KAMMER DER
WIRTSCHAFTSTREUHÄNDER

Unser Zeichen 2015/KG

Sachbearbeiter Mag.Goldhahn/CS

Telefon +43 | 1 | 811 73-250

eMail goldhahn@kwt.or.at

Datum 22. Juli 2015

BUNDESMINISTERIUM FÜR FINANZEN
BMF – IV/2
z.H. Herrn Mag. Alfred Hacker
Johannesgasse 5
1010 Wien

Stellungnahme zum Entwurf der Registrierkassensicherheitsverordnung

Sehr geehrter Herr Mag. Hacker,

die Kammer der Wirtschaftstreuhänder dankt für die Einladung zur Abgabe einer Stellungnahme zur Registrierkassensicherheitsverordnung und begrüßt die Schnelligkeit, mit der dieser VO-Entwurf zu einer durchaus schwierigen Materie vorgelegt werden konnte.

Präambel

Vorweg dürfen wir zweierlei festhalten:

- Wünschenswert wäre eine „systemoffene Lösung“ um derart die Rechtssicherheit zu erhöhen. Das bedeutet, dass keine starre Bindung an eine ganz bestimmte Technik vorgegeben wird, sondern gleichwertige Modelle in der Umsetzung nebeneinander zulässig sein können.
- Bei allem Verständnis für die technische Komplexität sollten die Begriffserläuterungen in der Verordnung noch ausgebaut werden, um die Lesbarkeit und Handhabbarkeit auch und eben für die Normunterworfenen sicherzustellen.

Als unabdingbarer Grundsatz muss jedenfalls gelten: Die Rechtssicherheit von Manipulationsschutzsystemen ist rundum zu gewährleisten!

  - Auch ein Zusatznutzen der Kassensysteme für Unternehmen soll möglich sein.
  - Dadurch wird die Steuermoral erhöht. Dies führt zu freiwilligen Budgetbeiträgen.
  - Vorhandene Systeme sollen mit dem BMF abgestimmt werden können und dementsprechend akzeptiert sein.
  - Nur diese Voraussetzungen ermöglichen den Unterhalt kostengünstiger und optimal auf die einzelnen Betriebe abgestimmter Systeme.

In diesem Sinne dürfen wir darauf aufmerksam machen, dass folgender Änderungsbedarf besteht, um die Umsetzbarkeit in der Praxis zu ermöglichen:

- Keine Verpflichtung zu Hardware wie Chipkarten, Kartenleser oder HSM!
- Software-Signaturerstellungseinheiten können ebenso sicher und besser kontrollierbar verwendet werden.
- Systemoffenheit für App- und Cloud-Lösungen mittels Softwarelösung
- Nutzung eines „fortgeschrittenen elektronischen Siegels“ gemäß der EU-Verordnung 910/2014
- Signaturerstellungseinheit mit erweiterter Funktionalität wie Summenzähler und laufender Belegnummernerteilung
- Die Regelung für geschlossene Gesamtsysteme, einen Feststellungsbescheid zu erwirken, soll auch für weit verbreitete Manipulationsschutzsysteme anwendbar sein. Diese Systeme können dadurch auch bei kleinen Unternehmen als rechtssicher verwendbar gelten.
- Die Zeitpunkte des Inkrafttretens sollten vorgezogen werden, um die Notwendigkeit des mehrmaligen Umrüstens zu vermeiden. Der Jahresbeginn 2016 erscheint deshalb zu früh gewählt, weil der Anschluss an das FON-System erst zur Mitte dieses Jahres möglich sein soll. Am besten wäre es, wenn die FON-Verbindung schon mit 01.10.2015 bereitstünde, um dementsprechende Rechtssicherheit in Vorbereitung auf den 01.01.2016 zu gewährleisten.

Allgemeines

Entsprechend den Ausführungen in der Präambel ist derzeit die Verständlichkeit der geplanten VO zu bezweifeln. Damit ist aber die Gesetzes- bzw Verfassungskonformität der Verordnung insgesamt fraglich (vgl VfGH 14.3.1997, G392/96; G398/96; G399/96: „*Im Lichte der Rsp des VfGH liegt in §109a Abs. 3 Z 2 EStG eine verfassungswidrige Regelung vor, die selbst mit Fleiß, Sorgfalt, Sachkenntnis und einer gewissen Freude an der Lösung von Denksportaufgaben nicht in ihrem Regelungsgehalt erkennbar bzw interpretierbar wird*“).

Dazu kommt noch, dass die VO Vorgaben enthält, auf deren Erfüllung der betroffene Unternehmer keinen Einfluss hat, weil sie den Manipulationsschutz betreffen, der von einem anderen – dem Hersteller, nicht von ihm als den bloßen Anwender zu bewerkstelligen ist. § 1 der RKS-V weist eindeutig in diese Richtung, wenn dort bspw von der „technischen Umsetzung der Manipulationssicherheit“, „erforderlichen technischen Merkmalen der Registrierkasse“ oder der „Kommunikation zwischen Registrierkasse und Signaturerstellungseinheit“ die Rede ist.

Zu § 1

Es stellt sich die grundsätzliche Frage „Was ist eine Registrierkasse“? Dementsprechend sollte der Begriff näher definiert werden.

Zu § 3 Z 2

Der Verweis sollte richtigerweise auf „§ 131 b Abs. 1 Z **3** BAO“ lauten. Auch wäre ausdrücklich sicherzustellen, dass Sendungen per Nachnahme bzw. Inkassos durch Dritte nicht als Barumsätze gelten.

Zu § 3 Z 3

Der Begriff „Eckdaten“ sollte wegen seiner untechnischen Allgemeinheit durch einen (präzisen) Verweis auf § 18 Abs. 2 ersetzt werden.

Weiters: Wem ist die „Datenbank“ zugänglich und wie kann der Einzelne die Richtigkeit der dort gespeicherten Daten überprüfen (lassen)? Ein gangbarer Weg könnte die Implementierung des Auskunftsrechts nach § 26 DSG 2000 sein. Ein entsprechender Hinweis samt Bekanntgabe der Stelle, wo abgefragt werden kann, wäre zweckmäßig.

Zu § 3 Z 4 – Datenerfassungsprotokoll

Das Datenerfassungsprotokoll (DEP) wird in der KRL 2012 für die beispielhafte Protokollierung nach § 131 Abs. 1 Z 6 BAO verwendet. Bei Typ-2-Kassen wird dieses Protokoll als „elektronisches Journal“ bezeichnet. Die Verträglichkeit“ der RKS-V mit der KRL 2012 sollte überlegt werden. Da diese so sicher nicht mehr gegeben ist, wird empfohlen, die KRL 2012 zur Gänze aufzuheben.

