Stand 16. Februar 2017

Bewertung des „Gesetzes zum Schutz vor Manipulationen an digitalen Grundaufzeichnungen“ und Anforderungen an die „Kassensicherheitsverordnung“

Das Ende 2016 beschlossene Gesetz zum Schutz vor Manipulationen an digitalen Grundaufzeichnungen schafft lediglich einen Rahmen für konkrete Lösungen und enthält mehrere problematische Regelungen. Daher wird die noch nicht vorliegende Verordnung – im Gesetzentwurf Kassensicherheitsverordnung (KassenSichV) genannt – entscheidend dafür sein, ob die praktische Umsetzung des Gesetzes erfolgreich und termingerecht möglich ist.

Die aus Sicht des DFKA e.V. bestehenden technischen und praktischen Aspekte sind im Folgenden kurz beschrieben. In der Anlage werden sie ausführlicher erläutert.

Schwachpunkte des Gesetzes

A. **Schutzziele nicht klar definiert**: Das Gesetz benennt nur unpräzise und indirekt, was wovor geschützt werden soll.
B. **Keine Registrierung der Sicherheitsmodule**: Nur durch eine Registrierung der Sicherheitsmodule kann die Authentizität der Daten (also die Rückführbarkeit auf den Urheber) gewährleistet werden, nicht durch die vorgesehene Meldung der Aufzeichnungssysteme.
C. **Kein Sicherheitsmerkmal auf dem Beleg**: Eine schnelle, einfache und sichere Kassen-Nachschau erfordert leicht prüfbare Belege. Dazu müssen diese über ein praxistaugliches Sicherheitsmerkmal verfügen.
D. **„Andere Vorgänge“ unbestimmt**: Es wird eine Aufzeichnung anderer Vorgänge gefordert, ohne dass es Ansätze zu deren konkreter Definition gibt.
E. **Widersprüchliche Regelung zur Datenspeicherung**: Der Wortlaut ist widersprüchlich bezüglich der Frage, ob die digitalen Grundaufzeichnungen nur innerhalb der Sicherheitseinrichtung abgelegt werden dürfen oder auch außerhalb.
F. **Fehlende Ordnungsmäßigkeitsvermutung bezüglich der Vollständigkeit**: Eine Vermutung der Ordnungsmäßigkeit gem. §§ 158, 146 Abs. 4 AO bei korrekter Verwendung der Sicherheitseinrichtung ist nicht im Gesetz verankert.
G. **Billigkeitsmaßnahmen**: Über Billigkeitsanträge (Ausnahmen von Belegpflicht und Pflicht zum Einsatz einer Sicherheitseinrichtung) werden die Finanzbehörden mangels eigener technischer Expertise nicht sachgerecht entscheiden können.
H. **Keine Sanktionen bei Verstößen gegen Belegausgabe- und Meldepflicht**: Während für diverse Verstöße hohe Bußgelder vorgesehen sind, fehlt jegliche Sanktion beim Verstoß gegen die aus Sicherheitsgesichtspunkten zentralen Pflichten zur Belegausgabe und zur Anmeldung der Aufzeichnungssysteme (die eigentlich die Sicherheitsmodule erfassen müsste, siehe B).
I. **Nicht-gewerbsmäßige Manipulation straffrei**: Manipulationsversuche sind nur strafbar, wenn deren gewerblicher Charakter nachgewiesen werden kann.
J. **Fehlende Registrierkassenpflicht**: Das Risiko des Ausweichens auf kaum prüfbare offene Ladenkassen besteht weiter.

Die Punkte A bis G sollten sich grundsätzlich durch eine geeignete Formulierung der Verordnung ganz oder zumindest teilweise korrigieren lassen.

Anforderungen an die Verordnung

Im Einzelnen ergeben sich aus Sicht des DFKA die folgenden Forderungen:

