www.betriebs-berater.de

BB

Betriebs Berater

46 | 2024

Recht ... Wirtschaft ... Steuern ... Recht ... Wirtschaft ... Steuern ... Recht ... Wirtschaft ...

11.11.2024 | 79. Jg.
Seiten 2625–2688

Fachmedien Recht und Wirtschaft | dfv Mediengruppe | Frankfurt am Main

Dr. Axel-Michael Wagner, RA, und Stefan Groß, StB, CISA

Zu den neuen Vorgaben des BSI bei der Kassendatenfiskalisierung, oder: Die Grenzen administrativer Rechtssetzung im Rechtsstaat – Teil I

Im Gefolge von § 146a AO und der Kassensicherungsverordnung hat sich eine „Parallelwelt" aus administrativen Vorgaben des BSI entwickelt, deren Einhaltung immer höheren Aufwand erfordert. Derartige autonome Rechtssetzung durch die Exekutive im technischen Bereich fernab parlamentarischer Kontrolle wird im juristischen Diskurs nur selten im Detail hinsichtlich ihrer technischen Erforderlichkeit sowie aus verfassungsrechtlicher Perspektive hinterfragt, sondern üblicherweise hingenommen. Der nachfolgende Beitrag zeichnet im ersten Teil die historische Entwicklung, fokussiert auf die Vorgaben im Bereich Umgebungsschutz und PKI, nach und geht der Frage der gesetzlichen Ermächtigungsgrundlage für diese Vorgaben nach.

I. Einleitung

Durch Gesetz vom Dezember 2016 eingeführt und mit längerer Vorlaufzeit erstmals zur Anwendung ab dem 1.1.2020 vorgesehen hat das sog. „Kassengesetz"[1] in Form der §§ 146a, 146b AO seither durchaus zu Frustration bei den verschiedenen Beteiligten geführt, was sich nicht nur in einer mangels Verfügbarkeit von zertifizierten Produkten bis zum 1.4.2021 aufgeschobenen Anwendbarkeit widerspiegelt.[2] Ziel des Gesetzes war es, die Gleichmäßigkeit der Besteuerung zu sichern,[3] indem durch das neue „Kontrollinstrument" der Kassennachschau[4] Manipulationsmöglichkeiten steuerlicher Grundaufzeichnungen[5] in Betrieben mit Bargeld-Kundentransaktionen eingedämmt werden. Der Zweck ist damit die Validierung von für die Besteuerung relevanten Daten, nicht aber – wie in § 87b AO – die Übermittlung bzw. Zurverfügungstellung von für die Berechnung der Steuerlast durch den Steuerpflichtigen erheblichen Daten selbst.[6] Die einzudämmenden Manipulationen[7] hatten nach der Vermutung des Gesetzgebers[8] in der Vergangenheit zu erheblichen Steuerausfällen geführt. Noch kurz vor dem Gesetzgebungsverfahren hatte die Bundesregierung 2015 auf (sehr punktuelle) Erkenntnisse der Finanzverwaltung verwiesen, wonach einige Kassenhersteller ihre Systeme in der Regel bereits mit Manipulationsmöglichkeit auf den Markt bringen würden, um überhaupt verkäuflich zu sein.[9] Ungeachtet entsprechender Mechanismen zur Manipulation von digitalen Aufzeichnungen besteht allerdings die wohl einfachste und häufigste, durch Technik nicht vermeidbare Manipulationsmöglichkeit nach wie vor darin, Kassenvorgänge – etwa in einem Restaurant – gar nicht erst zu erfassen.[10] Die (finanz- und strafrechtliche) Rechtsprechung zu konkreten Manipulationsfällen gibt naturgemäß kein systematisches Bild wieder.[11] Der Gesetzgeber selbst scheint keine systematische Aufarbei-

1 Gesetz zum Schutz vor Manipulationen an digitalen Grundaufzeichnungen vom 22.12.2016 (BGBl. I 2016, 3152).

2 Vgl. exemplarisch *Hübner*, Neuer Streit um Regel-Wirrwarr, 14.9.2020, abrufbar unter https://www.lebensmittelzeitung.net/politik/nachrichten/Kassengesetz-HDE-geisselt-Regel-Wirrwarr-148253 (Abruf: 22.4.2024); FDP, Scholz tritt Wirtschaft in die Kniekehle, 15.9.2020, abrufbar unter https://www.fdp.de/scholz-tritt-wirtschaft-die-kniekehle (Abruf: 22.4.2024); bak/dpa, Wie die Kassenbonpflicht Händler in Deutschland in den Wahnsinn treibt, 10.12.2019, abrufbar unter https://www.stern.de/wirtschaft/news/kassenbonpflicht–haendler-muessen-teure-kassen-anschaffen—die-es-noch-gar-nicht-gibt-9041 252.html (Abruf: 22.4.2024).

