



Fiskus bittet künftig mehr zur Kasse

**– Gesetz zum Schutz vor Manipulationen an digitalen
Grundaufzeichnungen verabschiedet –**

23. Dezember 2016

Peters, Schönberger & Partner mbB

Schackstraße 2, 80539 München

Tel.: +49 89 381720

Internet: www.psp.eu

Autoreninformation:

- **Stefan Groß**, Steuerberater, Certified Information Systems Auditor (CISA),
Partner bei Peters, Schönberger & Partner
- **Max Oliver Sturm**, Master of Science,
Mitarbeiter bei Peters, Schönberger & Partner

Executive Summary

Das sogenannte „Kassengesetz“ beinhaltet im Wesentlichen die Einführung einer zertifizierten **Sicherheitseinrichtung** für elektronische Aufzeichnungssysteme und gilt insbesondere für Nutzer elektronischer Kassensysteme. Die Pflicht zur Nutzung eines elektronischen Kassensystems besteht jedoch nach wie vor nicht.

Die Definition der technischen Anforderungen an eine solche Sicherheitseinrichtung sowie deren **Zertifizierung** obliegt dem Bundesamt für Sicherheit in der Informationstechnik (BSI). Außerdem sieht das Gesetz mit der sogenannten Kassen-Nachschau ein neues Instrument für die Finanzverwaltung vor, womit die Ordnungsmäßigkeit der eingesetzten Kassensysteme spontan und unangemeldet überprüft werden kann.

Für die Implementierung bzw. Anschaffung eines gesetzeskonformen Systems bleibt den Unternehmen noch bis zum 1. Januar 2020 Zeit. Aktuellere Kassen erhalten gar noch einen Aufschub bis zum Ende des Jahres 2022. Dagegen ist eine Kassen-Nachschau bereits ab dem 1. Januar 2018 zulässig.

Hinweis: Unabhängig von der Gesetzesnovellierung sind Unterlagen, die mittels elektronischer Registrierkassen, Waagen mit Registrierkassenfunktion oder Taxametern erstellt wurden, ab dem 1. Januar 2017 für die Zeit der Aufbewahrungsfrist jederzeit verfügbar, unverzüglich lesbar sowie maschinell auswertbar aufzubewahren. Demnach sind elektronische Grundaufzeichnungen den **GoBD** entsprechend einzeln, vollständig, richtig, zeitgerecht, geordnet und unveränderbar aufzuzeichnen, sodass sich sämtliche Geschäftsvorfälle in ihrer Entstehung und Abwicklung nachverfolgen lassen.

Das **Gesetz zum Schutz vor Manipulationen an digitalen Grundaufzeichnungen** hat kurz vor dem Jahreswechsel die „Absolution“ von Bundestag und Bundesrat erhalten. Hiernach soll der Steuerpflichtige zukünftig verpflichtet sein, digitale Grundaufzeichnungen nach vordefinierten technischen Vorgaben zu machen und auf einem Speichermedium unveränderbar zu sichern. Die Notwendigkeit eines neuen Gesetzes begründet das Bundesministerium der Finanzen (BMF) insbesondere damit, dass technische Manipulationen von Kassendaten im Rahmen der steuerlichen Außenprüfung – wenn überhaupt – nur mit einem hohen Aufwand feststellbar sind. Allerdings sah sich der Gesetzgeber gezwungen, den ursprünglichen Entwurf anzupassen, hat doch gerade der Bundesrat in Abrede gestellt, dass die gesetzlich vorgesehenen Maßnahmen tatsächlich einen wirksamen Schutz vor Manipulationen an digitalen Grundaufzeichnungen bieten. Auch zahlreiche Interessengruppen und Verbände meldeten Kritik an, so wurden etwa alleine die für die deutsche Wirtschaft geschätzten Einführungskosten mit rund einer halben Milliarde Euro veranschlagt.

Der nachfolgende Beitrag stellt die Neuregelung im Detail vor und soll aufzeigen, welche Änderungen sich nicht nur für bargeldintensive Branchen ergeben werden, welches Instrumentarium der Finanzverwaltung künftig zur Verfügung steht und welche Übergangsfristen gelten.