1. **Ausreichende und verständliche Konkretisierung**: Die Verordnung muss so konkret sein, dass es in der Umsetzungsphase nicht zu veränderten Auslegungen oder gar Veränderungen an der Verordnung kommt. Sonst wird eine termingerechte und kostengünstige Umsetzung sehr unwahrscheinlich.
2. **Klare und sinnvolle Sicherheitsanforderungen**: Es ist eine Präzisierung der im Gesetz nur vage angedeuteten Schutzziele erforderlich.
3. **Verschiedene Schutzprofile für verschiedene Lösungsansätze**: Die verschiedenen heute denkbaren technischen Lösungsansätze erfordern teilweise grundsätzlich unterschiedliche Schutzmechanismen und Sicherheitsanforderungen. Dem sollte die Verordnung Rechnung tragen, indem unterschiedliche Schutzprofile vorgesehen werden, deren Schutzniveau sich aber entsprechen muss.
4. **Reine Belegkontrolle per Sicherheitsmerkmal ermöglichen**: Mit der Belegpflicht ist ein wesentlicher Baustein für einfache Kassennachschauen vorhanden. Es fehlt jedoch ein prüfbares Sicherheitsmerkmal. Hier ist eine Lösung zu finden, mit der auch verschiedene technische Verfahren für die Finanzverwaltung praktisch prüfbar bleiben. Nur so ist Rechtssicherheit für die Steuerpflichtigen erreichbar.
5. **Registrierung der Sicherheitsmodule**: Indirekt formuliert das Gesetz die sehr sinnvolle Anforderung, Mechanismen zur Sicherstellung der Authentizität und Vollständigkeit der Aufzeichnungen bereitzustellen. Um dies erfüllen zu können, ist eine zentrale Erfassung der Sicherheitsmodule erforderlich. Die im Gesetz ausdrücklich normierte Meldepflicht für Registrierkassen könnte und sollte im Zusammenhang damit gelöst werden.
6. **Eindeutige und sinnvolle Definition „anderer Vorgänge“**: Um Rechtssicherheit für alle Beteiligten zu schaffen, ist eine konkrete Definition der aufzeichnungspflichtigen „anderen Vorgänge“ erforderlich. Diese muss für jeden der möglichen technischen Ansätze eindeutig aus dem Gesetzeszweck abgeleitet werden können und praktikabel sein.
7. **Datenspeicherung außerhalb der Sicherheitseinrichtung ermöglichen**: Eine für alle Beteiligten praxisgerechte Lösung muss es erlauben, die Daten ohne besondere Maßnahmen außerhalb der Sicherheitseinrichtung abzulegen.
8. **Sicherungsmaßnahmen gegen technische Störungen nötig**: Die Auswirkungen von Datenverlusten aufgrund technischer Störungen sollten minimiert werden, vor allem, um die Interessen der Anwender zu schützen. Die Verordnung darf zumindest kein Hindernis sein, entsprechende Mechanismen anzubieten.
9. **Ordnungsmäßigkeitsvermutung**: Die Einhaltung aller relevanten Vorschriften muss gegenüber den Anwendern von Registrierkassen wieder mit der Vermutung der Ordnungsmäßigkeit in Bezug auf Richtigkeit und Vollständigkeit der Daten honoriert werden.
10. **Billigkeitsregelung darf Sicherheit nicht aushöhlen**: Falls Erleichterungen von Belegpflicht und/oder der Pflicht zum Einsatz einer zertifizierten Sicherheitseinrichtung gemäß § 146a Abs. 2 Satz 2 und § 148 AO gewährt werden, darf das Sicherheitsniveau nicht hinter den Anforderungen an alle anderen Steuerpflichtigen zurückbleiben.
11. **Praxisorientierung und technisches Fachwissen**: Da es sich bei der Verordnung vor allem um eine technische Regulierung handelt, auf deren Basis konkrete Produkte entstehen werden, muss hier Praxiserfahrung und technischer Sachverstand einfließen.
12. **Herausforderung einheitliche digitale Schnittstelle**: Aufgrund der großen Bandbreite an Aufzeichnungssystemen ist die Definition der im Gesetz geforderten einheitlichen und allgemeinverbindlichen Schnittstelle eine komplexe Aufgabe. Auch hier ist viel Fachwissen erforderlich.

Die Punkte 1 bis 10 behandeln die Inhalte der Verordnung während 11 und 12 den Prozess der Erstellung betreffen.

Der DFKA hält das INSIKA-Verfahren weiterhin für die einfachste und kostengünstigste aller heute verfügbaren technischen Lösungen. Bei einer Ausgestaltung der Verordnung wie hier beschrieben ist kein fachlicher Grund erkennbar, der gegen eine Zertifizierung von INSIKA sprechen könnte. Schon um den Terminplan sicher halten zu können, muss mindestens eine bestehende und bewährte Lösung zugelassen werden.

Anlage: Ausführliche Erläuterung der einzelnen Kritikpunkte und Anforderungen

Stand 16. Februar 2017

Erläuterungen und Hintergrundinformationen zu

Bewertung des „Gesetzes zum Schutz vor Manipulationen an digitalen Grundaufzeichnungen“ und Anforderungen an die „Kassensicherheitsverordnung“

1 Grundsätzliches

Das Gesetz zum Schutz vor Manipulationen an digitalen Grundaufzeichnungen ist sehr allgemein gehalten und schafft lediglich einen Rahmen für konkrete Lösungen. Es enthält mehrere Regelungen, die ohne eine geeignete Konkretisierung zu Umsetzungsproblemen führen werden. Daher wird die noch nicht vorliegende Verordnung – in der Begründung des Gesetzentwurfs Kassensicherheitsverordnung (KassenSichV) genannt – entscheidend dafür sein, ob die praktische Umsetzung des Gesetzes erfolgreich, termingerecht und mit vertretbaren Kosten möglich ist.