3 Vgl. Gesetzesbegründung in BT-Drs. 18/9535, 1.

4 Vgl. Prüfungsmitteilung des Bundesrechnungshofes vom 4.10.2023, Gz. VIII 3/VIII 4 – 2020 – 0323, S. 6.

5 Der Begriff „Grundaufzeichnungen" wird – obwohl das Gesetz zur Einführung von § 146a AO als „Gesetz zum Schutz vor Manipulationen an steuerlichen Grundaufzeichnungen" betitelt wurde – in der AO nicht definiert und in § 146a Abs. 3 S. 1 Nr. 2 e) AO nur verwendet. In § 2 KassenSichV wird der Begriff zwar in der Überschrift verwendet, aber nicht definiert (letztlich behandelt diese Regelung die „Daten des Vorgangs" nach § 2 S. 2 Nr. 4 KassenSichV). Nach Niedersächsischem FG, 25.3.2003 – 6 K 961/99, EFG 2003, 1215, sind Grundaufzeichnungen die in § 147 Abs. 1 AO umschriebenen, aufbewahrungspflichtigen Informationen, was sich aber ebenfalls nicht aus dem Gesetzestext ergibt. In der Datensatzbeschreibung der DSFinV-K wird der Begriff letztlich nur ein einziges Mal erwähnt (Kap. 1.2), aber nicht definiert.

6 Nach § 158 AO sind die entsprechenden Grundaufzeichnungen „der Besteuerung zugrunde zu legen", soweit die elektronischen Daten nach der Vorgabe des § 146a AO zur Verfügung gestellt werden.

7 Nach der Gesetzesbegründung in BT-Drs. 18/9535, 11, betreffen die (nachträglichen) Veränderungen hinsichtlich steuerrelevanter Vorfälle insbesondere nicht dokumentierte Stornierungen, nicht dokumentierte Änderungen mittels elektronischer Programme oder den Einsatz von Manipulationssoftware (eingebaute Phantomware, Internet-Zapper). Vgl. dazu auch *Teutemacher*, AO-StB 2020, 123.

8 Vgl. BT-Drs. 18/4660, 1: „Eine Schätzung des jährlichen Steuerausfalls durch Betrug mit manipulierten Registrierkassen ist der Bundesregierung nicht möglich, da es an belastbaren Grundlagen für eine Berechnung fehlt", S. 2: „Eine Schätzung der Bundesregierung des jährlichen Steuerausfalls durch Bar- bzw. Neben-der-Kasse-Geschäfte ist der Bundesregierung nicht möglich."

9 Vgl. BT-Drs. 18/4660, 2. Um welches Volumen es bei den im Rahmen des hier einzig konkret angeführten Berichts der OFD Münster und Rheinland von 2012 angeführten 136 Fällen „in zurückliegenden Prüfungszeiträumen" insgesamt ging, wird nicht mitgeteilt. Das Finanzministerium des Landes Nordrhein-Westfalen schätzte seinerzeit den bundesweiten Steuerausfall aus Kassenmanipulation auf 5 bis 10 Mrd. Euro. Die dafür angegebene Quelle ist allerdings nicht zugänglich. Weder der Gesetzesbegründung von 2016 noch im Bericht des Finanzausschusses (BT-Drs. 18/10667) wird auf die zugrundeliegenden Erkenntnisquellen eingegangen (vgl. dazu auch Wortprotokoll der 89. Sitzung des Finanzausschusses des Bundestages, S. 28 – Klaudia Peters, Bundesrechnungshof). In einer Prüfungsmitteilung des Bundesrechnungshofes vom 4.10.2023 (Gz. VIII 3/VIII 4 – 2020 – 0323) werden nicht namentlich „andere Quellen" erwähnt, wonach sich der Schaden auf jährlich bis zu 70 Mrd. Euro belaufe, und auf einen Artikel in der WirtschaftsWoche vom 13.12.2019 verwiesen, wonach die in den Jahren 2017/2018 festgestellten Betrugsquoten in der Berliner Gastronomie bei 80 %, im Taxigewerbe bei 50 % und in Spielhallen bei 66 % liegen.

10 Auf dieses fortbestehende Szenario weisen sowohl der Bundesrat in seiner Stellungnahme zum Gesetzentwurf (BT-Drs. 18/9957, 2) als auch der Bundesrechnungshof unter Verweis auf BMF-Äußerungen hin (vgl. Prüfungsmitteilung des Bundesrechnungshofes vom 4.10.2023 (Gz. VIII 3/VIII 4 – 2020 – 0323, S. 19). In diesen Fällen findet dann keine Eingabe in das Kassensystem statt und es wird – entgegen der Belegausgabepflicht des § 146a Abs. 2 AO, welche der Bundesrat zur Verhinderung dieses Szenarios angemahnt hatte – kein Bon ausgestellt (vgl. auch *Teutemacher*, AO-StB 2020, 123). Identifizierbar ist dies nur bei Testkäufen der Finanzverwaltung oder durch „whistle blower", denn ein ausgestellter und nicht vom Kunden entgegengenommener Bon muss nicht aufbewahrt werden, vgl. AEAO zu § 146a, Tz. 2.5.8. Vgl. auch Gegenäußerung der Bundesregierung in BT-Drs. 18/9957, 4: „Sofern Unternehmer und Kunde im Vorfeld vereinbaren, dass kein Beleg ausgestellt werden soll (kollusives Zusammenwirken) und der Umsatz überhaupt nicht erfasst wird, kann dieser Umstand auch durch eine Belegausgabepflicht nicht verhindert werden".