Ausgangssituation

Die bestehenden gesetzlichen Regelungen bieten nach Ansicht des BMF keine ausreichenden Möglichkeiten, um Manipulationen bezüglich sogenannter digitaler Grundaufzeichnungen aufzudecken. Dabei geht es in erster Linie um nicht dokumentierte Stornierungen, nicht dokumentierte Änderungen mittels elektronischer Programme sowie um den gezielten Einsatz von Manipulationssoftware (z. B. Phantomware, Zapper). Gerade diese „Hilfsmittel“ würden umfassende Veränderungen und Löschungen von Daten ermöglichen. Des Weiteren könnten Daten unterdrückt, Umsatz-Kategorien gelöscht, Datenbanken inhaltlich ersetzt oder neue, nie da gewesene Geschäftsvorfälle erfasst werden. Die gesetzliche Neuregelung soll künftig derartigen Praktiken den Riegel vorschieben und dazu der Finanzverwaltung neue Prüfungsmöglichkeiten eröffnen.

1. Die Gesetzesnovellierung im Detail

Das Gesetz zum Schutz vor Manipulationen an digitalen Grundaufzeichnungen verfolgt im Wesentlichen drei Zielsetzungen:

- *Verpflichtender Einsatz einer **technischen Sicherheitseinrichtung** bei Nutzung eines elektronischen Aufzeichnungssystems*
- *Einführung einer **Kassen-Nachschau***
- ***Sanktionierung** von Verstößen*

(1) Technische Sicherheitseinrichtung, Einzelaufzeichnung und Belegausgabepflicht

Mittels einer technischen Sicherheitseinrichtung sollen dem Gesetz entsprechend elektronische Grundaufzeichnungen vor Verlust und nicht nachverfolgbaren Veränderungen geschützt und auf spezifischen Speichermedien gesichert werden. Den Kernpunkt der neuen Regelung bildet insoweit eine Ergänzung der Abgabenordnung (AO), durch die gewährleistet werden soll, dass spezifische elektronische Aufzeichnungssysteme alle Handlungen unmittelbar im Zeitpunkt des Vorgangsbeginns auf-

zeichnen und zugleich protokollieren. Als elektronische Aufzeichnungssysteme sollen ausschließlich elektronische oder computergestützte Kassensysteme und elektronische Registrierkassen gelten. Fahrscheinautomaten, Fahrscheindrucker und elektronische Buchhaltungsprogramme gehören nicht zu den elektronischen Aufzeichnungssystemen im Sinne des § 146a Abs. 1 AO. Auch Waren- und Dienstleistungsautomaten sowie Geldautomaten sollen nicht in den Anwendungsbereich der Rechtsverordnung einbezogen werden.

Konkret müssen alle elektronischen Aufzeichnungen über sämtliche nachfolgenden Prozesse in ihrer **Integrität** und **Authentizität**, einschließlich der zur maschinellen Auswertung erforderlichen Strukturinformationen bzw. der Anforderungen der digitalen Schnittstelle, vollständig erhalten bleiben. Um dies zu gewährleisten, sollen elektronische Aufzeichnungssysteme gem. § 146a Abs. 1 AO künftig durch eine **zertifizierte technische Sicherheitseinrichtung** geschützt werden, um damit die vorgenannten Manipulationen zu verhindern. Hierzu schreibt das Gesetz keine spezifische Technologie vor, sondern ist letztlich **technologieoffen** ausgelegt. Entsprechend ist davon auszugehen, dass auch das im Vorfeld viel diskutierte INSIKA-Verfahren (integrierte Sicherheitslösung für messwertverarbeitende Kassensysteme) eine zulässige Lösungsvariante darstellt, die grundsätzlich zertifizierungsfähig ist. So betonte auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) seinerzeit, dass konkrete technische Konzepte, wie die INSIKA-Technik oder bereits bestehende technische Lösungen anderer Staaten nicht im Widerspruch zu dem Zertifizierungsverfahren stünden, es bedürfe lediglich gewisser Anpassungen.