Zu § 3 Z 8 – Geschlossenes Gesamtsystem

Nicht jedes geschlossene System fällt darunter. Die Zahl „500“ erscheint sachlich nicht nachvollziehbar; ausreichend müsste vielmehr sein, dass ein System als solches „geschlossen“ ist

Außerdem erscheint fraglich, warum an dieser Stelle der Begriff „Kassensysteme“ verwendet wird. Unter „Registrierkassen“ ist nach der KRL 2012 richtigerweise eine Typ-2-Kasse zu verstehen. Daher sollte der Ausdruck „Registrierkasse“ in der gesamten RKS-V durch „Kassensystem“ ersetzt werden. Vermutlich werden die Kassensysteme in einem geschlossenen Gesamtsystem in vielen Fällen nicht mit den Warenwirtschafts-, oder Buchhaltungs-Systemen über direkte Schnittstellen (lückenlos) verbunden sein. Daher sollte dies kein Erfordernis für ein „geschlossenes System“ sein und gestrichen werden.

Zu § 3 Z 10 – Hardware-Sicherheitsmodul (HSM)

Es ist unklar, wie eine qualifizierte (elektronische) Signatur ohne persönliche Autorisierung (z.B. Pin) erstellt werden soll. Durch die Erwähnung eines „Hardware-Sicherheitsmoduls (HSM)“ entsteht der Eindruck, dass jedenfalls eine Hardware-Komponente erforderlich sein soll. Dies entspricht aber keinesfalls den politischen Aussagen und damit Willensäußerungen zur „Systemoffenheit“ und ist außerdem in der Praxis kaum praktikabel umsetzbar. Viele Unternehmen würden dadurch keine kostengünstigen Kassensysteme betreiben können bzw. wären im Arbeitsablauf praktisch nahezu unzumutbar eingeschränkt.

Zu § 3 Z 16 – Object Identifier (OID)

Problematisch erscheint, dass die Zertifikate der jeweiligen natürlichen Person (Kassiererin im Supermarkt) zugeordnet sein müssen. Der OID ordnet hingegen Zertifikate den einzelnen Unternehmen zu.

Zu § 3 Z 18 – Registrierkasse (auch elektronische Registrierkasse)

Was gilt für Preisabfragen bei elektronischen Waagen? (Die Ware wird gewogen, um den Preis abzufragen. Die Entscheidung, ob gekauft wird oder nicht, wird vom Preis abhängig gemacht.) Derartige Einrichtungen hängen nicht unmittelbar mit irgendwelchen Einnahmen oder auch Umsätzen zusammen. Der Begriff „Registrierkasse“ sollte an dieser Stelle im Sinne unserer Anmerkungen zu

§ 1 umschrieben werden. Ist die Definition so zu sehen, dass ein Server mit mehreren Eingabeplätzen in einer Filiale als EINE Registrierkasse mit mehreren Eingabestationen zu sehen ist. Wie ist die Definition zu verstehen, wenn der Server nicht in der Filiale vor Ort steht sondern in der Zentrale und an diesem online Eingabestationen hängen. Ist dann der Server die Registrierkasse und der PC vor Ort die Eingabestation?

Zu 3 Z 20 – Signatur (kryptografische Signatur)

Der Begriff „kryptografische Signatur“ sollte im gesamten Verordnungsentwurf gestrichen werden, da hier an keinerlei Rechtsbegriffe aus dem Signaturgesetz angeknüpft wird (angeknüpft werden kann).

Zu § 3 Z 21 und 22

Die Reihenfolge gehört weil streng alphabetisch – getauscht.

Zu § 3 Z 22 – Signaturerstellungseinheit

Sichergestellt sollte werden, dass die Software-Einrichtung mitumfasst ist. Eine Verpflichtung zur Verwendung jeglicher Hardware ist nicht „systemoffen“ und daher politisch nicht gewünscht!

Zu § 3 Z 27 – Umsatzzähler

Unbare Umsätze dürfen vom Umsatzzähler keinesfalls erfasst werden. Entsprechende Vorkehrungen sind vonnöten.

Zu § 3 Z 28 – Verifikation

PC-Kassen haben keinen Umsatzzähler, nur „Typ 2-Kassen“ sind damit ausgerüstet.

Zu § 3 Z 29 – Zahlungsbeleg (auch Beleg)

Der Begriff „übergeben“ sollte durch „bereitgestellt“ ersetzt werden, um auch elektronische Übertragungsformen zu ermöglichen. Die Definition des Zahlungsbelegs im Mittelteil ist viel zu weitgehend: Ein Beleg bestätigt einen Zahlungseingang und enthält darüber hinaus die eine oder andere zusätzliche Angabe. Er dokumentiert aber deswegen noch lange nicht den „wesentlichen Inhalt des Rechtsgeschäfts zwischen den Geschäftspartnern“. Nicht nur, dass selbst ein noch so informativer Beleg „nur“ Beweismittel ist und solcherart nur Tatsachen, nicht aber die rechtliche Seite betrifft, kann er nur den Vorgang der Bezahlung bestätigen, aber nicht einmal Auskunft über den Zahlenden geben. Dass hängt mit der Leistungsfähigkeit der einzelnen Beweisarten zusammen: Die Urkunde kann nur beweisen, dass ihr Textgehalt darauf dokumentiert ist, nicht hingegen, dass er auch zutrifft (zB. Hamm/Hassemer/Pauly Beweisantragsrecht2 Rz 80). Da jeder Beleg dieser Beweisart zuzurechnen ist, sind ihm auch diese Grenzen immanent.

Die letzten beiden Ziffern werden mit „29“ bezeichnet, richtig wäre den letzten Absatz mit „Z 30“ zu nummerieren.

Zu § 5 – Allgemeine Anforderungen an die Registrierkasse

In § 5 des Entwurfes der Registrierkassenverordnung werden jeweils zu Beginn der Absätze 1 bis 4 die Worte "Jede Registrierkasse muss...." verwendet. In § 3 Z 18 wird der Begriff "Registrierkasse" definiert. Die Kombination der beiden zitierten Verordnungsstellen indiziert, dass strenggenommen

jede Registrierkasse, also auch historische Registrierkassen, die in § 5 genannten Anforderungen erfüllen müssen. Wir regen daher an, dass der Begriff „Registrierkasse“ entsprechend unseren Bemerkungen zu § 1 iVm § 3 Z 18 entsprechend klargestellt wird.