11 Vgl. FG Rheinland-Pfalz, 7.1.2015 – 5 V 2068/14, DStRE 2016, 40, zu Manipulationssoftware zur Umsatzverkürzung; LG Oldenburg, 19.5.2021 – 2 KLs 940 Js 26952/18, BeckRS 2021, 50929 mit Revision zum BGH, 8.3.2022 – 1 StR 360/21, NZWiSt 2022, 379; LG Osnabrück, 28.11.2019 – 2 KLs 2/19, FD-Strafrecht 2019, 422557, zu einer speziellen Pro-

tung zu beabsichtigen, welche (technischen) Manipulationsmöglichkeiten durch die neuen Regelungen überhaupt wirksam beseitigt wurden oder, umgekehrt formuliert, welchen in der Praxis nicht relevanten, theoretischen Risiken durch hinsichtlich ihres Aufwands außer Verhältnis stehenden Maßnahmen begegnet wurde.[12] Geplant ist lediglich, vier Jahre nach erstmaliger Anwendung – also 2024/2025 – zu evaluieren, ob Wirtschaftlichkeit und Effizienz durch den verstärkten Einsatz von Informationstechnologie gestiegen sind und ein „zielgenauer Ressourceneinsatz" stattgefunden hat,[13] was immer das im Einzelnen bedeuten mag. Zudem sollte das Statistische Bundesamt „voraussichtlich" zwei Jahre nach Inkrafttreten des Gesetzes eine „ex-post Folgekostenvalidierung bei den Normadressaten durchführen".[14] Beides liegt bislang nicht vor. Ohnehin hielt es die Bundesregierung schon 2015 für ausgeschlossen, dass eine (zukünftige) Aussage darüber möglich sein wird, ob die Größenordnung vermuteter Steuerausfälle durch das Gesetz signifikant reduziert wurden.[15]

Nach § 146a Abs. 1 S. 1 und 5 AO ist es verboten, ein elektronisches Aufzeichnungssystem – insbesondere Kassensystem – in den Verkehr zu bringen, das nicht „jeden aufzeichnungspflichtigen Geschäftsvorfall und anderen Vorgang einzeln, vollständig, richtig, zeitgerecht und geordnet aufzeichnet". Diese Vorgabe an die Hersteller von Kassensystemen, obwohl bußgeldbewehrt,[16] erschien dem Gesetzgeber wohl von Anfang an als zu stumpfes Schwert, sonst hätte es einer zusätzlichen Absicherung in Gestalt der zertifizierten technischen Sicherheitseinrichtung (TSE) in § 146a Abs. 1 S. 2 bis 4 AO gar nicht bedurft. Während das Kassensystem ordnungsgemäße „Quelldaten" im richtigen Format anzuliefern hat und die TSE hierauf auch angewiesen ist,[17] soll der Einsatz der TSE diese Quelldaten in erster Linie gegen *nachträgliche* Manipulationen schützen. Erstmals hat der deutsche Steuergesetzgeber damit die Verwendung einer technischen „Einrichtung" ausschließlich zu Zwecken der Überprüfung steuerrelevanter Daten vorgegeben. Doch die zumindest in der Vergangenheit mutmaßlich üblichen Vorrichtungen, um die Aufzeichnung von Daten (und die Ausgabe von Bons) temporär auszusetzen, können funktional nach wie vor im Kassensystem selbst umgesetzt werden, ohne dass dies anhand der TSE-Daten nachvollziehbar wäre.[18] Ebenso kann eine Zweitkasse mit einer „Schwarz-TSE" betrieben werden.[19] Im Unterschied zum elektronischen Aufzeichnungssystem selbst, das nur sehr abstrakten rechtlichen Vorgaben unterliegt und als solches auch kaum Untersuchungsobjekt einer Betriebsprüfung oder eines Ermittlungsverfahrens wird,[20] wurden die TSE und ihre IT-Ausführungsumgebung jedoch einem fein ziselierten Geflecht von (Sicherheits-)Vorgaben des Bundesamts für Sicherheit in der Informationstechnik (BSI) unterworfen, die im steuerrechtlichen Umfeld in ihrer technischen Spezifität ihresgleichen suchen. Die diesbezüglichen Rechtsquellen führen, wie unten noch zu zeigen ist, ein vom Gesetzgeber letztlich nicht mehr beachtetes „Eigenleben". Man mag sich ausmalen, was passieren würde, wenn etwa die DSGVO in gleicher Weise vom BSI „konkretisiert" worden wäre.

Die ursprünglich vom Statistischen Bundesamt prognostizierten Kosten der Umsetzung des Gesetzes[21] sind mit großer Wahrscheinlichkeit um Größenordnungen zu niedrig angesetzt worden.[22] Zwar sind neue (TSE-)Dienstleister, (TSE-)Hersteller und (TSE-)Produkte entstanden, aber bei den betroffenen Steuerpflichtigen entstanden nicht nur