Die wesentlichen Komponenten der technischen Sicherheitseinrichtung bestehen aus einem **Sicherheitsmodul**, einem **Speichermedium** sowie einer digitalen **Schnittstelle**. Die damit einhergehenden technischen Anforderungen sollen durch das BSI bestimmt und die technische Sicherheitseinrichtung entsprechend vom BSI zertifiziert werden. Dabei sind – wie bereits aus den **GoBD** bekannt – die elektronischen Grundaufzeichnungen einzeln, vollständig, richtig, zeitgerecht, geordnet und unveränderbar aufzuzeichnen (**Einzelaufzeichnungspflicht**). Kasseneinnahmen und Kassenausgaben sind täglich festzuhalten. Soweit Verkäufe an eine Vielzahl von nicht bekannten Personen gegen Barzahlung erfolgen, soll die Pflicht zur Einzelaufzeichnung aus Zumutbarkeitsgründen jedoch entfallen. Allerdings stellt der Gesetzgeber

zugleich klar, dass bei Nutzung eines elektronischen Aufzeichnungssystems im obigen Sinne gerade keine Ausnahme von der Einzelaufzeichnungspflicht möglich ist.

Weiter wird konkretisiert, dass aufzeichnungspflichtige Geschäftsvorfälle laufend zu erfassen und einzeln festzuhalten sowie aufzuzeichnen sind, sodass sich die einzelnen Vorgänge in ihrer Entstehung und Abwicklung nachverfolgen lassen. Flankierend wurde die endgültige Gesetzesfassung durch eine **Belegausgabepflicht** ergänzt, wonach Verwender von elektronischen Aufzeichnungssystemen bzw. Registrierkassen ihren Kunden gegenüber künftig verpflichtend sind, einen Beleg über den jeweiligen Geschäftsvorfall aus- und zur Verfügung zu stellen. Der Beleg kann dabei elektronisch oder in Papierform bereitgestellt werden. Die Erstellung des Belegs muss jedoch stets in unmittelbarem zeitlichem Zusammenhang mit dem Geschäftsvorfall erfolgen. Mit der Belegausgabepflicht entsteht jedoch nicht zugleich für den Empfänger eine Pflicht zur Mitnahme des Belegs. Soweit die Leistungserbringung wiederum an eine Vielzahl von nicht bekannten Personen erfolgt, können die Finanzbehörden aus Gründen der Zumutbarkeit und Praktikabilität von der Pflicht zur Belegausgabe absehen. Hierzu ist vom Steuerpflichtigen allerdings vorab ein Antrag gemäß § 148 AO zu stellen, wobei eine etwaige Befreiung jederzeit widerrufen werden kann, insbesondere wenn Anhaltspunkte für Missbrauch vorliegen.

Schließlich sind die Grundaufzeichnungen auf einem Speichermedium zu sichern und über die Dauer der gesetzlichen Aufbewahrungsfrist verfügbar zu halten. Der Finanzverwaltung soll damit im Ergebnis die progressive und retrograde Prüfbarkeit jedes einzelnen Geschäftsvorfalles ermöglicht werden. Die progressive Prüfung beginnt beim Beleg und setzt sich über die Stufen Grundbuchaufzeichnung und Journale, Konten, Bilanz sowie Gewinn- und Verlustrechnung bis hin zur Steueranmeldung bzw. Steuererklärung fort. Die retrograde Prüfung verläuft entsprechend umgekehrt. Die progressive und retrograde Prüfung muss den **GoBD** folgend für die gesamte Dauer der Aufbewahrungsfrist und in jedem Verfahrensschritt möglich sein.

