ZUR FÖRDERUNG DER WISSENSCHAFT VON RECHNUNGSWESEN UND CONTROLLING
Wissenschaftliches Institut des BVBC

Wissenschaftliches Institut des BVBC e.V. ▪ Auguststraße 19–29 ▪ 53229 Bonn ▪ E-Mail: kontakt@bvbc-wib.de

An das Bundesministerium
der Finanzen

- per E-Mail -

Bonn, 4. August 2022

Eingaben:
Änderung des Anwendungserlasses zur Abgabenordnung (AEAO) zu § 146a

Das Wissenschaftliche Institut des BVBC (WIB) hat sich mit Mitgliedsunternehmen und weiteren wissenschaftlichen und wirtschaftlichen Akteuren zu den beabsichtigten Änderungen des Anwendungserlasses zur Abgabenordnung (AEAO) zu § 146a fachlich ausgetauscht. Die eingebrachten Bedenken und Kommentierungen möchte das WIB mit den folgenden Ausführungen dem Bundesministerium der Finanzen zur Kenntnis überlassen.

I. Marktliche und politische Auswirkungen der geplanten Änderung des Anwendungserlasses

1. Wir begrüßen grundsätzlich das Anliegen der Bundesregierung, die Fiskalisierung im Sinne einer vorwärtsgewandten Novellierung des Kassengesetzes und der Steuererfassung aktiv voranzutreiben, alle Transaktionen eines Kassensystems sicher zu speichern sowie digitale Daten vor nachträglicher Manipulation zu schützen. Die dazu vom Gesetzgeber in der Vergangenheit formulierten Anforderungen, Marktteilnehmende zu einer Zertifizierung einer technischen Sicherheitseinrichtung (TSE) zu verpflichten, werten wir als wichtigen Beitrag einen fairen Wettbewerb und geeignete Standards im Markt zu etablieren.

Mit dem Fortschreiten technologischer Entwicklungen eröffnen sich neue Möglichkeiten zur Sicherung digitaler Daten in verteilten Systemen (Cloud), die hingegen regulatorische Evaluationen hinsichtlich TSE-Standards erforderlich machen können. Im Markt befindliche, vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifizierte, cloudbasierte Lösungen (Cloud-TSE) nutzen hierzu bereits bestehende Potentiale geltender Sicherheitsanforderungen, die die Sicherung digitaler Daten vereinfachen und weniger manipulationsanfällig machen.

Gleichzeitig führt die Weiterentwicklung technologischer Lösungen zu neuen Wechselwirkungen im Verhältnis von gesellschaftlichen Erfordernissen und unternehmerischer Leistungsfähigkeit, die fortwährend beobachtet werden müssen. Wir befürworten ausdrücklich über die geplante Änderung des zugeleiteten Anwendungserlasses hinaus, einen direkten Austausch genauso wie einen gesellschaftlich-sektorenübergreifenden Dialog hierzu anzustoßen.

2. Digitale Lösungen brauchen Innovationsoffenheit, die gerade bei der Interaktion in verteilten Systemen gesellschaftliche Erfordernisse zur Orientierung benötigt und der wiederum in der Ausgestaltung gesetzlicher Standards Rechnung getragen werden muss. Wir begrüßen daher ausdrücklich die Intention der Bund-Länder-Arbeitsgruppe sich mit Aspekten zur Lösung von Anwendungsfragen über die gesetzlichen Anforderungen hinaus zu beschäftigen. An den Wortlaut des vorliegenden Referentenentwurfs zur Änderung des Anwendungserlasses schließen sich hingegen insbesondere mit

Blick auf cloudbasierte TSE-Lösungen zahlreiche Fragen an, die ohne weitere Klarstellung technologieausschließende und sicherheitsbeschränkende Wirkung entfalten können.

i. Die physische Einsatzumgebung (3.2.11)