grammdatei, die versteckt installiert wurde und mit deren Hilfe die über den Tag eingegebenen Umsätze nachträglich verringert werden konnten; FG Berlin-Brandenburg, 20.10.2017 – 4 K 4206/14, BeckRS 2017, 133609: „eine Manipulation wegen nicht vorgelegter Programmierungsprotokolle der elektronischen Kasse und in den Streitjahren erfolgter unterdrückter Stornos [erscheint] naheliegend"; VG Anspach, 26.11.2013 – AN 4 K 13.01021/01022, BeckRS 2013, 23024: „jahrelanger Einsatz von Manipulationssoftware", „tägliche manuelle Änderung der Kassenbestände". Bei derartigen Fällen ist generell zwischen der Bedienung (d. h. der Nutzung der vorgegebenen Möglichkeiten) und der nachträglichen Manipulation der Daten selbst „auf digitaler Ebene" zu unterscheiden. Im Sachverhalt der Grundsatzentscheidung des BFH, 11.1.2017 – X B 104/16, BFH/NV 2017, 561, waren die mit der Kasse erstellten Rechnungen und verschiedene weitere Ausdrucke gar nicht aufbewahrt worden und alle übrigen Berichte aus dem Speicher gelöscht worden. Hinzu kamen zahlreiche Buchungsfehler. Die Buchführung war im gesamten Prüfungszeitraum nicht ordnungsgemäß gewesen. Unter diesen weiteren Umständen forderte der BFH bei grundsätzlich bestehender Manipulationsmöglichkeit einer Registrierkasse eine Darlegung über die Programmierung der Kasse selbst. Um die nachträgliche Manipulation von Speicherinhalten des Kassensystems ging es dabei nicht. Im Fall des FG Berlin-Brandenburg, 13.8.2013 – 2 K 2229/10, BeckRS 2016, 95050, wurde der „Z-Bon-Zähler mehrfach jährlich auf null zurückgestellt", dass „die fortlaufende und vollständige Erfassung aller Bons nicht mehr gewährleistet ist".

12 Dazu bedürfte es einer Analyse des durch sämtliche Regelungsebenen (Gesetz, Verordnung, BSI-Richtlinien, BSI-Schutzprofile, BSI-"Nebenregelungen") geschaffenen Gesamtsituation inklusive der Kenntnis, welche anfänglichen und welche nach wie vor bestehenden (Steuerausfall- bzw. Missbrauchs-) Risiken sich tatsächlich in welchem Umfang realisiert hatten und nach wie vor realisieren. Dem vor und nach 2020 von Verbänden und Steuerpflichtigen erhobenen Vorwurf der Überregulierung in technischen Details, die zu unangemessen erhöhten Kosten für Kassen-Aufzeichnungssysteme geführt haben soll, wurde seitens des Gesetzgebers bislang nicht nachgegangen. Vgl. auch Stellungnahme des Bundesrates zum Gesetzentwurf in BT-Drs. 18/9957, 2, zur Manipulationsbekämpfung durch eine „technische Komponente": „Zu befürchten ist vielmehr, dass der Gesetzentwurf außer höheren Kosten für alle Beteiligten, keine weitere Wirkung entfalten wird."

13 Vgl. BT-Drs. 18/9535, 18.

14 Vgl. BT-Drs. 18/9535, 18.

15 Vgl. BT-Drs. 18/4660, 2: „Ob es bei Einsatz einer vorgeschriebenen technischen Sicherheitslösungen für Registrierkassen (z. B. kryptographische Signierung jeder Erfassung) durch mögliche Ausweichreaktionen zu einem höheren Steuerausfall kommt, hängt vom Verhalten der Steuerpflichtigen ab und kann durch die Bundesregierung nicht prognostiziert werden."

16 § 379 Abs. 1 S. 1 Nr. 6 AO.

17 Aufgabe der TSE ist es nicht (und könnte es technisch auch gar nicht sein), sicherzustellen, dass die Quelldaten des elektronischen Aufzeichnungssystems den materiellrechtlichen Vorgaben des § 146a Abs. 1 S. 1 AO entsprechen.

18 Man kann die „Überbrückung" der TSE lediglich am Bon – wenn denn einer verlangt und ausgegeben wird – erkennen. Vgl. auch SMAERS-Schutzprofil des BSI, Kap. 3.2: „The TOE [d. h. die SMAERS-Komponente als Teil der TSE] does not protect against threats that result from temporarily or permanently not using an ERS as required by law".

19 Vgl. Prüfungsmitteilung des Bunderechnungshofs vom 23.10.2023, Gz. VIII 3/VIII 4 – 2020 – 0323, Ziff. 4.4.4, sowie *Teutemacher*, AO-StB 2020, 123, 124. Ebenso ist denkbar, falsche TSE- bzw. Signaturinformationen auf einen ansonsten scheinbar korrekten Bon aufzudrucken und das Risiko der Entdeckung im Rahmen einer Kassen-Nachschau einzugehen.

20 Auch über vier Jahre nach der Einführung sind Fälle von Ermittlungen nach § 379 Abs. 1 S. 1 Nr. 6 AO im Hinblick auf elektronische Aufzeichnungssysteme – ebenso wie für TSE-Systeme – nicht bekannt geworden, geschweige denn sind gerichtliche Entscheidungen dazu ersichtlich. In der finanzgerichtlichen Rechtsprechung geht es, soweit ersichtlich, ausschließlich um formale Aspekte der Nichtvorlage von Programmierprotokollen bzw. -unterlagen, nicht aber um eine Untersuchung des Kassensystems selbst durch einen (IT-) Experten.

