perspektive, postulierten sachlichen Notwendigkeiten aus und entscheidet – insbesondere im Rahmen von Zertifizierungen – punktuell, was im Einzelnen gefordert wird (und das nicht immer nur anhand der allgemein verfügbaren Spezifizierungen). Das BSI wird so zum „technischen Gesetzgeber“, an den der eigentliche Gesetz- und Verordnungsgeber die Fragen auslagert, die er selbst nicht hinreichend durchdringt. Das ist einerseits gut, um dringend benötigte Digitalkompetenz in den Normsetzungsprozess einzubringen, andererseits aber schlecht, wenn die Vorgaben an das BSI, insbesondere in „investitionsintensiven“ Bereichen, nicht hinreichend präzise formuliert wurden. Weit über das Thema Kassengesetz hinaus ist dem Gesetzgeber für die Zukunft viel eigene Digitalkompetenz zu wünschen, um überhaupt mit einer Welt Schritt halten zu können, die sich zunehmend ins Digitale verlagert, darüber hinaus aber auch diese zum Nutzen aller mit gestalten zu können. ▪

Dr. Axel-Michael Wagner
Rechtsanwalt und Partner bei Peters, Schönberger & Partner

Dr. Axel-Michael Wagner beschäftigt sich u.a. mit Themen an der Schnittstelle zwischen Recht und Digitalisierung. Er berät Mandanten über die rechtliche Machbarkeit innovativer digitaler Geschäftskonzepte und über Compliance-Fragen sowie bei Unternehmenstransaktionen.