Neu hinzugekommen ist eine **Meldepflicht** für die verwendeten elektronischen Aufzeichnungs- bzw. Kassensysteme sowie die zertifizierte Sicherheitseinrichtung. Entsprechend haben Steuerpflichtige, die sich ein elektronisches Aufzeichnungssystem

anschaffen oder ein solches außer Betrieb nehmen, dies ihrem zuständigen Finanzamt innerhalb eines Monats mitzuteilen. Nach amtlichem Vordruck sind dabei Ausführungen zur Art der zertifizierten technischen Sicherheitseinrichtung, zur Anzahl der verwendeten elektronischen Aufzeichnungssysteme sowie deren Seriennummern sowie zu den Daten der Anschaffung bzw. Außerbetriebnahme zu treffen. Bereits vorhandene Systeme (bzw. Systeme, die noch vor dem 1. Januar 2020 angeschafft werden) müssen bis zum 31. Januar 2020 angezeigt werden. Von dieser Meldepflicht erhofft sich die Finanzverwaltung insbesondere Informationen, welche Systeme und Sicherheitseinrichtungen bei der risikoorientierten Fallauswahl für Außenprüfungen und bei der Prüfungsvorbereitung zur Verfügung stehen.

Hinsichtlich der **Durchführung des Gesetzes zum Schutz vor Manipulationen an digitalen Grundaufzeichnungen** wird das BMF ermächtigt, eine **technische Verordnung** zu erlassen. Als Novum wurde dabei festgelegt, dass die Rechtsverordnung nur mit Zustimmung des Bundestages erlassen werden kann. Darin soll präzisiert werden, welche elektronischen Aufzeichnungssysteme durch eine zertifizierte technische Sicherheitseinrichtung zu schützen sind und wie eine Protokollierung der elektronischen Aufzeichnungen sowie deren Speicherung erfolgen muss. Neben den Protokollierungsinhalten sind gerade die Vorgaben an die **Speicherung** der Grundaufzeichnungen von besonderem Interesse. Diese Speicherung muss manipulationssicher auf einem **nichtflüchtigen** Speichermedium erfolgen. Unter einem nichtflüchtigen Speichermedium werden Datenspeicher verstanden, deren gespeicherte Informationen auf Dauer erhalten bleiben, also auch während der Zeit, in der das elektronische Aufzeichnungssystem nicht in Betrieb ist oder nicht mit Strom versorgt wird. Dabei ist die Verfügbarkeit der gespeicherten digitalen Grundaufzeichnungen durch technische und organisatorische Maßnahmen sicherzustellen. Soweit für die Aufbewahrung ein externes elektronisches Archiv verwendet wird, muss sichergestellt sein, dass auch dieses manipulationssicher, nichtflüchtig und schnittstellenkonform ist. Letzteres betrifft die Möglichkeit, die betreffenden Daten via Schnittstelle in einer vordefinierten Datensatzbeschreibung aufzubewahren und insbesondere für Zwecke der Kassen-Nachschaue ausgeben zu können.

(2) Kassen-Nachschau

Flankierend zur technischen Sicherheitseinrichtung wird eine sogenannte Kassen-Nachschau eingeführt – die Umsatzsteuer-Nachschau lässt grüßen. Dabei ist die Kassennachschau keine Außenprüfung im Sinne des § 193 AO, sondern soll ein eigenständiges Verfahren zur zeitnahen Aufklärung steuererheblicher Sachverhalte im Zusammenhang mit der ordnungsmäßigen Erfassung von Geschäftsvorfällen mittels elektronischer Aufzeichnungssysteme oder offener Ladenkassen darstellen. Hierzu soll der zuständige Amtsträger **ohne vorherige Ankündigung** in den Geschäftsräumen des Steuerpflichtigen die Ordnungsmäßigkeit der Aufzeichnungen und Buchungen von Kasseneinnahmen und Kassenausgaben überprüfen können. Eine solche Kassen-Nachschau gem. § 146b AO ist bereits ab dem 1. Januar 2018 zulässig und damit deutlich früher, als noch im Gesetzentwurf vorgesehen. Ab dem 1. Januar 2020 erweitert sich der Prüfungsgegenstand zudem auf die Prüfung des ordnungsgemäßen Einsatzes des elektronischen Aufzeichnungssystems an sich.