21 Vgl. BT-Drs. 18/9535, 2: „Für die Wirtschaft entsteht ein einmaliger Erfüllungsaufwand i. H. v. rd. 470 Mio. Euro für die Neuanschaffung und Umstellung der Geräte und jährlich laufender Erfüllungsaufwand i. H. v. rd. 106 Mio. Euro für die Kosten der Zertifizierung, Personalkosten für die Mitwirkung bei der Kassen-Nachschau sowie laufende Kosten für Wartung und Support." Weiter a. a. O., S. 15/16. Das Statistische Bundesamt ging u. a. davon aus, dass jede Kasse in Zukunft bei Neuanschaffung eine TSE als Modul enthalten würde (für 10 Euro pro Modul; tatsächlich kosten derartige Module derzeit zwischen 200 und 300 Euro), dass es bei der Ersetzung vorhandener Kassensysteme um „Sowieso-Kosten" gehe, die nicht eigenständig ins Gewicht fallen, und dass sowohl jede Kassen-Nachschau als auch jede Beschaffung und Installation einer TSE einen Zeitaufwand von 30 Minuten verursacht. Der Zeitbedarf einer Kassennachschau wird hingegen vom Bundesrechnungshof (Prüfungsmitteilung vom 23.10.2023, Gz. VIII 3/VIII 4 – 2020 – 0323, Ziff. 0.7) mit 90 bis 190 Minuten, einschließlich Vor- und Nacharbeiten 1,4 Arbeitstage veranschlagt. Themen bei Filialisten wie die Anbindung an Archivsysteme, Änderungen von IT-Landschaften durch veränderte Datenströme, Aktualisierung von Verfahrensdokumentationen, Beschaffung von laufenden Cloud-Dienstleistungen, vorzeitige Aktualisierung von Hardware etc. wurden in die ursprüngliche Ermittlung nicht mit einbezogen.

22 Vgl. schon DStV, Stellungnahme S 05/16 vom 25.4.2016, zum Kassengesetz, S. 6 unter I, abrufbar unter https://www.bundesfinanzministerium.de/Content/DE/Gesetzestexte/Gesetze_Gesetzesvorhaben/Abteilungen/Abteilung_IV/18_Legislaturperiode/Gesetze_Verordnungen/2016-12-28-Kassenmanipulationsschutzgestz/Stellungnahme-14-DStV.pdf?__blob=publicationFile&v=1 (Abruf: 22.4.2024); HDE, Kassenbon-Pflicht bürokratisch und umweltschädlich, 17.12.2019, abrufbar unter https://einzelhandel.de/presse/pressearchiv/1399-pressemitteilungen-2019/12484-kassenbon-pflicht-buerokratisch-und-umweltschaedlich (Abruf: 22.4.2024); Handelsverband: Bonpflicht trägt nicht zur Eindämmung von Steuerbetrug bei, 27.12.2019, abrufbar unter https://www.deutsche-apotheker-zeitung.de/news/artikel/2019/12/27/handelsverband-bonpflicht-traegt-nicht-zur-eindaemmung-von-steuerbetrug-bei (Abruf: 24.4.2024).

(spiegelbildlich) wesentlich höhere Erst-Anschaffungskosten für TSE-Systeme bzw. -Dienstleistungen als veranschlagt,[23] sondern es entstehen auch bei jeder Veränderung des komplexen und mehrschichtigen Regelungsdschungels Umstellungs- und Folgeinvestitionen in einer nie anfänglich bedachten oder nachträglich erhobenen Höhe.

Die Finanzverwaltung konnte ihr Ziel einer höheren Kontrolldichte hinsichtlich der Regelungsumsetzung durch die Normadressaten nicht erreichen. Jährlich sollte bei 2,4 % sämtlicher Betriebe eine Kassen-Nachschau erfolgen. Eine Prüfung des Bundesrechnungshofs zu Verfahren, Möglichkeiten und Wirksamkeit der Kassen-Nachschau nach § 146b AO kam im Oktober 2023 zu dem Ergebnis, dass im gesamten betrachteten Vier-Jahres-Zeitraum von 2018 bis 2021 insgesamt 4,0 % der Betriebe geprüft wurden und das Jahresziel dementsprechend deutlich unterschritten worden ist.[24] Das ursprüngliche Ziel entspricht einem Nachschauturnus von 42 Jahren, tatsächlich beträgt der Nachschauturnus in verschiedenen Zweigen der Bargeldbranche mehr als 100 Jahre.[25] Zudem gibt es nur wenige Erfahrungen im praktischen Umgang mit § 146a AO geschweige denn einschlägige Rechtsprechung.[26] Ohnehin ist fraglich, ob und wie die Finanzverwaltung im Rahmen einer Kassen-Nachschau oder Betriebsprüfung eine ordnungsgemäße Umsetzung der komplexen rechtlich-technischen Vorgaben zu TSE-Architekturen überhaupt im Einzelnen prüfen kann, insbesondere, ob ein System vollständig im Rahmen der BSI-Zertifizierung betrieben wird.[27]

Vor diesem Hintergrund soll nachfolgend anhand einzelner Beispiele aufgezeigt werden, wie sich die Rechtsquellen „unterhalb" von § 146a AO im Hinblick auf bestimmte Fragen der TSE-Architektur entwickelt haben und welche Probleme sich dadurch – sowohl rechtlich als auch bei der praktischen Umsetzung – ergeben. Dabei fokussiert sich die Darstellung auf TSE-Architekturen, bei denen einzelne Komponenten in der Cloud betrieben werden, im Gegensatz zu Hardware-TSEs in Form eines (verkürzt ausgedrückt) „USB-Steckers", der eine vollständige TSE enthält. Aus unterschiedlichen technischen, organisatorischen und teils auch finanziellen Gründen[28] ist für viele Steuerpflichtige, insbesondere aber für große Filialisten, die Verwendung von Hardware-TSEs nicht bzw. nur mit großen Einschränkungen und unverhältnismäßigem Aufwand umsetzbar.