Der Zeitraum bis zur verpflichtenden Nutzung einer Sicherheitseinrichtung, d.h. bis zum 1.1.2020, mag lang erscheinen, mit Blick auf die Möglichkeiten technischer Realisierung ist er angesichts deutlich höherer Priorisierung von „Technologieoffenheit“ gegenüber einer Standardisierung außerordentlich eng (Abschnitt 2). Gerade durch den knappen Zeitplan müssen Fehler, Unklarheiten und Regelungslücken, die unweigerlich zu Nachbesserungen und Verzögerungen führen, unbedingt vermieden werden.

Der DFKA bewertet das Gesetz vor allem aus der technischen Sicht sowie mit Blick auf die praktische Umsetzung. Aus dieser Perspektive ergeben sich die im Abschnitt 3 beschriebenen Schwachstellen. Konkrete Lösungsansätze für die Kassensicherheitsverordnung werden im Abschnitt 4 dargestellt.

2 Zeitplan

Für von Grund auf neu zu konzipierende Lösungen ergibt sich aus unserer Sicht im Idealfall etwa der folgende Zeitplan:

Aufgabe	Start	Dauer (Monate)
Erstellung Verordnung und Schutzprofile	2/2017	5
Entwicklung, Erprobung und Zertifizierung	7/2017	18
Flächendeckende Installation	1/2019	12
Einführung	1.1.2020	

Die 12 Monate für eine flächendeckende Installation sind bereits optimistisch geschätzt. Der Zeitraum von 18 Monaten für Entwicklung und Erprobung ist bereits anspruchsvoll, wenn man die BSI-Zertifizierung ausklammert. Eine Erstellung der Verordnung und der Schutzprofile in weniger als einem halben Jahr erscheint ebenfalls nur schwer machbar.

Die Zertifizierung gänzlich neu konzipierter Lösungen auf Basis von Schutzprofilen in dem durch das Gesetz vorgegeben Zeitrahmen erscheint dagegen unmöglich. So dürften Smart-Meter-Gateways in Bezug auf die Komplexität in etwa mit einer neu konzipierten Manipulationssicherung für Registrierkassen vergleichbar sein. Alleine die Erstellung des 90 Seiten um-

fassenden Schutzprofils für Smart-Meter-Gateways dauerte fast zwei Jahre.[1] Sechs Jahre nach dem Start des Prozesses ist noch kein einziges Smart-Meter-Gateway zertifiziert.

Aufgrund dieser Terminrisiken halten wir es im Interesse aller Marktteilnehmer für unbedingt erforderlich, dass bereits bestehende und auf vorzertifizierten Komponenten[2] basierende Verfahren wie z.B. INSIKA nicht grundsätzlich oder durch fachlich nicht erforderliche Anforderungen[3] ausgeschlossen werden. Sie müssen natürlich in der Lage sein, die Zielsetzung des Gesetzes zu erfüllen. Systeme ohne ausreichendes Schutzniveau können selbstverständlich keine Zertifizierung erhalten.

3 Erläuterung der Schwachpunkte des Gesetzes

A. Schutzziele nicht klar definiert

Der Gesetzestext fordert lediglich, dass elektronische Aufzeichnungssysteme und die digitalen Aufzeichnungen durch eine zertifizierte Sicherheitseinrichtung zu schützen sind. Wovor sie geschützt werden sollen, lässt sich direkt nur aus Namen des Gesetzes ableiten.

Aus der Verordnungsermächtigung und der Begründung im Regierungsentwurf lässt sich jedoch schließen, dass es um die Sicherheitszeile Integrität (Veränderungen der Daten nach Erfassung müssen verhindert oder erkennbar gemacht werden) und Authentizität (also die sichere Rückführbarkeit der Daten auf den Urheber) geht. Darüber hinaus wird auch die Vollständigkeit genannt – da die Forderung nach Integrität bereits nachträgliche Löschungen abdeckt, kann es dabei nur um die vollständige Erfassung sämtlicher Vorgänge gehen. Alle diese Anforderungen sind sinnvoll und sachgerecht.