Die EB zu § 5 vermitteln den Eindruck, die Ausstellung elektronischer Zahlungsbelege wäre auf Online Geschäft beschränkt. Dies wäre eine durch Verordnung unzulässige Einschränkung zum neuen § 132a BAO. Vielmehr sollte eindeutig klargestellt werden dass die Ausstellung elektronischer Belege bei allen Zahlungsvorgängen zulässig ist.

Zu § 6 - Inbetriebnahme der Sicherheitseinrichtung für die Registrierkasse

Abs. 1 müsste richtig umformuliert werden:
Die zur Inbetriebnahme notwendige Eingabe eines Initialwertes darf nicht älter als eine Woche sein. Wegen der kurzfristigen Lebensdauer des Initialwertes muss seine Lieferzeit kurzfristig, sein, also maximal 15 Minuten, da die Abfrage vor Ort bei der Inbetriebnahme erfolgen wird. Ebenso erforderlich ist eine kurze Wartezeit bei kurzfristig notwendigen Systeminstallationen im Zuge von Reparaturen etc. Der Initialwert sollte nicht nur vom Abgabepflichtigen sondern auch von seinem Steuerberater angefordert werden können.
Jedenfalls sollte dieser Initialwert mittels FON bereits ab Herbst 2015 generiert werden können.

Abs. 3
Es ist davon auszugehen, dass es Registrierkassen gibt, die sowohl die Möglichkeit des Ausdruckes als auch der elektronischen Übermittlung vorsehen. Wir gehen davon aus, dass in diesem Falle der letzte Satz des § 6 Abs. 3 RKS-V zur Anwendung kommt und keine Verpflichtung besteht, dass der Startbeleg ausgedruckt aufbewahrt werden muss.

Zu § 7 – Datenerfassungsprotokoll

Abs. 3
Diese Verspeicherung muss dem Manipulationsschutz entsprechen.
Gemäß § 7 Abs. 3 RKS-V im gegenständlichen Entwurf gilt folgendes:
"(3) Die Daten des Datenerfassungsprotokolls sind zumindest vierteljährlich auf einem externen Medium zu sichern. Diese Sicherung ist aufzubewahren (§ 132 BAO)." Aufgrund der obigen Formulierung gehen wir davon aus, dass auch ein Ausdruck des Datenerfassungsprotokolls eine mögliche Form der Sicherung darstellt. Sollte es gewünscht sein, dass die Daten in elektronischer Form gesichert werden sollen, so wäre dies gegebenenfalls klarzustellen. Es soll noch erwähnt werden, dass die Verwendung eines Online-Systems die Kosten der Datensicherung meist wesentlich verringert.

Abs. 5
Wir regen an, dass Änderungen am Exportformat im Erlasswege bekanntzugeben sind. Weiters wird angeregt, dass Änderungen am Exportformat innerhalb bestimmter Frist vorangekündigt werden, damit sich die Benützer rechtzeitig darauf einstellen können. Für die praktische Handhabbarkeit ist es auch sehr wichtig, dass es nicht zu unterschiedlichen (Branchen)Datenerfassungsprotokollen kommt.

Man muss im Sinne der Praktikabilität davon ausgehen können, dass es grundsätzlich verschiedene Exportformate geben sollte. Daher regen wir an, die Veröffentlichung einer Mehrzahl von Exportformaten in die Verordnung aufzunehmen:

Zu § 8 – Summenspeicher

Abs. 1

Diese Bestimmung trifft wohl nur für „Typ 2-Kassen“ zu, nicht jedoch für Typ 3-Kassen;
An dieser Stelle müsste der Begriff „Registrierkasse“ durch den der „Sicherheitseinrichtung“ ersetzt werden, um sachgerecht zu sein;

Abs. 2

Es stellt sich die Frage, wie vorzugehen ist, wenn Monatsende und Mitternacht zusammenfallen? Um Mitternacht ein „künstliches Schichtende“ zu generieren, scheint absolut unpraktikabel.

Abs. 3

Gilt der „Ablauf eines Kalenderjahres“ auch bei abweichendem Wirtschaftsjahr?

Zu § 9 – Signaturerstellung durch die Signaturerstellungseinheit

Der Ausdruck „Kryptografische“ Signatur wäre, entsprechend unseren Anmerkungen zu § 3 Z 20, zu streichen (auch in § 8 Abs. 2).

Abs. 1

„Trainings- und Stornobuchungen“ wäre zu ergänzen um „alle anderen Buchungen“, um sicherzustellen, dass es zu einer vollständigen Erfassung aller Kassenbetätigungen kommt. Dabei würde allerdings das Erfordernis, Monatsbelege zu erstellen, zu einem, auch gemessen an § 114 BAO, völlig unverhältnismäßigen Aufwand führen (§ 114 BAO).

Abs. 2 Z 4

Die Erfassung der USt bringt keine wesentliche Verbesserung in der Betrugsverhinderung. Die KWT regt daher an, dass bei Barzahlungen nicht nach Steuersätzen getrennt aufzuzeichnen ist.
Ein Beleg ist keine Rechnung gemäß § 11 UStG! Zudem ist die Höhe der Umsatzsteuer im Zeitpunkt der Belegerstellung möglicherweise noch gar nicht bekannt. Hier stellt sich z.B. die Frage, wie dies bei Gutscheinen oder Kautionen zu verstehen ist?

Zudem wäre ein klarstellender Verweis auf § 10 UStG nötig. Der Textvorschlag hierfür: "Betrag der Barzahlung nach Steuersätzen gemäß § 10 UStG getrennt".

Abs. 2 Z 5

Die Bestimmung sollte besser lauten; …..„mindestens in ganzen Hundertern“ statt „in ganzen Hundertern“. Damit wären auch genauere Stände zugelassen.

Abs. 3 Der Ausdruck „automatisiert“ entspricht nicht der Eingabe des PIN!

Abs. 4 sollte wie folgt ergänzt werden:
„Die rückgemeldete Signatur ist in die Beleginhalte aufzunehmen“.
Bei einigen derzeit am Markt vorhandenen Systemen ist der Ausdruck eines QR-Codes nicht in angemessener Zeit möglich. Zudem resultiert aus dem QR-Code ein hoher Papierverbrauch. Das Papier besteht häufig aus einem hohen Kunststoffanteil.
Die Signatur kann ebenso als alphanumerischer Code gedruckt werden. Dieser ist ebenso maschinell erfassbar und dadurch kontrollierbar.