II. Die Delegationskette des § 146a AO

Die 2016 eingeführte Regelungskonstruktion spiegelt die Misere eines „Technik-Gesetzgebers" wider. In abstrakt-funktionaler Sprache wurden verschiedene neue Begriffe kreiert,[29] deren Ausfüllung der Gesetzgeber dem Verordnungsgeber überließ. Schon diese „Regelungstechnik" ist verfassungsrechtlich im Kontext von Art. 80 GG nicht unbedenklich,[30] zumal in der Gesetzesbegründung zu § 146a AO bereits Inhalte dieser neuen Gesetzesregelung und der kurz darauf verabschiedeten KassenSichV vermischt werden[31] und § 1 Abs. 1 S. 1 KassSichV fälschlicherweise „elektronische Aufzeichnungssysteme im Sinne des § 146a Abs. 1 S. 1 AO" definiert anstatt, wie in der Ermächtigungsgrundlage in § 146a Abs. 3 S. 1 Nr. 1 AO vorgesehen, diejenige Teilmenge (nämlich Kassensysteme) der elektronischen Aufzeichnungssysteme zu definieren, „die über eine zertifizierte technische Sicherheitseinrichtung verfügen müssen".[32] Auf die Probleme der Regelungstechnik wurde im Gesetzgebungsverfahren hingewiesen.[33] In der Literatur hingegen wurde später (im Wesentlichen vor 2020) lediglich vertieft über die Frage diskutiert, ob die Entscheidung, welche elektronischen Aufzeichnungssysteme durch eine TSE abzusichern sind, vom Gesetzgeber hätte getroffen werden müssen.[34]

Der im Gesetz geprägte Kernbegriff der Regelungen ist die TSE selbst, von der die abstimmenden Bundestagsabgeordneten vermutlich eine allenfalls sehr vage Vorstellung hatten,[35] und die – im Wege der Ersetzung von undefinierten Begriffen durch undefinierte Begriffe – aus einem Sicherheitsmodul, einem Speichermedium und einer einheitlichen digitalen Schnittstelle[36] bestehen sollte. Der Verordnungsgeber der „Kassensicherungsverordnung" (KassenSichV), das BMF, führte diese Regelungstechnik fort und delegierte die Festlegung der technischen Anforderungen im Wesentlichen weiter, nämlich in § 5 Kassen-

23 In diesem Zusammenhang weist beispielsweise *Achilles*, DB 2019, 1920, 1927, auf die Kosten der Belegausgabepflicht hin und dass diese Kosten keine sachliche Härte im Rahmen von § 148 AO darstellen.

24 Vgl. Prüfungsmitteilung vom 23.10.2023 (Gz. VIII 3/VIII 4 – 2020 – 0323), Ziff. 0.3, 4.1.2 (die vorläufigen Feststellungen des Bundesrechnungshofes datieren vom 12.5.2023). Eine Steigerung innerhalb dieses Zeitraums ergibt sich aus den Daten auch nicht.

25 Bundesrechnungshof, Prüfungsmitteilung vom 23.10.2023 (Gz. VIII 3/VIII 4 – 2020 – 0323), Ziff. 5.1.

26 Auch die Entscheidung des FG Düsseldorf, 13.9.2023 – 5 V 1048/23 A (E,G,U,F), StB 2023, 386, bezieht sich noch auf die vorherige Rechtslage.

27 Da beispielsweise – insoweit nachfolgend Fokus des vorliegenden Beitrags – die Umgebungsschutzvorgaben im Laufe der Zeit und der Zertifizierungen von Hersteller zu Hersteller variieren, ist eine automatisierte Prüfsoftware der Finanzverwaltung etwa für diese Komponente der Zertifizierung kaum denkbar.

28 Vgl. *Kowallik*, DB 2022, 2697, 2698: „Für die Stpfl. sind Cloud-TSE oft günstiger, da keine Hardware notwendig ist".

29 Technische Sicherheitseinrichtung, Sicherheitsmodul, Speichermedium, einheitliche digitale Schnittstelle, Grundaufzeichnungen, elektronisches Aufzeichnungssystem, aufzeichnungspflichtige Geschäftsvorfälle, andere Vorgänge.

30 Nach BVerfG, 19.9.2018 – 2 BvF 1/15, 2 BvF 2/15, NVwZ 2018, 1703, Rn. 243, muss der Gesetzgeber „hinreichend genaue Zielvorgaben" machen und diejenigen Regelungen erlassen, „aus denen ein bestimmt umrissenes Handlungsprogramm für die Exekutive abgeleitet werden kann und die die erforderlichen Abwägungsentscheidungen hinsichtlich konkurrierender Rechtspositionen enthalten". Die genannte Entscheidung bezog sich dabei auf die Volkszählung 2011, wobei das Zensusgesetz 2011 im Unterschied zu § 146a AO das „Ergebnis eines über ein Jahrzehnt angelegten komplexen Prozesses [darstellt], in dem normative und fachliche Anforderungen kontinuierlich miteinander abgeglichen worden sind und der Spielraum des Gesetzgebers hinsichtlich der verfahrensrechtlichen Ausgestaltung nach und nach verengt wurde".