Der Gesetzgeber verspricht sich von diesem Instrument, ein für mögliche Betrüger deutlich erhöhtes Entdeckungsrisiko zu schaffen. Gegenstand der Prüfung sind dabei sowohl **computergestützte Kassensysteme** und **Registrierkassen** als auch **offene Ladenkassen**. Sofern im Rahmen der entsprechenden Kassen-Nachschau Beanstandungen festgestellt werden, soll der Amtsträger nach § 146b Abs. 3 AO ohne vorherige Prüfungsanordnung unmittelbar zur Außenprüfung übergehen können. Ergänzend soll auch eine Beobachtung der Kassen und ihrer Handhabung in Geschäftsräumen, die der Öffentlichkeit zugänglich sind (auch ohne Pflicht zur Vorlage eines Ausweises), zulässig sein. Dies kann beispielsweise mittels sogenannter Testkäufe erfolgen. Die Mitwirkungspflicht des Steuerpflichtigen betrifft sowohl die Gewährung einer Einsichtnahme in die (elektronischen) Kassenaufzeichnungen und -buchungen als auch die Zurverfügungstellung der Kassenaufzeichnungen und -buchungen über die digitale Schnittstelle. Dazu sind dem Prüfer auf Anforderung auch Kassenbuchungen auf einem maschinell auswertbaren Datenträger nach den Vorgaben der digitalen Schnittstelle zur Verfügung zu stellen. Schließlich soll auf Anforderung des Amtsträgers das Zertifikat und die Systembeschreibungen zum verwendeten Kassensystem vorgelegt werden. Soweit sogenannte offene Ladenkassen Verwendung finden, soll

es dem Amtsträger zur Prüfung der ordnungsgemäßen Kassenaufzeichnungen erlaubt sein, einen sogenannten „Kassensturz“ zu verlangen sowie sich die Aufzeichnungen der Vortage vorlegen zu lassen.

Soweit die relevanten Daten bei Dritten liegen (**Outsourcing**), sieht § 147 Abs. 6 S. 3 AO vor, dass diese Dritten der Finanzbehörde im Rahmen einer Außenprüfung oder einer Kassen-Nachschau Zugriff auf die aufzeichnungspflichtigen Daten des Steuerpflichtigen zu gewähren haben oder der Finanzbehörde die für den Steuerpflichtigen gespeicherten Unterlagen und Aufzeichnungen auf einem maschinell verwertbaren Datenträger zur Verfügung stellen müssen.

(3) Sanktionierungsmaßnahmen

Werden Verstöße gegen die neuen Verpflichtungen zur ordnungsgemäßen Nutzung der technischen Sicherheitseinrichtung festgestellt, können diese als Steuerordnungswidrigkeit mit einer Geldbuße von bis zu 25.000 Euro geahndet werden, unabhängig davon, ob ein steuerlicher Schaden entstanden ist. Eine entsprechende Sanktionierung soll in folgenden Fällen greifen:

- **Einsatz** eines technischen Systems, das nicht den Anforderungen des § 146a Abs. 1 AO entspricht,
- **Fehlen** oder **fehlerhafte Verwendung** einer zertifizierten technischen Sicherheitseinrichtung in elektronischen Aufzeichnungssystemen oder
- **Inverkehrbringen** oder **Bewerbung** elektronischer Aufzeichnungssysteme, technischer Sicherheitseinrichtungen oder sonstiger Software, die nicht jeden einzelnen Geschäftsvorfall vollständig, richtig, zeitgerecht und geordnet erfassen bzw. die die Möglichkeit eröffnen, nachträglich nicht nachvollziehbar steuerrelevante Daten zu verändern, zu löschen oder zu unterdrücken.

Von einer Sanktionierung sollen Fälle ausgenommen sein, welche bereits nach § 378 AO geahndet werden können.

2. Inkrafttreten der Neuregelungen

Entgegen der im Referentenentwurf vorgesehenen erstmaligen Anwendung für Wirtschaftsjahre, die nach dem 31.12.2018 beginnen, findet das Gesetz nun **erstmalig Anwendung ab dem 1. Januar 2020**. Somit bleibt den Unternehmen ein Jahr mehr Zeit für die Implementierung bzw. Anschaffung eines gesetzeskonformen Systems.