Zu § 10 – Aufbereitung des maschinenlesbaren Codes
Abs. 2 Z 3:
Es ist unklar, was genau hier gemeint ist.
Alle Belege, die keine Auswirkung auf den Summenspeicher haben, d.h. nicht nur Trainings- oder Stornobuchungen, sondern z.B. auch innerbetriebliche Belege, sollten als solche erkennbar sein, und müssten in anderer geeigneter Weise – eben nicht als „Trainings- bzw. „Stornobuchung“ - gekennzeichnet werden.
Generell sollte die Anforderung des § 10 Abs. 2 Z 3 aus systematischen Gründen in § 11 Abs. 2 verschoben werden.

Zu § 11 – Belegerstellung
Generell erscheint bedenklich, dass die Anforderungen der Verordnung ausdrücklich über die des Gesetzes, nämlich § 132a Abs 3 BAO neu, hinausgehen („Verordnung strenger als das Gesetz“!?).

Abs. 1 Z 4
Der „Inhalt des maschinenlesbaren Codes (QR-Code)“ würde bedeuten, dass alle Informationen des § 10 Abs. 2 Z 1 bis 8 angeführt sein müssen. Erforderlich wäre aber nur, dass entweder der QR-Code grafisch oder als alphanummerische Ziffernfolge, die dem QR-Code entspricht, aufgedruckt sein muss. Die Verfolgbarkeit der jeweiligen Buchung wäre damit vollauf gesichert.

Zu § 12ff – Zur Signaturerstellungseinheit und Signatur
Die Probleme im Zusammenhang mit der Verwendung einer elektronischen Signatur sind im Grunde ähnlich jener der e-Rechnung. Es geht um die „Unversehrtheit des Inhaltes“ und die „Identität der Herkunft“. Beides wird im Grunde durch eine elektronische Signatur ermöglicht.
Im Zusammenhang mit der RKS-V ist dieser Nachweis (zumindest mittelbar) auf dem Beleg zu erbringen, indem der Beleg eindeutig mit einem Wert markiert wird, der den Signaturdaten entspringt. Eine elektronische Signatur (im Sinne des Signaturgesetzes) wird mittels eines elektronischen Zertifikates erzeugt.

Um die Identität der Herkunft zu sichern, sollte dieses Zertifikat von einem Zertifizierungsdiensteanbieter ausgestellt werden, der gewährleistet, dass das jeweilige Zertifikat dem Signator eindeutig zugeordnet ist. Das wäre demnach ein fortgeschrittenes Zertifikat (abgeleitet aus §2 Z 3 SigG „fortgeschrittene Signatur“).

Für derartige Zertifikate ist keine „sichere Signaturerstellungseinheit“ erforderlich, es kann sich dabei auch um Software-Zertifikate handeln.

Die Verwendung eines qualifizierten Zertifikates macht insofern wenig Sinn, als dieses

1. Nur auf eine natürliche Person ausgestellt werden kann
2. An eine sichere Signaturerstellungseinheit gebunden ist und
3. Die Eingabe eines PINs vor Auslösen des Signaturvorganges erfordert.

Da fortgeschrittene (insb. Softwarezertifikate) keine Signaturerstellungseinheit verwenden, sondern die Signatur über Programmfunktionen aufgerufen wird, sollte das Kernthema der Signaturerstellungseinheit grundsätzlich anders angegangen werden.
Es sollte eine funktional erweiterte Signaturerstellungseinheit von einem ZDA betätigt werden können.

Sinnvollerweise sollten die Zertifikate nur von ZDAs ausgestellt werden, die bei der Aufsichtsbehörde akkreditiert sind. Nachdem die Aufsichtsstelle für „fortgeschrittene" Zertifikate nicht mehr zuständig ist, müsste hierzu möglicherweise auch das SigG bzw. die SigV angepasst werden.

Das Problem der RKS-V ist derzeit aber jedenfalls der Verweis auf die „Trusted List" – denn diese bezieht sich ausschließlich auf qualifizierte Zertifikate. Der Verweis auf die Trusted-List und alle damit verbundenen Bestimmungen der RKS-V sollten daher ersatzlos gestrichen werden. Diese Trusted-List ist eigentlich ein EU-Thema, wogegen die RKS-V ausschließlich Österreich betrifft. Sowohl in der BAO als auch in der RKS-V (§ 4, § 9) wird auf eine „kryptografische Signatur" verwiesen. Wir haben bereits voranstehend darauf aufmerksam gemacht, dass weder im SigG noch in der SigV verankert ist, was eine „kryptografische Signatur" überhaupt sein soll, Im SigG (§ 2) finden sich lediglich Begriffsbestimmungen für „elektronische Signatur", „fortgeschrittene elektronische Signatur" und „qualifizierte elektronische Signatur". Die RKS-V (§12) verweist bei den technischen Anforderungen an die Signaturerstellungseinheit auf die „Anforderungen an Signaturerstellungseinheiten für qualifizierte Signaturen nach SigG (§ 18)". Die RKS-V (§ 15) verweist bei der Beschaffung der Signaturerstellungseinheit auf einen „… zugelassenen Zertifizierungsdienstanbieter, der qualifizierte Signaturzertifikate anbietet, zu erwerben.". Jedoch existiert weder im SigG noch in der SigV der Begriff „Signaturzertifikat", im SigG (§2) finden sich nur Begriffsbestimmungen für „Zertifikat" und „qualifiziertes Zertifikat".

Ausgehend von der daraus zu gewinnenden Erkenntnis eigenmächtig gewählter Begriffe beruht unsere Stellungnahme daher auf folgender Interpretation: Die Sicherheitseinrichtung besteht aus einer sicheren Signaturerstellungseinheit, welche auf Basis von wesentlichen Belegdaten und einem qualifizierten Zertifikat eine qualifizierte elektronische Signatur für jeden Beleg erstellt. Alle unterstrichenen Begriffe finden sich im SigG (§ 2) wieder und sind somit definiert. Der Begriff „elektronische" wird in Folge weggelassen.