31 Vgl. BT-Drs. 18/9535, 20, vermutlich wegen § 62 Abs. 2 S. 2 GGO. Vor diesem Hintergrund ist bei einigen zentralen Weichenstellungen und aufgrund der Tatsache, dass die KassenSichV und ihre späteren Änderungen der Zustimmung des Bundestages und des Bundesrates bedurften, gleichwohl unverständlich, warum diese nicht – gerade wegen Art. 80 GG – in § 146a AO aufgenommen wurden.

32 Auch diese Gesetzesformulierung ist – ebenso wie § 146 Abs 1 S. 2 AO – inhaltlich nicht richtig. Es geht nicht darum, das elektronische Aufzeichnungssystem selbst (d. h. als solches) zu schützen oder dass dieses über eine TSE als integralen Bestandteil „verfügen" muss, sondern darum, dass die vom elektronischen Aufzeichnungssystem produzierten Datensätze über erfasste „aufzeichnungspflichtige Geschäftsvorfälle oder andere Vorgänge" als solche „geschützt" werden. Ein Eingriff durch die TSE in das elektronische Aufzeichnungssystem findet nicht statt, sondern die TSE wird „angebunden" (so die Formulierung des BSI, vgl. TR-03153, Kap. 5.1).

33 Vgl. Wortprotokoll der 89. Sitzung des Finanzausschusses des Bundestages, S. 17 (Carsten Rothbart, Zentralverband des Deutschen Handwerks e. V.): „Zum einen wird das elektronische Aufzeichnungssystem an eine Rechtsverordnung delegiert. Für uns ist es nicht nachvollziehbar, wie dieses Kernelement, was denn eigentlich nun in den Anwendungsbereich fallen soll, erst in einer Verordnung geregelt werden soll. Dieser Punkt ist so wesentlich, dass er schon von Verfassung wegen im Gesetz selbst geregelt werden müsste. Ferner besteht hier natürlich die Gefahr, dass im Nachgang ohne Einfluss des Bundestages – denn die Verordnungsermächtigung ist von den Ministerien mit Zustimmung aus dem Bundesrat zu erlassen – der Anwendungsbereich weiter gefasst wird, als sich dies jetzt im Moment nach den Plänen des in Diskussion befindlichen Gesetzesentwurfs darstellt. Wir befürchten im Nachgang dort nachträgliche Verschärfungen. Von daher ist unser Petitum, den Anwendungsbereich im Gesetz selbst, also in der Abgabenordnung, zu regeln."

34 Vgl. *Haselmann*, in: Koenig, AO, 5. Aufl. 2024, § 146a, Rn. 16, m. w. N.

35 Zumal die Gesetzesbegründung in BT-Drs. 18/9535, 14, zwar im Zusammenhang mit der damals alternativ evaluierten „INSIKA-Technik" von einer „kryptographischen Signierung einer jeden Aufzeichnung nach Abschluss des Geschäftsvorfalls" spricht, beim letztlich aber vom Gesetzgeber gewählten „Zertifizierungsverfahren" jeder Hinweis auf eine Signierung der Vorfallsdaten (als identische technische Basis) fehlt. Vielmehr werden hier die Begriffe „Zertifizierung" und „Signierung" austauschbar verwendet („Das Zertifizierungsverfahren ist geeignet, die Integrität (Unveränderbarkeit) und Authentizität (Herkunft der Daten) zu sichern").

36 Gemeint war damit keine physische Schnittstelle (wie USB oder HDMI), sondern eine Datensatzbeschreibung („Digitale Schnittstelle Finanzverwaltung-Kassen", DSFinV-K), auch für den standardisierten Export der abgesicherten Aufzeichnungen, und eine Datenschnittstelle zur Übermittlung von Datensätzen des Kassensystems an das Sicherheitsmodul der TSE (Einbindungsschnittstelle).