Der Referentenentwurf sieht in I. Nr. 3, 3.2.11 vor, dass die Sicherheitsmodulanwendung (SMA) in der „physischen Einsatzumgebung" des elektronischen Aufzeichnungssystems (ERS) zu betreiben ist. Durch die in den weiteren Ausführungen unklare Definition dieser Einsatzumgebung lässt diese Formulierung erhebliche Zweifel an der Zulässigkeit einer cloudbasierten TSE-Lösung zu. Bei einer cloudbasierten TSE-Lösung läge die physische Einsatzumgebung nicht außer-, sondern innerhalb der Cloud. In Zertifizierungsprozessen hat das BSI jedoch bereits in Anlehnung an die dazu erforderliche sichere Kommunikation von SMA und ERS diverse Lösungen als hinreichend in ihrer Schutzwirkung nach vorgeschriebenen Prüfstandards anerkannt.

Es drängt sich hierzu die Frage auf, welches Ziel die leider definitorisch unklare Beschreibung einer sicheren Einsatzumgebung hat, wenn diese keinen zusätzlichen Sicherheitszweck in der Kommunikation von SMA und ERS erfüllt. Hinzu kommt, dass in einer Sicherheitskonzeption außerhalb der Cloud stets organisatorische bzw. technische Schutzmaßnahmen ergriffen werden müssen, um die Kommunikation zwischen ERS und SMA abzusichern – ungeachtet der Beschaffenheit der TSE-Lösung – unabhängig davon, ob cloud- oder hardwarebasiert (z.B. in Form eines USB-Sticks oder einer micro-SD).

ii. Bestimmung des Ortes (3.2.12)

Der Referentenentwurf führt in seinen Ausführungen zu I. Nr. 3, 3.2.12 den „Ort" als neues Merkmal des ERS ein. Dies sieht im Wortlaut vor, dass „der Ort eines elektronischen Aufzeichnungssystems der jeweilige Teil des elektronischen Aufzeichnungssystems ist, an dem die abzusichernden Geschäftsvorfälle inhaltlich, unabhängig von ihrer Formatierung oder Codierung, erstmalig vollständig vorliegen."

Für die Absicherung von Transaktionsdaten mit Blick auf eine cloudbasierte TSE-Lösung lassen sich mit der Bestimmung eines physischen Ortes keine sicherheitstechnischen und informationsgewinnenden Mehrwerte ableiten, da die Transaktionsdaten über steuer- und abgabenrechtliche Vorgänge jederzeit sicher verfügbar und abrufbar sind. Im Verständnis verteilter Systeme ist zusätzlich aus Sicherheitsgründen nicht erstrebenswert, einen Ort festzustellen, da der Prozessfluss der Daten verteilt, diese asynchron ablaufen und mehrfach gesichert sind (redundant).

Hinzu kommt, dass die Daten codiert sind und verschlüsselt vorliegen. Wenn innerhalb von verteilten Systemen die Feststellung eines spezifischen Ortes nicht wünschenswert ist und eine cloudbasierte TSE-Lösung hierzu allen zentralen Sicherheitsmerkmalen Rechnung trägt, warum ist die Einbringung dieses Tatbestandsmerkmals aus Sicht des Ministeriums der Finanzen notwendig? Ist es in der Konsequenz entsprechend verhältnismäßig Sicherheitsanforderungen an einen physischen Ort für die Kommunikation von ERS und SMA zu knüpfen?

iii. Der Notfallbetrieb (7.3)