Verbindliche Aussagen zum gewünschten technischen Schutzniveau gibt es bisher nicht. Das BSI hat allerdings hohe Anforderungen in Aussicht gestellt – vergleichbar mit der qualifizierten elektronischen Signatur.[4]

B. Keine Registrierung der Sicherheitsmodule

Das Schutzziel der Sicherstellung der Authentizität der Daten lässt sich nur mit fälschungssicheren und nachprüfbaren Merkmalen in den Daten erreichen, die eindeutig dem jeweiligen Unternehmen zugeordnet werden können. Die Vergabe dieser Merkmale kann nur Aufgabe des Sicherheitsmoduls sein. Also muss eine Verknüpfung zwischen Sicherheitsmodul und Unternehmen hergestellt werden und zwar so, dass hier keine Manipulationen (z.B. durch die Angabe einer falschen Identität) möglich sind. Eine Registrierung der Aufzeichnungssysteme (und dann noch ohne eine Prüfung, ob die Angaben korrekt sind) allein vermag das nicht zu leisten.

C. Kein Sicherheitsmerkmal auf dem Beleg

Erst eine schnelle, einfache und sichere Kassen-Nachschau ermöglicht eine flächendeckende Überwachung des tatsächlichen/korrekten Einsatzes der Sicherheitseinrichtung und der zeitgerechten Aufzeichnung des Geschäftsvorfalls. Nur diese kann die Vollständigkeit der Erfassung deutlich wahrscheinlicher machen, als das heute der Fall ist. Dazu muss es bei einer Nichterfassung ein nennenswertes Entdeckungsrisiko geben.

Die dafür erforderliche Art von Kassen-Nachschau (im Sinne einer Feldüberwachung) erfordert neben der Belegausgabepflicht leicht prüfbare Belege. Dazu müssen diese über ein Sicherheitsmerkmal verfügen, das weitgehend automatisch, zweifelsfrei und rechtssicher

---

[1] Die erste Tagung dazu fand am 28.1.2011 statt, das Schutzprofil wurde am 21.12.2012 veröffentlicht.

[2] So basiert INSIKA auf zertifizierten Signaturkarten und ergänzt diese mit einer noch zu zertifizierenden Software-Erweiterung. Für die Schlüsselverwaltung können ebenfalls bereits zertifizierte Verfahren benutzt werden. Das in Österreich genutzte Verfahren verwendet Standard-Signaturkarten wird aber vermutlich aufgrund bekannter Sicherheitslücken in Deutschland nicht zertifizierbar sein.

[3] Ein Beispiel dafür wäre die Forderung nach einer sicheren Zeitquelle, die bei einem geeigneten Lösungskonzept überflüssig ist.

[4] In der Präsentation des BSI für das Fachgespräch mit Herstellern im Bundesfinanzministerium am 25.5.2016 wurde auf Folie 6 eine Zertifizierung des Sicherheitsmoduls nach EAL 4+ gefordert.

überprüft werden kann. Auch bei mehreren verschiedenen zugelassenen Sicherheitsverfahren muss die Finanzverwaltung praktisch in der Lage sein, diese Kontrollen durchzuführen.

D. „Andere Vorgänge“ unbestimmt

Es wird weiterhin eine Aufzeichnung „anderer Vorgänge“ gefordert. Das konkrete Ziel dieser Verpflichtung wird nicht genannt, so dass es bisher keinen Ansatzpunkt für eine praktisch verwendbare Definition dieser „anderen Vorgänge“ gibt. Die Erläuterungen in der Gesetzesbegründung führen jedenfalls nicht zu einer tauglichen Lösung.[5]

E. Widersprüchliche Regelung zur Datenspeicherung

Zum einen verlangt das Gesetz, dass die Aufzeichnungen „auf dem Speichermedium zu sichern“ sind – zum anderen legen Gesetzesbegründung[6] und Verordnungsermächtigung[7] nahe, dass die Daten auch außerhalb der Sicherheitseinrichtung weiterhin manipulationsgeschützt sein müssen. Warum das Speichermedium dann Teil der zertifizierten Sicherheitseinrichtung sein soll, bleibt unklar.

F. Fehlende Ordnungsmäßigkeitsvermutung bezüglich der Vollständigkeit

Das Gesetz schafft zumindest prinzipiell die Voraussetzungen, die es im Fall einer Erfüllung verschiedener Kriterien erlauben, bei einer Betriebsprüfung grundsätzlich von einer vollständigen und richtigen Erfassung der Geschäftsvorfälle auszugehen. Damit könnte der § 158 AO auch bei bargeldintensiven Unternehmen wieder seinen eigentlichen Zweck erfüllen, also dem Steuerpflichtigen einen Vertrauensvorschuss zu gewähren.

Eine Vermutung der Ordnungsmäßigkeit bei korrekter Verwendung der Sicherheitseinrichtung ist im Gesetzestext selbst jedoch nicht verankert.

