PSP

MÜNCHEN

Fiskus bittet zur Kasse

– Gesetzentwurf gegen Kassenmanipulationen geht in die nächste Runde –

7. November 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, Peters, Schönberger & Partner*

Zur Bekämpfung manipulierter Kassensysteme hatte der Gesetzgeber mit Datum vom 18. März 2016 den Referentenentwurf eines ***„Gesetzes zum Schutz vor Manipulationen an digitalen Grundaufzeichnungen"*** nebst dem ***Entwurf einer technischen Verordnung*** vorgelegt. Hiernach soll der Steuerpflichtige zukünftig verpflichtet sein, digitale Grundaufzeichnungen nach vordefinierten technischen Vorgaben aufzuzeichnen 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. Vor dem Hintergrund des bereits im Detail ausformulierten Gesetzesvorschlags war es umso erstaunlicher, dass der ***Bundesrat*** mit Stellungnahme vom 23. September 2016 die geplante gesetzliche Umsetzung als nicht geeignet ansieht, um die gesteckten Ziele zu erreichen. Mit dem Gesetzentwurf werde kein fertig entwickeltes Verfahren vorgeschlagen, sondern lediglich allgemein gehaltene Anforderungen formuliert. Dem Entwurf mangele es an entscheidenden Komponenten für einen wirksamen Schutz vor Manipulationen an digitalen Grundaufzeichnungen, wie einer Belegausgabepflicht oder einer zentralen Registrierung der zu verwendenden Sicherheitseinrichtungen sowie an Offenheit gegenüber bereits etablierten Technologien.

Die Gegenäußerung der ***Bundesregierung*** ließ nicht lange auf sich warten. Mit Datum vom 12. Oktober 2016 verteidigte diese den ursprünglichen Gesetzentwurf. Insbesondere widerspricht die Bundesregierung dem Bundesrat bezüglich der von ihm beanstandeten fehlenden Technologieoffenheit mit der Begründung, dass auch die von vielen propagierte ***INSIKA***-Technik (integrierte Sicherheitslösung für messwertverarbeitende Kassensysteme) grundsätzlich zertifizierungsfähig und damit zulässig sei. Egal, für welchen Lösungsweg man sich letztlich entscheiden wird, die entsprechenden Maßnahmen bergen 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 und die angemahnten Alternativen etwas näher zu beleuchten. Der nachfolgende Beitrag stellt die unterschiedlichen Sichtweisen gegenüber und soll dem Leser damit einen Überblick zum Stand des Gesetzgebungsverfahrens und möglichen Gesetzesänderungen geben.

Ausgangssituation

Die bestehenden gesetzlichen Regelungen bieten nach Ansicht des BMF keine ausreichenden Möglichkeiten, um Manipulationen bzgl. sog. 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. Eine gesetzliche Neuregelung soll künftig derartigen Praktiken den Riegel vorschieben und dazu der Finanzverwaltung neue Prüfungsmöglichkeiten eröffnen.

1. Der Referentenentwurf vom 18. März 2016

Der Referentenentwurf des Gesetzgeber 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.

2. Stellungnahme des Bundesrates vom 23. September 2016

Am 23. September 2016 hat der Bundesrat zu dem dargestellten Gesetzesentwurf Stellung genommen. Auch wenn der Bundesrat die Gesetzesinitiative ausdrücklich begrüßt, erachtet er die Umsetzung im vorliegenden Entwurf als ungeeignet, um die gesteckten Ziele zu erreichen. Der Bundesrat kritisiert dabei, dass der Gesetzesentwurf kein fertig entwickeltes Verfahren präsentiere, sondern lediglich allgemein gehaltene Anforderungen formuliere, deren Konkretisierung durch das Bundesamt für Sicherheit in der Informationstechnik erfolgen solle. Außerdem weise der Entwurf zwei gravierende konzeptionelle Mängel auf – er beinhalte weder eine Belegausgabepflicht noch eine zentrale Registrierung der Sicherheitskomponenten. So könne kein wirksamer Schutz gegen Manipulationen an digitalen Grundaufzeichnungen erreicht werden. Lediglich nachträgliche Manipulationen, bspw. mithilfe sog. Zapperprogramme, könnten dadurch verhindert werden. Gegen die Verwendung von „Zweitkassen", deren Daten an der Buchhaltung „vorbeilaufen", oder die schlichte Nichteingabe von Geschäftsvorfällen seien die im Gesetzentwurf niedergelegten Maßnahmen machtlos. Daher seien eine Belegausgabepflicht sowie eine zentrale Registrierung der Sicherheitskomponenten unverzichtbare „Waffen" im Kampf gegen derartige Betrugsszenarien. Ferner kritisiert der Bundesrat, dass der Gesetzesentwurf Sicherungsverfahren ausschließlich für Registrierkassen vorsieht, Manipulationen jedoch in allen bargeldintensiven Bereichen stattfinden würden. Dazu ließe der Gesetzentwurf die Offenheit gegenüber bereits etablierten Technologien, wie dem INSIKA-Verfahren vermissen. Die Anforderungen des Bundesrats zielen im Kern darauf ab:

- den Gesetzentwurfs um ein Verfahren auf der Basis eines Schutzsystems mit standardisierten Signaturerstellungseinheiten zu erweitern und
- vorgesehene Sicherungsverfahren auf sämtliche elektronische oder computergestützte Systeme, mit denen aufbewahrungspflichtige Grundaufzeichnungen geführt werden können (u. a. Taxameter, Wegstreckenzähler, Geldspielgeräte, Warenautomaten, Waagen mit Registrierkassenfunktion), anzuwenden.

Zuletzt sollte die Kassen-Nachschau auf einfach überprüfbare Merkmale abzielen, um keinen unangemessenen Zeitaufwand auszulösen. Eine erweiterte Übergangsfrist hält der Bundesrat für nicht erforderlich, würde dies doch gerade die Möglichkeit eröffnen, Manipulationssoftware noch länger einzusetzen.

3. Gegenäußerung der Bundesregierung vom 12. Oktober 2016

Auf die beschriebene Kritik des Bundesrates reagierte die Bundesregierung ihrerseits am 12. Oktober 2016 und verteidigt darin ihren Vorschlag einer Belegausgabe auf Verlangen, da ihres Erachtens nach auch eine Belegausgabepflicht nicht verhindern könne, dass sich Steuerpflichtiger und Kunde im Voraus abstimmen, keinen Beleg zu erstellen. Auf die Forderung des Bundesrates, die verwendeten Sicherheitseinrichtungen zentral registrieren zu lassen, entgegnet die Bundesregierung, dass dies nicht erforderlich und zudem sehr aufwändig sei. Hersteller von Sicherheitseinrichtungen sollten stattdessen Möglichkeiten schaffen, die eine Zuordnung zwischen personalisierter Sicherheitseinrichtung und des „dazugehörigen" Steuerpflichtigen erlauben. Hinsichtlich der Umgehungsszenarien „Nichterfassung" und „Verwendung einer Zweitkasse" ist die Bundesregierung der Auffassung, dass das neue Kontrollinstrument der Kassen-Nachschau mit der Möglichkeit der unangekündigten Überprüfung ein ausreichendes Entdeckungsrisiko schaffen würde. Auch widerspricht die Bundesregierung dem Bundesrat bezüglich der von ihm beanstandeten fehlenden Technologieoffenheit mit der Begründung, dass auch die INSIKA-Technik grundsätzlich zertifizierungsfähig und damit zulässig sei. Dem Anliegen des Bundesrats, den Geltungsbereich auf alle kassenähnlichen Systeme auszudehnen, soll ggf. im Rahmen der im Anschluss an das Gesetzgebungsverfahren zu erlassenden Rechtsverordnung Rechnung getragen werden.

PSP-Kommentar:

Es war durchaus überraschend, dass sich das von Ländern und der Steuergewerkschaft favorisierte ***INSIKA***-Konzept zunächst nicht durchsetzen konnte. Inzwischen zeichnet sich nun ein Kompromiss ab, in welchem auch INSIKA seine Daseinsberechtigung haben dürfte. So betont das BSI in seiner Stellungnahme, dass auch 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. Nach wie vor muss dabei jedoch insbesondere das vom Gesetzentwurf propagierte 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. So gibt 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 steuerehrliche 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 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, insbesondere hinsichtlich der Definition eines „nichtflüchtigen Datenträgers“. 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 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 – 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.

Aber vielleicht ist dies auch nur noch Makulatur, wenn die vielfach kolportierten Überlegungen zur Abschaffung des Bargeldsektors bis dahin zur „Orwellschen Realität“ werden. Oder aber es ist der Aufgalopp zur „Fiskal-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.