Die Erstellung einer qualifizierten Signatur setzt laut SigV (§ 4 Abs. 2) die Verwendung eines Authorisierungscodes (z.B. PIN, Fingerabdruck, …) voraus. Weiters ist dort festgehalten: „Eingabeerleichterungen bei wiederholter Eingabe von Authorisierungscodes müssen ausgeschlossen sein.". Ist die Eingabe eines PINs bei Erstellung jedes einzelnen Belegs gewünscht? Jede momentan am Markt befindliche und zugelassene „sichere Signaturerstellungseinheit" hält sich an diese Vorgabe!

Um ein qualifiziertes Zertifikat zu erlangen, muss man sich rechtsverbindlich als natürliche Person ausweisen. Das qualifizierte Zertifikat ist einer natürlichen Person zugeordnet. Belege, welche durch die qualifizierten Signaturen geschützt werden und welche mittels qualifizierten Zertifikaten erstellt worden sind, müssen somit einer natürlichen Person zuordenbar sein. Wie soll das bei Belegen, die durch juristische Personen ausgestellt werden, zu bewerkstelligen sein? Wenn die natürliche Person, auf welche ein qualifiziertes Zertifikat ausgestellt wurde, das Unternehmen verlässt, ist es dann als ungültig zu melden? Ist auf Belegen dann der Geschäftsführer (ähnlich wie bei Deutschen Web-Seiten) anzuführen, um die Verbindung zwischen Beleg und qualifiziertem Zertifikat herzustellen?

Wir schlagen daher eine Abschwächung der Signatur zu einer „fortgeschrittenen Signatur“ vor:
Wird anstatt einer qualifizierten Signatur eine fortgeschrittene Signatur vorgeschrieben, so kann ein „normales“ Zertifikat verwendet werden und auch die PIN-Eingabe fällt unter bestimmten Umständen weg.

Ein Zertifikat kann sowohl für juristische als auch für natürliche Personen ausgestellt werden. Durch die Meldung der Zertifikat-Seriennummer bei der Registrierung der Signaturerstellungseinheit in FinanzOnline ist die Identität, auf die das Zertifikat ausgestellt wurde, eher zweitrangig, da nur der Unternehmer und Vertretungsbefugte auf FinanzOnline Zugriff haben. Somit sind nur Belege gültig, welche mit Zertifikaten signiert sind, deren Seriennummer in FinanzOnline gespeichert ist.
Um eine Signatur ohne einen Benutzereingriff auszulösen, muss die Signaturerstellungseinheit auf den privaten Schlüssel des Zertifikats zugreifen können. Um eine Genehmigung als sichere Signaturerstellungseinheit zu erlangen, muss eben dieser Zugriff mittels Authorisierungscode geschützt sein. Hier sollte die RKS-V eine Zulassungsmöglichkeit für „Signaturerstellungseinheiten mit besonderen Merkmalen“ vorsehen. Ist eines dieser Merkmale die Erlaubnis zur Nutzung des privaten Schlüssels per Opt-Out-Fernsteuerung, so kann das SigG (§ 2 Abs 3c) gewahrt werden, und Signaturen können ohne Signator-Eingriff generiert werden.

Somit müsste die RKS-V folgende Interpretation erlauben: Die Sicherheitseinrichtung besteht aus einer Signaturerstellungseinheit mit besonderen Merkmalen, welche auf Basis von wesentlichen Belegdaten und einem Zertifikat eine fortgeschrittene elektronische Signatur für jeden Beleg erstellt.

Aufwertung der Signaturerstellungseinheit – Funktionelle Erweiterung

Zusätzlich zum Opt-Out des Zugriffs auf den privaten Schlüssel sollte die Signaturerstellungseinheit noch um zwei weitere Merkmale erweitert werden: Die Vergabe einer fortlaufenden Belegnummer sollte ausschließlich durch die Signaturerstellungseinheit erfolgen, denn nur so kann der letzte Beleg gesichert werden. Ohne eine laufende Nummer kann trotz einer Verkettung der Signaturen die Belegkette von hinten gelöscht werden. Die Belege sind daher nicht vor Manipulation geschützt!
Ein weiteres wichtiges Erfordernis für den Manipulationsschutz sind zwei Umsatzzähler direkt in der Signaturerstellungseinheit, einer für positive Umsätze und einer für negative Umsätze. Die Beleg-Gesamtsumme soll zur visuellen Belegprüfung im Klartext in die Signatur einfließen und die Signaturerstellungseinheit führt eigene Summenspeicher für positive und negative Umsätze.

Derartige Summen- und Belegzähler sind auch bei Insika ein wesentlicher Bestandteil des Sicherheitskonzepts, deren Fehlen die Sinnhaftigkeit der Gesamtregelung in Frage stellt.

Es soll eine reine Softwarelösung als Signaturerstellungseinheit mit besonderen Merkmalen erlaubt sein. Laut SigG (§ 2) ist eine Signaturerstellungseinheit eine konfigurierte Software ODER(!) eine Hardware. In dem gegenständlichen Entwurf einer RKS-V ist kein Platz für eine reine Softwarelösung, was zu Ansteuerungen von Chip-Karten per Internet führen wird, denn auch diese Verordnung wird die Verbreitung von Handy-Apps, Cloud-Anwendungen und Online-Betriebssystemen nicht aufhalten können.

Der größte Vorteil von Online-Systemen ist
- Die leichte und sichere Prüfbarkeit durch die Finanzpolizei.
- Die einfache und sichere Aufbewahrung des Datenerfassungsprotokolls
- Erhöhung des Nutzens für Unternehmen und Kunden durch elektronische Zusatzprodukte (z.B. Automatische Archivierung, Rechnungsarchiv des Kunden, …)

Alternative „fortgeschrittenes elektronisches Siegel“

Die „VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 23. Juli 2014“, welche die „Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates“ außer Kraft setzt, auf der auch das SigG und die SigV beruht, könnte eine alternative Lösung für die RKS-V bieten. Ein Zertifikat für elektronische Siegel wird hier eingeführt, welches Daten mit einer juristischen Person verknüpft. Bezüglich der Anforderungen für die Erstellung wird hier in Artikel 36c auf ein „ … mit einem hohen Maß an Vertrauen unter seiner Kontrolle … “ verwiesen, und das im Gegensatz zu §2 Abs. 3c SigG, wo die Wortfolge „… unter seiner alleinigen Kontrolle … “ zu finden ist.