Aktuellere Registrierkassen erhalten vom Gesetzgeber gar noch einen Aufschub bis zum Ende des Jahres 2022. Diese verlängerte Übergangsregelung gilt für alle Kassensysteme, die nach dem 25. November 2010 und vor dem 1. Januar 2020 angeschafft wurden. Allerdings müssen diese den Anforderungen des BMF-Schreibens vom 26. November 2010 (BStBl. I S. 1342) entsprechen und dürfen bauartbedingt nicht aufrüstbar sein.

Hinweis: Bereits zum 31. Dezember 2016 lief die Übergangsfrist des BMF-Schreibens vom 26. November 2010 zur Aufbewahrung digitaler Unterlagen bei Bargeschäften ab. Unterlagen, die mittels elektronischer Registrierkassen, Waagen mit Registrierkassenfunktion oder Taxametern erstellt wurden, müssen ab dem 1. Januar 2017 für die Zeit der Aufbewahrungsfrist jederzeit verfügbar, unverzüglich lesbar sowie maschinell auswertbar aufbewahrt werden. Demnach sind elektronische Grundaufzeichnungen einzeln, vollständig, richtig, zeitgerecht, geordnet und unveränderbar aufzuzeichnen, sodass sich sämtliche Geschäftsvorfälle in ihrer Entstehung und Abwicklung nachverfolgen lassen.

PSP-Kommentar:

Auch wenn die längeren Übergangsfristen durchweg positiv zu werten sind, muss nach wie vor das vom Gesetzentwurf propagierte Zertifizierungsverfahren kritisch hinterfragt werden, insbesondere was die erforderliche Zertifizierungsfrequenz angeht. Der Gesetzgeber erhebt dementsprechend den Anspruch, dass die Zertifizierung „fortlaufend aufrechtzuerhalten“ sei. Dazu führt der vorliegende Entwurf zur technischen Verordnung aus, dass für Fälle, in welchen eine zertifizierte technische Sicherheitseinrichtung durch ein **Update im sicherheitsrelevanten Bereich** modifiziert oder sonstige Änderungen des sicherheitsrelevanten Bereichs der zertifizierten

Sicherheitseinrichtung vorgenommen werden, die Zertifizierung **automatisch erlischt**. Vor dem Hintergrund stetig abnehmender IT-Halbwertszeiten wird es dementsprechend entscheidend um die Frage gehen, was als sicherheitsrelevanter Bereich zu qualifizieren ist. Dies ist umso wichtiger, als ansonsten jegliche Updates, welche heute nahezu an der Tagesordnung sind, einen neuen vollumfänglichen Zertifizierungsbedarf und damit erhebliche Kosten auslösen würden.

So gab auch der Deutsche Industrie- und Handelskammertag (DIHK) in seiner Stellungnahme zu Recht zu bedenken, dass mit den Umrüstungsmaßnahmen und dem erhöhten bürokratischen Aufwand in erster Linie steuererliche Unternehmen belastet würden. Dabei hat die Bedeutung von Programmänderungen auch bereits die Gerichte beschäftigt. So kommt der BFH in seinem Urteil vom 25. März 2015 zum Ergebnis, dass bei einem programmierbaren Kassensystem bereits das Fehlen der Protokolle nachträglicher Programmänderungen einen formellen Mangel darstellt, der grundsätzlich für sich genommen zu einer Hinzuschätzung berechtigt.

Alleine also die Prüfung, ob bzw. in welcher Intensität eine Rezertifizierung geboten ist, dürfte den Beteiligten nicht unerhebliche Ressourcen abverlangen, deren Finanzierung letztlich wohl die Unternehmen tragen müssen. Dabei hängt die Eignung von Sicherheitsmaßnahmen stark davon ab, welchem Angriffspotenzial die jeweilige Lösung ausgesetzt ist. So führt das BSI in seiner Stellungnahme zu Recht aus, dass Angriffe auf technische Systeme in der Regel Schwachstellen nutzen, die nicht selten auf Fehler in der Implementierung oder auf die mangelhafte Umsetzung von Sicherheitsmaßnahmen zurückzuführen sind. Deshalb sind nach Meinung des BSI auch unabhängige und systematische Prüfungen sowie die Bestätigung des erforderlichen Sicherheitsniveaus durch ein standardisiertes Zertifizierungsverfahren unabdingbar.

