PSP

MÜNCHEN

Fiskus sagt Kassenmanipulation den Kampf an

– Eine erste Analyse zum Entwurf eines Gesetzes zum Schutz vor Manipulationen an digitalen Grundaufzeichnungen –

21. März 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*

Im Kampf gegen manipulierte Kassensysteme will der Gesetzgeber nun ernst machen und hat hierzu mit Datum vom 18. März 2016 den Referentenentwurf eines ***„Gesetzes zum Schutz vor Manipulationen an digitalen Grundaufzeichnungen"*** nebst dem ***Entwurf einer technischen Verordnung*** vorgelegt. Hintergrund sind die in den letzten Jahren bekannt gewordenen Fälle manipulativer Eingriffe in Kassensysteme, die auch bereits Gegenstand von sowohl steuerrechtlicher als auch strafrechtlicher höchstrichterlicher Rechtsprechung waren (vgl. insbesondere BFH vom 25. März 2015 – X R 20/13; BGH vom 27. Oktober 2015 1 StR 373/15). 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. Die bestehenden gesetzlichen Regelungen bieten hier nach Ansicht des BMF keine ausreichenden Möglichkeiten, um Manipulationen bzgl. sog. digitaler Grundaufzeichnungen aufzudecken. Dabei richtet sich das Augenmerk auf nicht dokumentierte Stornierungen, nicht dokumentierte Änderungen mittels elektronsicher Programme sowie auf den gezielten Einsatz von Manipulationssoftware (z. B. Phantomware, Zepper). Dies würde 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 derartigen Manipulationen den Riegel vorschieben und dazu der Finanzverwaltung neue Prüfungsmöglichkeiten eröffnen. Hierzu soll der Steuerpflichtige nach § 146a Absatz 1 Satz 4 AO zukünftig verpflichtet sein, digitale Grundaufzeichnungen nach vordefinierten technischen Vorgaben aufzuzeichnen und auf einem Speichermedium unveränderbar zu sichern. Allerdings bergen die Maßnahmen ein nicht unerhebliches steuerliches und IT-technisches Konfliktpotenzial. Alleine die für die deutsche Wirtschaft geschätzten Einführungskosten i. H. v. rund einer halben Milliarde Euro rechtfertigen es, den Gesetzentwurf etwas näher zu beleuchten. Das Rahmenwerk bilden dabei die ***Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)*** vom 14. November 2014. Der Gesetzentwurf nebst technischer Verordnung soll damit insbesondere die sich aus den GoBD ergebenden Anforderungen technisch absichern.

Der Referentenentwurf verfolgt im Wesentlichen drei Zielsetzungen:

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

Technische Sicherheitseinrichtung

Mittels einer technischen Sicherheitseinrichtung sollen dem Gesetzentwurf entsprechend elektronische Grundaufzeichnungen vor Verlust und nicht nachverfolgbaren Veränderungen geschützt und auf spezifischen Speichermedien gesichert werden. Den Kernpunkt des Referentenentwurfs bildet insoweit eine Ergänzung der Abgabenordnung (AO), durch die gewährleistet werden soll, dass spezifische elektronische Aufzeichnungssysteme alle Handlungen unmittelbar im Zeitpunkt des Vorgangsbeginns aufzeichnen und zugleich protokollieren. Konkret müssen alle elektronischen Aufzeichnungen über alle 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 künftig durch eine ***zertifizierte technische Sicherheitseinrichtung*** geschützt werden, um damit die vorgenannten Manipulationen zu verhindern. Die wesentlichen technischen Komponenten bestehen dabei aus einem ***Sicherheitsmodul***, einem ***Speichermedium*** sowie einer digitalen ***Schnittstelle***. Die damit einhergehenden technischen Anforderungen sollen durch das Bundesamt für Sicherheit in der Informationstechnik (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***). 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. 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 Geschäftsvorfalls 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.

Über eine geplante ergänzende ***Technische Verordnung zur Durchführung des Gesetzes zum Schutz vor Manipulationen an digitalen Grundaufzeichnungen*** soll zudem 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 Gundaufzeichnungen 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-Nachschau ausgeben zu können.