Praxistauglichkeit

Mehrere Punkte der RKS-V sind nicht praxistauglich:
Der mehrstufige Registrierungs- und Beschaffungsprozess ist umständlicher als er sein müsste. Bereits bei der Zertifikatsanfrage müssen alle Daten vom Steuerpflichtigen vorhanden sein, somit kann das auch automatisch bei Bestellung/Erstellung vom ZDA an FinanzOnline weitergeleitet werden.

Der Initialwert, welcher aus dem FinanzOnline kommt, und der Datenschlüssel für den Summenspeicher sollten zusammengefasst werden. Z.B. wird ein Private/ Public Key bei Meldung einer Zertifikatseriennummer generiert, wobei der Public Key ins Zertifikat zurückgemeldet wird und als Initialwert verwendet werden soll und dieser auch zur Verschlüsselung des Summenspeichers genutzt werden kann.

Im Entwurf wird geregelt, dass sich Trainings-Buchungen nicht im Summenspeicher auswirken dürfen (§ 8 Abs. 1). Es gibt jedoch keine Regelungen betreffend Lieferscheine, Agenturgeschäfte, Hoteltransfers, Eigenverbrauch, Einladungen, Mitarbeiterrabatte usw.

Um nicht in die Geschäftsabläufe der einzelnen Branchen eingreifen zu müssen, sollten alle erzeugten Belege in den Summenspeicher aufgenommen werden. Eine dynamische Liste von Belegtypen soll im Internet nachlesbar sein und dieser Belegtyp sollte auch in die Beleg-Signatur einfließen, um nachträgliche Kennzeichnungen unmöglich zu machen.

Der geforderte maschinenlesbare Code soll laut RKS-V scheinbar ein QR-Code sein. Mit einfachen technischen Mitteln ist heute auch ein reiner Text maschinenlesbar. Der QR-Code ist daher eine unnötige technische Einschränkung und wenn das Format des Datenerfassungsprotokolls mittels Web-Seiten-Veröffentlichung geregelt werden kann, so sollte hier auch dieses technische Detail mittels Web-Seiten-Veröffentlichung flexibel geregelt werden können.

Der Manipulationsschutz ist momentan nicht hoch, da zu viele sensible Aufgaben direkt von der Registrierkasse erledigt werden. Solange die Registrierkasse selbst den Summenzähler, die fortlaufende Belegnummer und das Signieren der Belege durchführt, ist der Manipulationsschutz nicht optimal. Erst bei Übertagung der oben genannten sensiblen Funktionen an die Signaturerstellungseinheit ist ausgeschlossen, dass die Registrierkasse nicht Belege nach der Signierung wieder rückgängig machen kann.

Derzeit in der Praxis verwendete Systeme erfüllen diese Anforderung bereits und es ist unverständlich, warum diese notwendigen Funktionen nicht in der geplanten Signaturerstellungseinheit aufgenommen werden sollen.

Zu § 13 – Signaturschlüsselpaar und Signaturerstellung

Hardware und PIN-Eingabe scheinen gleichermaßen erforderlich zu sein. Sowohl die Pflicht zur Hardware als auch die PIN-Eingabe sind strikt abzulehnen, um die politisch klar gewollte Systemoffenheit zu garantieren.

In § 13 wäre es überdies richtiger, von den „Punkten 1-7“ anstatt von den „Absätzen 1-7“ (des Anhangs zur SigV 2008) zu sprechen.

Zu. § 13 Z. 2

Es sollte eine Regelung zu diversen Sonderfällen geben, die keine Barumsätze im eigentlichen Sinn sind, bzw. keine Zahlung mit Bankomat-/EC-Karte erfolgt. Dies betrifft ohne Anspruch auf Vollständigkeit zB Zahlungen mit Scheck, Wechsel, Bezahlung mittels Tausch, nach dem Kauf wesentlich spätere Barzahlung, usw. Dabei geht es lediglich um eine Klarstellung bzw. Vervollständigung.

Zu § 14 – Verifizierbarkeit der Signaturen

Hier erschiene (präzisierend) die Einfügung angebracht: „… auf dem Beleg aufgebrachten maschinenlesbaren Codes **entsprechend § 10 Abs. 2** ….“

Zu § 15 – Beschaffung der Signaturerstellungseinheit

Abs. 1 muss sinnrichtig lauten:
*„… bei **einem der** im EU-/EWR-Raum oder in der Schweiz…“*

Abs. 3

Beim Verweis auf § 5 Abs. 1 Z 8 SigG dürfte es sich um ein Fehlzitat handeln.

Zu § 16 – Registrierung der Signaturerstellungseinheit

Abs. 3

Es sollte ergänzt werden, in welcher Reaktionsgeschwindigkeit FinanzOnline antworten muss. Der Initialwert müsste binnen 15 Minuten vorliegen, um die Wirtschaft nicht unerträglich zu behindern.

Zu § 17 – Bekanntgabe der Außerbetriebnahme der Sicherheitseinrichtung für die Registrierkasse

Abs. 1. und 2.

Was hat zu geschehen, wenn der Ausfall zu einer Zeit erfolgt, bei dem sich der Unternehmer z.B. aus Gründen einer Geschäftsreise, Krankheit oder Urlaub außer Haus befindet bzw. wenn das Unternehmen geschlossen hat (z.B. Saisonbetrieb)? Zudem erscheint die Formulierung „ohne unnötigen Aufschub“ überzogen (vgl. dazu Ritz BAO5 § 85a Tz 5). Als Alternative böte sich „zeitnah“ an.

Abs. 3

*„Der **nicht nur vorübergehende** Ausfall und die Außerbetriebnahme…“*

Abs. 4

Es sei an folgenden Fall gedacht: Die Kasse funktioniert, aber die Signatursicherheitseinheit liefert keine Signatur. Es stellt sich die Frage, ob Ausfälle nicht ohnehin protokolliert werden (müssen). Wenn ja, wozu ist eine separate Anmerkung nötig? Muss diese händisch erfolgen? Wenn ja, kann dies Fehlerquellen herrührend von dem Verkaufspersonal bedeuten.

In diesem Zusammenhang erscheint auch unklar, was mit "über alle Belege" gemeint ist und wie somit dieser Sammelbeleg in dieser Hinsicht auszugestalten ist.

Abs. 5

Statt „nach zu erfassen“ sollte schriftlich besser „nachzuerfassen“ gewählt werden.

Abs. 6

Auf Grund dieses Wortlautes wäre es nötig, dass der Unternehmer, wenn eine Registrierkasse nicht mehr in Betrieb genommen werden kann, eine neue Signatureinheit beschaffen muss. Und zwar auch dann, wenn die Signatureinheit selbst voll funktionstüchtig ist. Wir regen eine entsprechende Abänderung an.