Aber auch die Vorgaben an die **Speicherung** werfen Fragen auf, bspw. hinsichtlich der Definition eines „nichtflüchtigen Datenträgers“, auf dem die elektronischen Grundaufzeichnungen gemäß dem Entwurf der technischen Verordnung gespeichert werden sollen. Dies gilt umso mehr, als die Verpflichtung, elektronische Aufzeichnungen zu sichern und für Prüfungen verfügbar zu halten, auch vorsieht, dass bei einem Verkauf oder einer Verschrottung des elektronischen Aufzeichnungssystems

die elektronischen Aufzeichnungen für die Dauer der Aufbewahrungsfristen auf einem (anderen) Speichermedium zu sichern und verfügbar zu halten sind. In Anknüpfung an die GoBD könnte sich hier die Forderung verbergen, dass die bloße Ablage in einem **Dateisystem** nicht ausreicht, wenn nicht weitere Maßnahmen getroffen werden. Welche Maßnahmen dies im Einzelnen sind, lassen sowohl das vorliegende Gesetz als auch die GoBD weitgehend offen. Gerade mit Blick auf die Sanktionierung von Verstößen bedürfte es hier zwingend einer Präzisierung, welche zugleich im Umfeld der GoBD für mehr Klarheit sorgen würden.

3. Fazit

Es steht außer Zweifel, dass der Fiskus – letztlich auch im Interesse aller steuerrechtlichen Unternehmen – gegen vorsätzliche Steuerhinterziehung vorgehen muss. In bargeldintensiven Branchen sind Fiskalspeicher hierfür sicherlich ein probates Mittel. Allerdings darf dies nicht dazu führen, den Unternehmen unverhältnismäßig hohe Lasten aufzuerlegen. So bedarf es – mit oder ohne INSIKA – zwingend einer Präzisierung des Zertifizierungsprozederes, gerade was den Prüfungsgegenstand und das Erfordernis einer Rezertifizierung angeht. Kontraproduktiv wirken dabei die Verwendung neuer bzw. die Neudefinition feststehender Begrifflichkeiten, wie etwa „nichtflüchtige Datenträger“ oder auch „elektronische Archivierung“. Dazu bedarf es zwingend der Präzisierung der technischen Vorgaben in Bezug auf die Verwendung zulässiger Speichersysteme. Ansonsten stellt sich die Aufbewahrung schnell als Vabanquespiel mit unkalkulierbarem Ausgang dar. Gut, dass die verlängerten Übergangsvorschriften hier genügend Zeit zur Präzisierung bieten.

Aber vielleicht ist dies auch nur noch Makulatur, wenn die vielfach kolportierten Überlegungen zur Abschaffung des Bargeldsektors bis dahin zur „Orwellischen Realität“ werden. Oder aber es ist der Aufgalopp zur „Fiscal-Cloud“, die jeden Umsatz digital speichert und im Hinblick auf eine korrekte steuerliche Behandlung validiert – die Systeme zur Meldung umsatzsteuerpflichtiger Umsätze in Südamerika lassen grüßen.

Die vorliegenden Ausführungen geben die persönliche Meinung der Autoren zur derzeitigen Rechtslage wieder und enthalten lediglich einen Überblick über einzelne Themenkomplexe. Spezielle Umstände einzelner Fallkonstellationen wurden nicht berücksichtigt; diese können durchaus zu abweichenden Betrachtungsweisen und/oder Ergebnissen führen. Die dargestellten Ausführungen können daher keine rechtliche oder steuerliche Beratung ersetzen; bitte holen Sie eine auf Ihre Umstände zugeschnittene, weitere Entwicklungen berücksichtigende Empfehlung Ihres Steuerberaters oder Wirtschaftsprüfers ein, bevor Sie Entscheidungen über die in diesen Ausführungen betrachteten Themen treffen. Die Finanzverwaltung und/oder Gerichte können abweichende Auffassungen zu den hier behandelten Themen haben oder entwickeln.