G. Billigkeitsmaßnahmen

Dem Gesetz nach können die Finanzbehörden Befreiungen von der Belegpflicht zulassen. In diesem Fall muss es anderweitige Mechanismen geben, die eine vollständige Erfassung der Geschäftsvorfälle überprüfbar machen. Die Finanzverwaltung müsste dazu die Tauglichkeit dieser Mechanismen beurteilen.

Laut „Beschlussempfehlung und Bericht des Finanzausschusses“ zum Gesetz ist ebenfalls vorgesehen, dass die Finanzverwaltung Ausnahmen von der Pflicht zur Nutzung einer Sicherheitseinrichtung im Billigkeitswege zulassen kann.[8] Hier dürfte eine sachgerechte Prüfung der jeweiligen Sicherheitsverfahren durch die Finanzbehörden praktisch unmöglich sein.

Außerdem würde man dann vom bisherigen Verwaltungsstandpunkt abweichen, der in den GoBD so formuliert wird: „Positivtestate zur Ordnungsmäßigkeit der Buchführung – und damit zur Ordnungsmäßigkeit DV-gestützter Buchführungssysteme – werden weder im Rahmen einer steuerlichen Außenprüfung noch im Rahmen einer verbindlichen Auskunft erteilt.“[9]

H. Keine Sanktionen bei Verstößen geben Belegausgabe- und Meldepflicht

Durch die Einführung neuer Tatbestände der Steuergefährdung können verschiedene Verstöße mit hohen Bußgeldern sanktioniert werden, auch ohne dass es zu einer nachgewiesenen Steuerhinterziehung gekommen ist.

---

[5] Regierungsentwurf vom 13.7.2016: „Andere Vorgänge sind solche, die unmittelbar durch Betätigung der Kasse erfolgen (z.B. Tastendruck, Scanvorgang eines Barcodes), unabhängig davon, ob sich daraus ein Geschäftsvorfall entwickelt.“ Diese Anforderung ist weder erfüllbar noch zielführend – siehe auch Stellungnahme des DFKA zu Sachverständigenanhörung im Finanzausschuss am 17.10.2016.

[6] Dort wird ausgeführt, dass die Aufzeichnungen auch bei einem Verkauf oder einer Verschrottung „für die Dauer der Aufbewahrungsfristen auf einem (anderen) Speichermedium gesichert und verfügbar gehalten werden“ müssen.

[7] Es sollen in der Verordnung neben den Anforderungen an das Speichermedium der Sicherheitseinrichtung auch „Anforderungen an die elektronische Aufbewahrung der Aufzeichnungen“ definiert werden.

[8] Bundestags-Drucksache 18/10667 vom 14.12.2016, Seite 22, dritter Absatz

[9] Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) vom 14.11.2014, Rz. 180

Die Belegausgabepflicht und die Pflicht zur Anmeldung der Aufzeichnungssysteme (die eigentlich eine Pflicht zur Anmeldung der Sicherheitsmodule sein sollte) sind für die Sicherheit des Verfahrens mindestens so wichtig wie die anderen Punkte. In diesen Fällen sind Verstöße aber nicht bußgeldbewehrt.

I. Nicht-gewerbsmäßige Manipulation straffrei

Die Strafandrohung für Manipulationsversuche verschiedener Art beschränkt sich ausschließlich auf gewerbsmäßige Tätigkeiten. Zum einen dürfte es eindeutig nicht gewerbsmäßige Angriffe geben (z.B. Hacker, die versuchen das System zu „knacken“) und zum anderen muss der gewerbliche Charakter auch in jedem Einzelfall erst einmal nachgewiesen werden, so etwa wenn eine Zapper-Software vom Anbieter eines Systems kostenlos und ohne direkten Zusammenhang mit dem Geräteverkauf abgegeben wird.

J. Fehlende Registrierkassenpflicht

Die Führung einer offenen Ladekasse wird – ob bewusst oder unbewusst – durch die neuen gesetzlichen Regelungen deutlich schwieriger. So ist auch bei einer offenen Ladenkasse eine Befreiung von der Einzelaufzeichnungspflicht nur beim „Verkauf von Waren an eine Vielzahl von nicht bekannten Personen gegen Barzahlung“ vorgesehen. Bei der Erbringung von Leistungen gilt diese Regelung offenbar nicht.

Das Risiko des Ausweichens auf offene Ladenkassen besteht dennoch weiter.