Abs. 7

Der letzte Satz in Abs. 7 sollte lauten: „*Der Schlussbeleg ist ~~auszudrucken und~~ aufzubewahren (§132 BAO).“* Die sichere elektronische Erfassung muss jedenfalls genügen.

Zu § 18 – Datenbank über Sicherheitseinrichtungen für die Registrierkassen

Abs. 2:

Das Wort „zumindest“ wäre zu streichen, um sonstige Unklarheiten zu vermeiden.

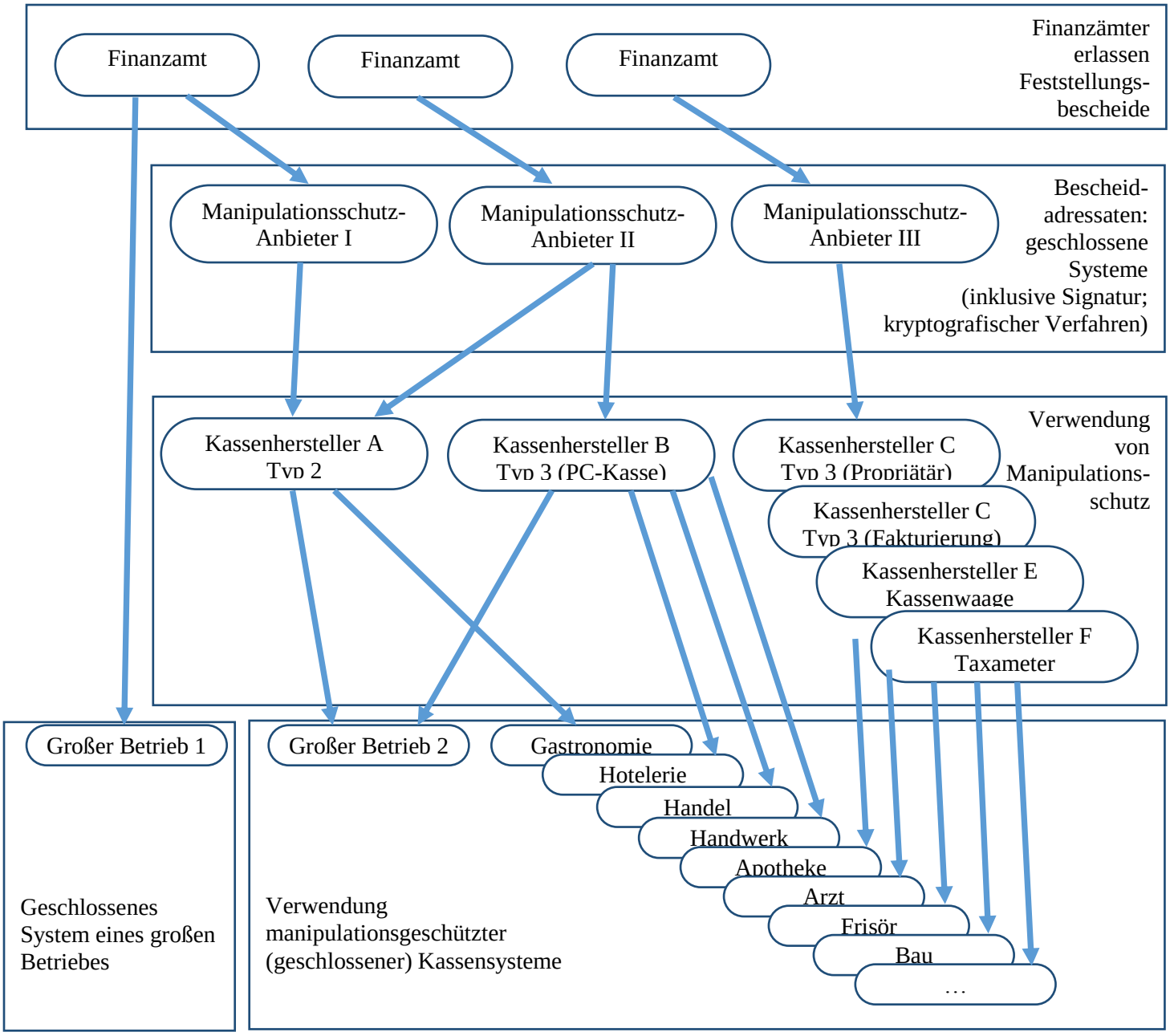
Ziffer 13
Abgabenbehörden können nur durch „Organe“ tätig werden, daher kann „der Organe“ gestrichen werden, sodass es heißt „Kontrollen ~~der Organe~~ der Abgabenbehörden.“ Auch die Finanzpolizei ist eben keine Behörde, sondern nur ein Organ der jeweils zuständigen Behörden.

Zu § 19 – Kontrolle und Prüfung der Datensicherheit für die Registrierkassen
Abs. 1
In Abs. 1 kann wieder „der Organe“ gestrichen werden. Dies gilt ebenso für die folgenden Paragraphen. Darüber hinaus der letzte Satz („Bei Registrierkassen … zur Verfügung zu stellen.“), da dieser überflüssig erscheinen muss.

Abs. 2
Auch an dieser Stelle wäre „der Organe“ zu streichen. Weiters ergibt sich die Verpflichtung, das Datenerfassungsprotokoll auf einem externen Datenträger zu exportieren, schon aus § 7 Abs. 5. Die (nochmalige) Regelung an dieser Stelle ist daher verzichtbar.

Zu § 20 – Technische und organisatorische Anforderungen
Die Regelung betreffend „Geschlossene Systeme“ sollte sowohl für große Betriebe als auch für (große) Anbieter von Manipulationsschutzsystemen gelten.
Gutachten von gerichtlich beeideten Sachverständigen sollen sowohl für große „geschlossenen Gesamtsysteme“ als auch für weit verbreitete Manipulationsschutzsysteme (eines ZDA) möglich sein.

Mit „geschlossenem Gesamtsystem, das im Unternehmen … verwendet wird“, soll nicht nur ein Unternehmen gemeint sein, sondern auch unternehmensübergreifende Systeme, wie sie z.B. bei BILLA und auch ADEG in Verwendung stehen (selbständige Unternehmer. Die folgende Grafik soll die Schaffung der Rechtssicherheit durch große Manipulationsschutzsysteme verdeutlichen:



<u>Zu § 20 Abs. 1</u>

Der Begriff „kryptografische Verkettung“ ist nicht definiert.