Der Referentenentwurf greift in II. Nr. 2., 7.3 anschließend an die vorgelegten Ausführungen hinsichtlich einer „physischen Einsatzumgebung" sowie der Bestimmung „eines Ortes" Aspekte für die zusätzliche Absicherung im Notfallbetrieb einer ERS auf und folgert eine vermeintlich sicherheitstechnisch vorteilhafte durch die Anwendung einer hardware-basierten TSE daraus, die mit Mehraufwand verbunden ab Januar 2026 zusätzlich zertifiziert werden müsste. In dieser Ausführung wird hingegen eine vermeintliche Sicherheit angenommen, Transaktionsdaten auch im Notfallbetrieb für die Steuerprüfung besser nachvollziehen zu können, da eine cloudbasierte TSE-Lösung auch im Falle einer technischen Unterbrechung den Störungsfall dokumentiert.
Darauf aufbauend rechtfertigt der Notfallbetrieb nicht, die damit verbundene Konsequenz und Schadenswirkung im Markt hochinnovativer Fiskalisierungslösungen per Cloud auszuschließen.

3. Die oben beschriebenen Ausführungen schaffen weniger Klarstellungen als vielmehr Unsicherheiten, insbesondere für die Anwendung cloudbasierter TSE-Lösungen. Problematisch sind vor allem das Festhalten an einer „physischen Einsatzumgebung" sowie die Einführung eines neuen Tatbestandsmerkmals „Ort des elektronischen Aufzeichnungssystems (ERS)", die Missverständnisse zum intendierten Regelungszweck des Erlasses hervorrufen. Damit geht die Änderung des Anwendungserlasses zudem über den gesetzlichen Auftrag, Transaktionen von Kassensystemen vor Manipulation zu schützen, hinaus und macht den Erlass in diesem Punkt besonders juristisch angreifbar.

4. Der Erlass schließt in dessen Wortlaut in seiner unmittelbaren Auswirkung die Anwendung von sicheren, cloudbasierten TSE-Lösungen aus und lässt die Tendenz im Verständnis des Marktes ableiten, hardware-basierte Anwendungen würden für die Sicherung von digitalen Daten den vermeintlich einzigen Schutzzweck erfüllen können. Die Folge wäre eine unverhältnismäßige Marktkonzentration bei hardwarebasierten TSE-Herstellern, die zu alternativlosen Monopolisten aufgewertet würden. Unabhängig von diesem gesellschaftlich wenig wünschenswertem Befund eines Marktes ist der faktische Ausschluss von digitalem Wettbewerb in Form von cloudbasierten TSE-Lösungen weder mit technologieneutralen behördlichen Anforderungen noch gesetzlichen Vorgaben vereinbar.

II. Technische Erläuterungen zur Kernproblematik der geplanten Änderung des Anwendungserlasses

In der folgenden technischen Herleitung unserer vorangestellten Einschätzung hinsichtlich der marktlichen und politischen Auswirkungen des Änderungserlasses in seiner jetzigen Form möchten wir auf einzelne Aspekte vertieft eingehen. Dies soll darüber hinaus dem besseren Verständnis der faktischen Marktbedingungen sowie der technologischen Potentiale cloudbasierter Dienstleistungen zur Fiskalisierung beitragen.

Zu 2. im Unterpunkt i)

Vorliegende Formulierung aus dem Referentenentwurf zu I. Nr. 3, 3.2.11

"Aus den Sicherheitsvorgaben des BSI zur zertifizierten technischen Sicherheitseinrichtung geht hervor, dass die Sicherheitsmodulanwendung (SMA) in der physischen Einsatzumgebung des elektronischen Aufzeichnungssystems zu betreiben ist. Im Sinne der Sicherheitsvorgaben erstreckt sich die physische Einsatzumgebung auf den gesamten zusammenhängenden Bereich in der das elektronische Aufzeichnungssystem steht und für den der Betreiber des elektronischen Aufzeichnungssystems unmittelbar verantwortlich ist."

Wie die oben bereits getätigten Ausführungen zu I. Nr. 3, 3.2.11 verdeutlichen, formuliert die geplante Änderung des Anwendungserlass Anforderungen an den Integritätsschutz der Kommunikation zwischen ERS und TSE. Demnach ist die SMA in der physischen Einsatzumgebung der ERS zu betreiben. Die Einsatzumgebung wird dabei allerdings nicht näher definiert und lässt bereits dadurch Zweifel an der grundsätzlichen Eignung cloudbasierter TSE-Lösungen zu. Denn bei einer cloudbasierten TSE-Lösung liegt die Einsatzumgebung der SMA gerade innerhalb der Cloud.