4 Anforderungen an die Verordnung

Damit die gesetzlichen Regelungen den gewünschten Zweck erfüllen und praxistauglich umgesetzt werden können, ergeben sich aus Sicht des DFKA die folgenden Anforderungen an die Verordnung:

1. Ausreichende und verständliche Konkretisierung

Schon aufgrund des knappen Zeitplans aber auch zur Vermeidung unnötiger Kosten muss ausgeschlossen werden, dass es während der Planung und Implementierung der Sicherheitseinrichtungen zu Missverständnissen, neuen Auslegungen oder gar Änderungen der Verordnung kommt.[10] Die Verordnung sowie die daraus abgeleiteten technischen Vorgaben müssen daher konkret, verständlich und vor allem eindeutig sein.

2. Klare und sinnvolle Sicherheitsanforderungen

Die im Gesetz genannten Schutzziele müssen unbedingt präzisiert werden. Die Sicherheitsanforderungen müssen aus den Schutzzielen nachvollziehbar abgeleitet werden können. Diese wiederum bilden die Basis für Schutzprofile oder technische Richtlinien.

Nur so ist zu verhindern, dass unzureichende, falsche oder gar überflüssige Maßnahmen gefordert werden.[11]

3. Verschiedene Schutzprofile für verschiedene Lösungsansätze

Trotz aller Forderungen nach „Technologieoffenheit“ sind heute nur einige wenige, allerdings grundsätzlich verschiedene Lösungsansätze denkbar. Diese erfordern auch unterschiedliche Sicherheitsanforderungen – ein Beispiel: Bei einer Datenspeicherung beim Steuerpflichtigen wird man andere Anforderungen an deren Schutz stellen als bei einer Speicherung im Rechenzentrum eines Vertrauensdiensteanbieters.[12]

---

[10] Diese Probleme waren und sind bei der Umsetzung von Kassensicherheitslösungen in anderen Staaten an der Tagesordnung und haben ihre Ursache meistens in einer unzureichenden oder unsauberen Festlegung der Anforderungen.

[11] Bei Betrachtung verschiedener internationaler Sicherheitsverfahren für Registrierkassen ist das eher die Regel als die Ausnahme.

[12] In dem Beispiel werden die Daten beim Steuerpflichtigen durch eine sichere Hardware oder Kryptographie geschützt werden müssen, während ein sicheres Rechenzentrum bereits selbst einen Schutz von unbefugten Zugrif-

Also wird es unterschiedliche Schutzprofile bzw. technische Richtlinien geben müssen.[13] Diese sollten voneinander getrennt werden, um die Fertigstellung eines Verfahrens nicht durch die unfertige Formulierung der Anforderungen an ein anderes Verfahren zu blockieren. Angesichts des engen Zeitplans (siehe Abschnitt 2) ist dieser Aspekt besonders wichtig.

4. Reine Belegkontrolle per Sicherheitsmerkmal ermöglichen

Das Gesetz ist nicht ausdrücklich so formuliert, dass eine aussagekräftige Kassen-Nachschau bereits mit einer reinen Belegkontrolle – also ohne Datenzugriff oder gar technische Prüfung der Aufzeichnungssysteme – möglich ist. Mit der Belegpflicht ist allerdings ein wesentlicher Baustein vorhanden. Es fehlt das prüfbare Sicherheitsmerkmal auf dem Beleg. Die Verordnungsermächtigung erlaubt es, „Anforderungen an den Beleg“ festzulegen. So kann dort auch das Sicherheitsmerkmal als Anforderung definiert werden.

In dem Zusammenhang ist eine Lösung dafür zu finden, dass auch verschiedene technische Verfahren für die Finanzverwaltung praktisch prüfbar sind. Das wird ohne eine weitgehende Standardisierung kaum möglich sein. Technisch sehr gut möglich wäre das bei der Verwendung von QR-Codes, die auf einen Prüfserver im Internet verweisen und die zu prüfenden Daten enthalten. Dieser Ansatz wurde allerdings bisher vom BMF abgelehnt.[14]

5. Registrierung der Sicherheitsmodule

In der Verordnungsermächtigung formuliert das Gesetz indirekt die Anforderung, einen Mechanismus zur Sicherstellung der Authentizität der Aufzeichnungen bereitzustellen. Diese Anforderung ist unbedingt sinnvoll. Das erfordert aber ein Sicherheitsmodul, das neben der eigentlichen Sicherung der Daten diese derart kennzeichnet, dass sie sicher auf den einzelnen Steuerpflichtigen rückverfolgbar sind. Das ist aufgrund der sachnotwendigen Einzigartigkeit dieser Kennzeichnung ohne eine zentrale Erfassung aller Sicherheitsmodule nicht gewährleistet.