Kassen-Nachschau

Flankierend zur technischen Sicherheitseinrichtung soll – die Umsatzsteuer-Nachschau lässt grüßen – eine sog. Kassen-Nachschau eingeführt werden. 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. Der Gesetzgeber beabsichtigt dadurch ein für mögliche Betrüger deutlich erhöhtes Entdeckungsrisiko zu schaffen. Gegenstand der Prüfung sind dabei sowohl ***computergestützte Kassensysteme***, ***Registrierkassen*** als auch offene ***Ladenkassen***. Sofern im Rahmen der entsprechenden Kassen-Nachschau Beanstandungen festgestellt werden, soll der Amtsträger nach § 146b Absatz 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 auch mittels sog. 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 sog. offene Ladenkassen Verwendung finden, soll es dem Amtsträger zur Prüfung der ordnungsgemäßen Kassenaufzeichnungen erlaubt sein, einen sog. „Kassensturz“ zu verlangen sowie sich die Aufzeichnungen der Vortage vorlegen zu lassen. Soweit die relevanten Daten bei Dritten (***Outsourcing***) liegen, sieht § 147 Abs. 6 S. 2 AO vor, dass der Dritte der Finanzbehörde im Rahmen einer Außenprüfung oder einer Kassen-Nachschau Zugriff auf die aufzeichnungspflichtigen Daten des Steuerpflichtigen zu gewähren hat oder der Finanzbehörde die für den Steuerpflichtigen gespeicherten Unterlagen und Aufzeichnungen auf einem maschinell verwertbaren Datenträger zur Verfügung stellen muss.

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* ***Erwerb*** *elektronischer Aufzeichnungssysteme, technischer Sicherheitseinrichtungen oder sonstiger Software, die nicht jeden einzelnen Geschäftsvorfall vollständig, richtig, zeitgerecht und geordnet erfasst bzw. die die Möglichkeit eröffnet, 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.

PSP-Kommentar:

Es ist durchaus überraschend, dass sich das von Ländern und der Steuergewerkschaft favorisierte ***INSIKA***-Konzept (integrierte Sicherheitslösung für messwertverarbeitende Kassensysteme) nicht durchsetzen konnte und insoweit auch nicht weiter verfolgt werden soll. Dies wird insbesondere damit begründet, dass die hierfür verwendete Smartcard derzeit nicht den europäischen Sicherheitsanforderungen entspräche und das Konzept zudem hinsichtlich der Smartcard-Vergabe und der Verwaltung der Smartcards im Unternehmen sehr aufwendig sei. Weiterhin würde das Konzept nicht unerhebliche rechtliche Risiken und Kosten hinsichtlich der Einbindung der autorisierten Stelle, der technischen Umsetzung der Schnittstelle zum Bundeszentralamt für Steuern sowie der Weitergabe der Profile der Finanzverwaltung mit sich

bringen. Im Ergebnis sei das INSIKA-Konzept kostenintensiver für die Wirtschaft, als das nun angestrebte Zertifizierungsverfahren.

Allerdings muss u. E. auch das nun angestrebte Zertifizierungsverfahren kritisch hinterfragt werden. Insbesondere den begründenden Ausführungen, dass ein Sicherheitsmodul nur einmal zertifiziert werden muss, kann u. E. nicht gefolgt werden. Soweit eine ***Zertifizierung*** – insbesondere im Kontext von Software – vorgenommen wird, kann sich diese immer nur auf den geprüften Release-Stand der Software beziehen. Sobald Änderungen jedweder Art an der Software vorgenommen werden, verliert das Zertifikat zwangsläufig seine Gültigkeit, ansonsten bedürfte der Prüfer geradezu hellseherische Fähigkeiten betreffend der künftigen Funktionsweise nach weiteren Releases. Und so führt auch die Begründung zur vorliegenden 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. 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.

Aber auch die Vorgaben an die ***Speicherung*** werfen Fragen auf, insbesondere hinsichtlich der Definition eines „nichtflüchtigen Datenträgers“. Dies gilt umso mehr, als die Verpflichtung die elektronischen Aufzeichnungen zu sichern und für die Prü-

fung 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, lässt sowohl der vorliegende Gesetzesvorschlag 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.

Fazit

Es steht außer Zweifel, dass der Fiskus – letztlich auch im Interesse aller steuerehrlichen Unternehmen – gegen vorsätzliche Steuerhinterziehung vorgehen muss. Im Bereich bargeldintensiver Branchen sind Fiskalspeicher hierfür sicherlich ein probates Mittel. Allerdings darf dies nicht dazu führen, den Unternehmen unverhältnismäßig hohe Lasten aufzuerlegen. So bedarf es 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. Insoweit ist zumindest gut daran getan, die dargestellte Novellierung erstmals für Wirtschaftsjahre anzuwenden, die nach dem 31. Dezember 2018 beginnen. Aber vielleicht ist dies dann auch Makulatur, wenn die vielfach kolportierten Überlegungen zur Abschaffung des Bargeldsektors bis dahin zur „Orwellschen Realität" werden.

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 besprochenen Themen treffen. Die Finanzverwaltung und/oder Gerichte können abweichende Auffassungen zu den hier behandelten Themen haben oder entwickeln.