Kommunikation zwischen TSE und ERS in verteilten Systemen

Entscheidender für den Schutz der Integrität der Kommunikation zwischen TSE und ERS sind die Konfigurationen die das Umgebungsschutzkonzept einer SMA an diese stellt als die nicht näher definierte Vorgabe, die SMA in der physischen Umgebung der ERS zu betreiben. Dabei ist ein Umgebungsschutzkonzept einer cloudbasierten TSE nachweislich imstande die Integrität, Vertraulichkeit und Authentizität der Kommunikation zwischen ERS und SMA sicherzustellen.

Darüber hinaus wird eine SMA, die in einer Cloudregion liegt auch aufgrund der allgemein für Cloudsysteme geltenden Sicherheitsvorkehrungen (z.B. Verschlüsselung) wirksam vor unerlaubtem Zugriff abgeschottet. Darin liegt ein großer Vorteil cloudbasierter TSE-Lösungen gegenüber hardwarebasierten TSE-Lösungen, die aufgrund ihrer tatsächlichen physischen Nähe zur ERS leichter kompromittierbar sind: Einmal an eine cloudbasierte SMA übermittelte Prozessdaten sind nachträglich nicht mehr manipulierbar. Damit erfüllen cloudbasierte TSE-Lösungen in besonderem Maße die gesetzlichen Vorgaben, die das Gesetz zum Schutz vor Manipulationen an digitalen Grundaufzeichnungen vom 22. Dezember 2016 (Kassengesetz) mit der Einführung des § 146a AO verfolgte.

Weitere Ausführungen zum Umgebungsschutzkonzept

Die durch die geplante Änderung des Anwendungserlasses formulierte Vorgabe, die SMA in der physischen Einsatzumgebung der ERS zu betreiben, sorgt nicht bereits dafür, dass die Kommunikation zwischen ERS und SMA geschützt wäre. Diese Aufgabe kommt den Spezifika des Umgebungsschutzkonzeptes zu, das hinsichtlich seiner Einzelbestandteile auf den Schutz der Integrität der Kommunikation zwischen ERS und SMA durch das BSI geprüft und zertifiziert wird. Dabei stellt das Umgebungsschutzkonzept cloudbasierter TSE-Lösungen nicht nur die Integrität der Kommunikation sicher, sondern sichert auch die Einzelbestandteile der SMA ab. So etwa ihre Softwareumgebung, den Transaktionszähler oder die Zugangsdaten für den Anbieter von Verschlüsselungsdienstleistungen (CSP-L, Crypto Service Provider Light).

Der bloße Einsatz in der physischen Einsatzumgebung schützt die Kommunikation zwischen ERS und SMA somit nicht wirksam. Weder bei TSE-Lösungen, die verteilte Systeme für sich nutzen, noch bei TSE-Lösungen, die hardwarebasierte TSE-Lösungen verwenden. Vielmehr sind immer technische und organisatorische Schutzmaßnahmen zu ergreifen, um die Integrität der Kommunikation zwischen ERS und SMA zu schützen. Das betrifft gleichermaßen die Cloudumgebung wie auch die Filiale des Steuerpflichtigen, und zwar unabhängig von der konkreten Beschaffenheit der TSE-Lösung – ob cloud- oder hardwarebasiert (z.B. in Form eines USB-Sticks oder einer micro-SD).