Die im Gesetz ausdrücklich normierte Meldepflicht für Registrierkassen kann dies nicht leisten. Dieser Aspekt könnte und sollte aber im Zusammenhang mit der Registrierung der Sicherheitsmodule gelöst werden, so dass es für die Anwender nur einen einzigen Vorgang gibt (z.B. die Bestellung eines Sicherheitsmoduls, die alle Registrierungsschritte automatisch nach sich zieht). Diese Zusammenfassung muss nicht verpflichtend in die Verordnung aufgenommen werden, sie sollte Anbietern von Sicherheitsmodulen/-einrichtungen aber erlauben, eine derartige Dienstleistung anzubieten.

6. Eindeutige und sinnvolle Definition „anderer Vorgänge“

Um ohne zeitaufwändige und teure Nachbesserungen bei der Entwicklung der technischen Lösungen auszukommen, müssen die aufzeichnungspflichtigen „anderen Vorgänge“ sauber definiert werden. Auch zur Herstellung von Rechtssicherheit ist dies zwingend erforderlich.

Die Definition der „anderen Vorgänge“ muss sich unmittelbar aus der Zielsetzung des Gesetzes ableiten lassen. Die zusätzlichen Aufzeichnungspflichten müssen also den Zielen Integrität, Authentizität und Vollständigkeit dienen. Darüber hinausgehende Anforderungen wären auch vom gesetzlichen Telos nicht legitimiert.

7. Datenspeicherung außerhalb der Sicherheitseinrichtung ermöglichen

Vermutlich war im Gesetzgebungsverfahren beabsichtigt, dass die Aufzeichnungen auch außerhalb der Sicherheitseinrichtung gespeichert werden dürfen, ohne dass dies besondere

---

fen bietet. Andererseits wird man bei so einer Lösung einen abgesicherten Zugriffsmechanismus für die Behörden benötigen.

[13] Eine Entscheidung für eine Zertifizierung nach Common Criteria mit Schutzprofilen oder nach technischer Richtlinie ist ebenfalls zu treffen. Diese hängt vor allem vom geforderten Sicherheitsniveau und ggf. auch vom Zeitplan ab.

[14] Siehe Regierungsentwurf vom 13.7.2016, Begründung A. III. 2a)

Schutzmaßnahmen erfordert. Dies ist dann möglich, wenn die Daten selbst mit geeigneten Sicherungen versehen sind.[15]

Da dies dem Gesetzeswortlaut selbst jedoch nur durch Auslegung zu entnehmen ist, sollte die Verordnung in dieser Hinsicht eindeutig sein. Die Speicherung außerhalb der Sicherheitseinrichtung sollte jederzeit möglich sein und nicht erst bei Außerbetriebnahme des Aufzeichnungssystems.[16] Nur so sind praktikable Lösungen vor allem für mittlere und größere Unternehmen denkbar. Hier ist die zentrale Speicherung (also Speicherung außerhalb des Aufzeichnungssystems) der Normalfall – eine davon abweichende Behandlung der steuerrelevanten Daten würde einen erheblichen Aufwand verursachen. Hinzu kommt, dass Prüfungen durch die Finanzbehörden dann ebenfalls sehr stark verkompliziert würden.

8. Sicherungsmaßnahmen gegen technische Störungen nötig

Es besteht stets ein Risiko, dass Daten durch technische Probleme verloren gehen oder unbrauchbar werden. Daher sind Mechanismen, die in einem derartigen Fall zumindest die wesentlichen Informationen[17] in manipulationssicherer Form liefern, äußerst sinnvoll für alle Beteiligten.

Die Verordnung muss solche Mechanismen nicht vorschreiben, sollte aber zulassen, dass Hersteller entsprechende Funktionen anbieten.

9. Ordnungsmäßigkeitsvermutung

Die Einhaltung der in § 146a Abs. 1 Satz 1 und § 146 Abs. 4 AO genannten Kriterien zur Datenintegrität können im Wesentlichen allein durch technische Sicherheitsvorkehrungen, d.h. durch das Sicherheitsmodul, gewährleistet werden. Zur Gewährleistung der Datenvollständigkeit bedarf es darüber hinaus organisatorischer Maßnahmen, nämlich verpflichtende Belegausgabe durch den Steuerpflichtigen einerseits und Feldüberwachung durch die Finanzverwaltung andererseits. Das ist dem Grunde nach durch § 146a Abs. 2 Satz 1 und § 146b AO sichergestellt.