Abs. 3

Es ist nicht nachvollziehbar, warum die Anforderung bei mehr als 500 Eingabestationen liegen soll (siehe auch zu § 3 Z. 8).

Zu § 21 Abs. 1

Aus dieser Bestimmung geht nicht hervor, dass bei geschlossenen Gesamtsystemen eine „sachverständige Begutachtung“ jedenfalls zwingende Voraussetzung für deren Verwendung bzw Inbetriebnahme ist. Der Einleitungssatz dieser Bestimmung sollte daher lauten: „Für die Verwendung eines geschlossenen Gesamtsystems ist eine sachverständige Begutachtung zwingende Voraussetzung“.

Abs. 5 letzter Satz

Statt „Die Vollständigkeit der sicherheitsrelevanten Überprüfungen im Gutachten sind durch eine Bestätigungsstelle gemäß § 19 SigG zu bescheinigen“ müsste dieser lauten: „Die Vollständigkeit der sicherheitsrelevanten Überprüfungen im Gutachten ist durch eine Bestätigungsstelle gemäß § 19 SigG zu bescheinigen.“ Das Subjekt dieses Satzes (Vollständigkeit) steht nämlich im Singular.

Zu § 22

Wir regen an, dass sichergestellt wird, dass die zeitgerechte Erlassung des Feststellungsbescheides gesetzlich geregelt wird (zB Entscheidungsfrist), darüber hinaus klargestellt wird, welche Behörde entscheidungsbefugt ist, und ausreichend entsprechend qualifizierte Personalressourcen vorgesehen werden.

Zu § 22 Abs. 1

Die Bestimmung enthält aber keine konkrete Regelung, WORÜBER der Feststellungsbescheid abspricht und welche konkrete Abgabenbehörde dafür zuständig ist (offenbar jene, die erst weiter unten in § 23 Abs. 1 der RKS-V angeführt ist). Die Bestimmung sollte weiters die allgemeine Rechtsgrundlage für Feststellungsbescheide (§ 92 Abs. 1 lit. b BAO) anführen.

Zu § 22 Abs. 2

Statt „zu Grundelegung“ müsste es lauten: „Zugrundelegung“.

Zu § 22 Abs. 4

Der Hinweis auf die Bestimmungen der „§§ 343 ff BAO“ ist offenbar unzutreffend. Die Textierung lässt die Zuordnung zur zutreffenden BAO-Bestimmung zwar nur erahnen, aber offenkundig ist die Beschwerdemöglichkeit gemäß den §§ 243 ff BAO gemeint. Der Satz sollte daher lauten: „...hat der Unternehmer unbeschadet der Möglichkeit der Erhebung einer Bescheidbeschwerde gemäß den §§ 243 ff. BAO“…..

Zu § 23 Abs. 1: Änderung der tatsächlichen Verhältnisse

Dieser Satz sollte lauten: „Das zuständige Finanzamt hat über jede Änderung des geschlossenen Gesamtsystems mit Feststellungsbescheid im Sinne des § 22 Abs. 1 abzusprechen.“ Statt der Textierung „ab zu sprechen“ sollte jedenfalls die schriftlich wohl richtigere Formulierung „abzusprechen“ Verwendung finden.

Zu § 24 – Kontrolle der Identität der Softwarekomponenten

Im Sinne des bereits in dieser Stellungnahme des Öfteren angesprochenen Umstandes, dass eine Behörde nur durch ihre Organe handeln kann, wäre auch hier umzuformulieren: Die ~~Organe der~~ Abgabenbehörde~~n~~ ist ~~sind~~ berechtigt, die …“

Zu § 25 Inkrafttreten

Durch die unterschiedlichen Zeitpunkte des Inkrafttretens muss jedes Kassensystem DREI MAL umgerüstet bzw. umprogrammiert werden. Dies ist in keiner Weise verhältnismäßig! Die Inkrafttretensreglung sollte so gestaltet sein, dass bei Beginn der Registrierkassenpflicht bereits Sicherheitseinrichtungen samt Initialwert verfügbar sind, um Abgabepflichtige nicht in die Lage zu bringen, mehrfach investieren zu müssen. Außerdem sollte die Inkrafttretensreglung Systemanbietern und –nutzern genug Zeit geben, um die Lösung ordnungsgemäß und wirtschaftlich umzusetzen.

Der in § 25 Abs. 3 geregelte Inkrafttretenszeitpunkt sollte auf den 01.10.2015 verlegt werden, um die organisatorischen Voraussetzungen für die Einführung zu schaffen, jedoch mit der Maßgabe, dass ab dem Termin aus dem Abs. 3 zum Erwerb einer neuen Kasse (Abs. 1) sowie zur Umstellung einer bestehenden Kasse (Abs. 2) eine Frist von einem Jahr gegeben werden sollte.

Wenn das Inkrafttreten aus dem Abs. 3 mit 01.07.2016 erfolgen soll, dann muss den Unternehmen bis zum 01.07.2017 Zeit zum Erwerb (Abs. 2.) oder der Umstellung (Abs. 1) gewährt werden.

Andernfalls werden die Kassenhersteller die notwendigen Adaptierungen nicht in der geplanten Zeit bewirken können. Wir dürfen hier nochmals angesichts ihrer Wichtigkeit unsere Bemerkungen zum Ende der Präambel wiederholen.

Wir ersuchen höflich, unsere Vorschläge bzw. Anregungen zu berücksichtigen und verbleiben

mit freundlichen Grüßen

MMag.Dr.iur. Verena Trenkwalder LL.M.
(Vorsitzende des
Fachsenats für Steuerrecht)

Mag. Gregor Benesch e.h.
(Stellv. Kammerdirektor)

Referenten:

Mag.Dr. Martin Jann
Dr. Michael Kotschnigg
Ing.Mag.Dr. Axel Kutschera
Mag. Armin Obermayr
Mag. Bernhard Renner
Ing.Mag.Dr. Michael Schirmbrand
Mag. Stefan Schuster
Hon.-Prof.Univ.-Doz.Mag.Dr. Reinhard Schwarz
Mag. Thomas Strobach
em.Univ.-Prof.Dr. Michael Tanzer
MMag.Dr.iur. Verena Trenkwalder LL.M.
Mag.Dr. Peter Unger