Petitum: Formulierungsvorschlag zu I. Nr. 3, 3.2.11 für den anstehenden Erlass

Die geplante Änderung des Anwendungserlasses sollte nicht auf die Verortung der SMA in der physischen Einsatzumgebung der ERS abstellen, sondern die SMA daran messen, ob sie das durch das BSI zu zertifizierende Umgebungsschutzkonzept vollumfänglich einhält. In der aktuellen Fassung des Referentenentwurfs ist nicht erkennbar, welches Ziel die definitorisch unklare Beschreibung einer sicheren Einsatzumgebung hat, wenn diese keinen zusätzlichen Sicherheitszweck bei der Kommunikation zwischen SMA und ERS erfüllt.

Zu 2. im Unterpunkt ii)

Vorliegende Formulierung aus dem Referentenentwurf zu I. Nr. 3, 3.2.12

„Ort eines elektronischen Aufzeichnungssystems ist der jeweilige Teil des elektronischen Aufzeichnungssystems, an dem die abzusichernden Geschäftsvorfälle inhaltlich, unabhängig von ihrer Formatierung oder Codierung, erstmalig vollständig vorliegen."

Wie bereits oben ausgeführt bestehen vor allem Unsicherheiten mit Blick auf definitorische Fragestellungen hinsichtlich des Ortes. Auf die Definition, was genau fehlt, wollen wir im Folgenden näher eingehen:

Definitorische Unklarheiten

Die Definition ist wie oben bereits beschrieben nicht hinreichend bestimmt. Es ist unklar, wann die abzusichernden Geschäftsvorfälle nach der vorgeschlagenen, obigen Formulierung bei verteilten Systemen vorliegen. Aufgrund der Infrastruktur von verteilten Systemen ist der Ort für den Anfall der Prozessdaten in der Cloud nicht näher bestimmbar. Mit diesem Missverständnis aus der grundlegenden Funktionsweise von Cloud-Systemen wird verdeutlicht, dass der Aufbau und Sinn von verteilten Systemen nicht berücksichtigt wurde.

Anders sieht es hingegen aus, wenn man den Ort nach den Anforderungen des Umgebungsschutzes dahingehend begreift, dass ERS und SMA zusammen in derselben physischen Einsatzumgebung sind, wenn sie tatsächlich miteinander kommunizieren. Nur dann kann die verwendete TSE an einem Ort, wie bei cloud- und hardwarebasierten Lösungen gleichermaßen vorgesehen, ohne große marktliche Auswirkungen definiert werden. Denn die Einsatzumgebung der SMA lässt ausschließlich Kommunikation zwischen ERS und SMA zu, welche die Sicherheitsanforderungen des BSI erfüllt. Demnach sind ERS und SMA in der gleichen physischen Einsatzumgebung, wenn diese Kommunikation zwischen ERS und SMA tatsächlich zustande kommt und von der physischen Einsatzumgebung der SMA nicht unterbunden wird. Dies kann nachgeprüft werden, indem man die signierten Transaktions-Logs, welche von dem Aufzeichnungssystem abgesichert wurden, exportiert.

Zweck des Ortes bei verteilten Systemen

Es stellt sich grundsätzlich die Frage, zu welchem Zweck genau ein Ort eines Aufzeichnungssystems festgestellt werden möchte. Laut § 146a Abs. 2 AO bezieht sich die Unmittelbarkeit der Absicherung nicht auf einen Ort, sondern auf den "unmittelbaren zeitlichen Zusammenhang mit dem Geschäftsvorfall". Daher erscheint der Ort bzw. erscheinen die Orte des ERS nicht relevant für die Absicherung der relevanten Transaktionsdaten zu sein.

Petitum: Formulierungsvorschlag zu I. Nr. 3, 3.2.12 für den anstehenden Erlass

I. Nr. 3, 3.2.12 enthält gänzlich neue Anforderungen an ein elektronisches Aufzeichnungssystem, welche in dieser Form nicht rational begründbar sind. Des Weiteren kann der Ort eines Aufzeichnungssystems laut dieser Definition bei verteilten Systemen mehr als einer sein oder auch mangels Betrachtung der Codierung gar nicht feststellbar sein. Dementsprechend sollte dieser Punkt gänzlich gestrichen werden.