Vor diesem Hintergrund kann und muss die Einhaltung aller relevanten Vorschriften durch die Anwender von Registrierkassen wieder mit der Vermutung der Ordnungsmäßigkeit in Bezug auf Richtigkeit und Vollständigkeit der Daten honoriert werden.[18]

10. Billigkeitsregelung darf Sicherheit nicht aushöhlen

Es ist vorgesehen, dass im Billigkeitswege Ausnahmen von der Belegpflicht und der Pflicht zum Einsatz einer Sicherheitseinrichtung[19] zugelassen werden können. Nach allen vorliegenden Informationen ist für die Sicherheitseinrichtung ein sehr hohes Schutzniveau vorgesehen,[20] was vom DFKA ausdrücklich begrüßt wird. Es ist festzulegen, auf welcher Basis die Finanzbehörden Ausnahmen genehmigen, zugleich aber auch die Einhaltung dieses Schutzniveaus sicherstellen können.

---

[15] Z.B. digitale Signaturen

[16] So könnte die entsprechende Passage in der Gesetzesbegründung verstanden werden.

[17] Beispielsweise Tagesgesamtumsätze

[18] Grundsätzlich folgt das bereits aus der Formulierung des § 158, da hier auf die Befolgung der §§ 140 bis 148 abgestellt wird. Allerdings heißt es in der Gesetzesbegründung: „Es besteht eine gesetzliche Vermutung der Richtigkeit der Kassenaufzeichnungen, wenn eine zertifizierte technische Sicherheitseinrichtung vorhanden ist und ordnungsgemäß genutzt wird.“ (Regierungsentwurf vom 13.7.2016, Begründung B. zu Artikel 1, zu Nummer 3). Die Vollständigkeit wird nicht erwähnt.

[19] Im Gesetzestext wird eine Ausnahme für den Einsatz von Sicherheitseinrichtungen zwar nicht erwähnt – in der Drucksache 18/10667 vom 14.12.2016 (Beschlussempfehlung und Bericht des Finanzausschusses) aber ausdrücklich angesprochen.

[20] Entsprechende Aussagen wurden z.B. in den Fachgesprächen im Bundesfinanzministerium am 25.5.2016 von den Vertretern des BSI gemacht.

Vorstellbar wäre es, für eine Genehmigung Sachverständigengutachten[21] oder auch eine Zertifizierung des BSI vorauszusetzen. Speziell bei einer BSI-Zertifizierung wäre ein einheitliches Schutzniveau wesentlich leichter erreichbar.

11. Praxisorientierung und technisches Fachwissen

Auch wenn die Verordnung formal Teil des Steuerrechts ist, handelt es sich materiell um eine technische Regulierung. Jede technische Regulierung ist an sich schon komplex, wird hier durch den Anspruch der „Technologieoffenheit“ allerdings noch erheblich komplexer. Zugleich gibt es nur einen engen Zeitplan, der größere Nachbesserungen verbietet.

Aus diesem Grund muss sichergestellt werden, dass in den gesamten Erstellungsprozess Praxiserfahrung und technischer Sachverstand einfließen. Die bloße Möglichkeit zur Stellungnahme zu einem tatsächlich oder nur scheinbar fertigen Entwurf wird nicht ausreichen.

12. Herausforderung einheitliche digitale Schnittstelle

Das Gesetz ist in Bezug auf die einheitliche digitale Datenschnittstelle nicht eindeutig. Schon aufgrund der Anforderung, Integrität und Authentizität der Daten prüfen zu können, wird jedenfalls eine weitergehende Standardisierung erforderlich sein, als in der Vergangenheit.[22]

Die Definition dieser Schnittstelle ist eine komplexe Aufgabe, die mehrere Entwicklungszyklen und Praxistests erfordern wird. Auch hier ist entsprechendes Praxis- und Fachwissen für eine schnelle und zugleich praktikable Lösung unentbehrlich.

5 Fazit

Das „Gesetz zum Schutz vor Manipulationen an digitalen Grundaufzeichnungen“ ist grundsätzlich geeignet, seine Ziele zu erreichen. Es enthält eine Reihe von Schwächen, die aber überwiegend durch eine sachgerechte Verordnung „geheilt“ werden können.

Bei der Verordnung handelt es sich trotz ihres steuerrechtlichen Hintergrundes im Wesentlichen um eine technische Regulierung. Deshalb sind zu ihrer Erstellung unbedingt Experten einzubeziehen, die nicht nur über das allgemeine technische Fachwissen, sondern auch über konkrete Branchenerfahrung verfügen.

Der Zeitplan ist sehr ambitioniert, speziell wenn erzwungen werden sollte, grundsätzlich neue Lösungen zu entwickeln.

[21] Dieser Weg wurde in Österreich gewählt. Dort können Sachverständige per Gutachten die Manipulationssicherheit „geschlossener Gesamtsysteme“ bestätigen.

[22] Das einheitliche Datenformat wird eher Festlegungen analog zum ELSTER-Verfahren oder zur E-Bilanz bedingen als dem bisherigen „Datenbeschreibungsstandard für die Datenträgerüberlassung“ entsprechen.