Zu 2. im Unterpunkt iii)

Vorliegende Formulierung aus dem Referentenentwurf zu II. Nr. 2, 7.3

„Sofern die Nutzung eines elektronischen Aufzeichnungssystems mit Kassenfunktion erfolgt, dessen Ort (vgl. AEAO zu § 146a, Nr. 3.2.11) sich während desstabilen und störungsfreien Betriebs nicht auf einer lokalen Komponente befindet, sondern dieses über eine Internet- oder andere Kommunikationsverbindung angebunden ist, stellt der Ausfall dieser Kommunikationsverbindung einen Ausfall des elektronischen Aufzeichnungssystems dar (vgl. AEAO zu § 146a, Nr. 7.2). Eine zusätzlich lokal funktionierende Kassenfunktion, die bei einem Ausfall des elektronischen Aufzeichnungssystems nach Satz 1 dessen Aufgaben (insbesondere die Erfassung und Abwicklung von Zahlungsvorgängen) übernimmt (Notfallbetrieb), stellt ein zusätzliches lokales elektronisches Aufzeichnungssystem dar, daselbst die Voraussetzungen des § 146a AO und der KassenSichV erfüllen muss und mit einer zusätzlichen lokalen zertifizierten technischen Sicherheitseinrichtung zu schützen ist. Ein Notfallbetrieb ohne Absicherung durch eine zusätzliche lokale zertifizierte technische Sicherheitseinrichtung darf bei einem Ausfall des elektronischen Aufzeichnungssystems nicht verwendet werden."

Wie bereits beschrieben führen die Annahmen hinsichtlich der physischen Einsatzumgebung sowie der Bestimmung eines des Ortes in II. Nr. 2, 7.3 dazu, dass für den Notfallbetrieb ab Januar 2026 eine lokale TSE zwingend erforderlich ist.

Der Referentenentwurf geht von einer fehlgeleiteten Annahme für die zusätzliche Absicherung im Notfallbetrieb einer ERS hinsichtlich der „physischen Einsatzumgebung" sowie der Bestimmung „des Ortes" aus und folgert eine vermeintlich sicherheitstechnisch vorteilhaftere Lösung sei die Anwendung einer hardware-basierten TSE, die aber mit Mehraufwand verbunden ab Januar 2026 zusätzlich zertifiziert werden müsste.

Mit Inkrafttreten von II. Nr. 2, 7.3 am 1.Januar 2026 werden verteilte Systeme entsprechend gezwungen, eine "lokale" zertifizierte technische Sicherheitseinrichtung zu implementieren, die in der Funktionsweise einer cloudbasierten Lösung nicht angelegt und für die Sicherung von Transaktionsdaten beabsichtigt nicht vorgesehen ist. Bei Cloud TSE-Lösungen werden Störungsfälle jedoch kenntlich gemacht (Logs der Transaktionsdaten), so dass im Störungsfall zwar nicht weiter aufgezeichnet werden kann, jedoch gegenüber Steuerprüfbehörden sicher dokumentiert wird, dass ein Störungsfall vorlag.

Es befinden sich hingegen mit der cloudbasierten Lösung Aufzeichnungssysteme auf dem Markt, welche aufgrund ihrer Architektur und Funktionsweise nicht mit einer "lokalen" TSE abgesichert werden können. Durch den Wortlaut im vorliegenden Entwurf für die Änderung des Anwendungserlasses würden solche Systeme zukünftig in ungerechtfertigter Weise vom Wettbewerb ausgeschlossen.

Petitum: Formulierungsvorschlag zu II. Nr. 2, 7.3 für den anstehenden Erlass

Um Technologieneutralität und -offenheit zu wahren, sollte der gesamte Teil II. – insbesondere aber Nr. 2, 7.3 – ersatzlos gestrichen werden.