SichV an das BSI. Die Möglichkeit der Weiterdelegation an das BSI sieht § 146a Abs. 3 S. 3 AO zwar (als „kann"-Regelung) für die Bestimmungen der Anforderungen an Sicherheitsmodul, Speichermedium und einheitliche digitale Schnittstelle vor – der Verordnungsgeber hat davon weitreichend Gebrauch gemacht (§ 5 KassenSichV)[37] –, nicht aber für die Anforderungen an die Zertifizierung der TSE selbst (§ 146a Abs. 3 S. 1 Nr. 2 lit. g) AO), die in § 11 KassenSichV seitens des Verordnungsgebers durch Verweis auf das BSI-Gesetz und weitere Regelungen ausformuliert wurden. Die Weiterverweisung auf das BSI ist im Kontext des Art. 80 GG nicht unproblematisch, denn die Einbindung des Bundestages und des Bundesrates in die Entstehung der KassenSichV ist prominent geregelt (§ 146a Abs. 3 S. 4 bis 8 AO), während diese Kontrolle bei der Weiterdelegation an das BSI vollständig aufgegeben wird. Das BSI kann dann also formal im Rahmen der Begriffe (wie „Sicherheitsmodul") ohne Begründungs-[38] oder Zustimmungserfordernis[39] unkontrolliert seine eigenen Vorgaben frei erlassen, deren Einhaltung im Rahmen seiner eigenen Zertifizierungserteilungen prüfen und deren Einhaltung „im Feld" überwachen. Das ist auch deshalb bedeutsam, weil der Gesetzgeber wörtlich nur die „Anforderungen an" die einzelnen Bestandteile der TSE delegiert hat, nicht aber die „Definition" der Begriffe selbst. Aufgrund des Umstands, dass der Gesetzgeber selbst von einer Definition abgesehen hat, definiert das BSI diese Begriffe nun letztlich inhaltlich selbst und spezifiziert nicht nur im Rahmen einer gesetzgeberischen Definition die technischen Anforderungen im Detail. Es wird noch darauf zurückzukommen sein, dass der Gesetzgeber verfassungsrechtlich eine solche Delegation an die Exekutive nur unter besonders ausführlicher Vorgabe inhaltlicher „Leitplanken" vornehmen darf. Im Gesetzgebungsverfahren[40] – und in späterer Literatur[41] – wurde auf die Probleme auch dieser Weiterverweisung konkret hingewiesen.

Ungeachtet der Vermischung von rechtssetzender und vollziehender Gewalt erließ das BSI auf Basis der Weiterdelegation seit 2018 verschiedene technische Richtlinien,[42] Prüfkriterien und Testfälle, Schutzprofile und (Online-)FAQs[43] zur TSE und ihren Bestandteilen. In der Folge zertifizierte das BSI verschiedene Lösungen von (TSE-)Anbietern auf Basis von §§ 11 KassenSichV, 9 BSI-Gesetz und der „BSI-Zertifizierungs- und Anerkennungsverordnung" (BSIZertV). Rein formal ist ein Sicherheitszertifikat hiernach zu erteilen, „wenn informationstechnische Systeme, Komponenten, Produkte oder Schutzprofile den vom Bundesamt festgelegten Kriterien entsprechen".[44] So definierte das BSI in der Technischen Richtlinie TR-03153, dass das in § 146a Abs. 1 S. 3 AO erwähnte „Sicherheitsmodul" (als Teil einer TSE) aus einer Sicherheitsmodulanwendung (SMAERS-Komponente) und einem Krypto-Kern (CSP-Komponente) bestehen muss. Hinsichtlich der SMAERS-Komponente wurden 2020 vom BSI im SMAERS-Schutzprofil[45] technische Angriffsszenarien und abstrakt Maßnahmen zu deren Verhinderung definiert. Die Effektivität der vom TSE-Hersteller jeweils im Rahmen seiner Lösung konkretisierten Maßnahmen wird dann im Rahmen des BSI-Zertifizierungsprozesses überprüft.

Die Vorgaben des BSI orientierten sich an der ursprünglichen Vorstellung, dass eine TSE ein „Stück Hardware", etwa ein USB-Steckgerät, ist. Offensichtlich wurde dabei der Umfang und die Vielfalt der am Markt schon erhältlichen Kassensystemlösungen – einschließlich Cloud-Lösungen – unterschätzt. Auch bei der Öffnung der ersten Entwürfe für weitere technologische Konzepte, um die vielbeschworene Technologieoffenheit[46] umzusetzen, wurden weiterhin auf dieser Grundvorstellung einer hardware-gebundenen TSE basierende Konzepte vorgegeben. So ging das BSI schon im ursprünglichen SMAERS-Schutzprofil 2020 davon aus – was hier nachfolgend unter dem Stichwort „Umgebungsschutz" einen thematischen Fokus bilden soll –, dass sich eine lokale SMAERS-Komponente auf einer „zugrundeliegenden Plattform mit einem sicheren Speicher" befinden muss.[47] Diese lokale (Ausführungs-)Plattform soll die SMAERS-Komponente gegen „Manipulation und Missbrauch" schützen, eine „sichere Ausführungsumgebung" bereitstellen und in diesem Rahmen u. a. sicherstellen, dass Update-Pakete verifiziert werden und ein „sicherer Speicher für sensible Objekte" vorhanden ist. Genauere Ausführungen, wie diese Sicherheit erreicht werden soll bzw. welches Maß an Sicherheit erforderlich ist, enthält das Schutzprofil nicht. Da das BSI nur TSE-Lösungen außerhalb einer Hardware-TSE – also Cloud-Lösungen – zertifiziert, bei denen der TSE-Hersteller die „richtigen" konkreten Anforderungen an den vom bzw. beim Steuerpflichtigen einzuhaltenden Umgebungsschutz festgelegt hat, bestand für TSE-Hersteller das Risiko, dass (Re-)Zertifizierungen ihrer TSE-Produkte abgelehnt werden.[48] Bei den Steuerpflichtigen bestand spiegelbildlich die Besorgnis, Cloud-TSEs u. a. wegen Nichteinhaltung von Umgebungsschutz-Vorgaben nicht rechtskonform zu betreiben und deshalb dem Risiko von Ordnungswidrigkeiten ausgesetzt zu sein.[49] Wie genau die

37 Im Hinblick auf die einheitliche digitale Schnittstelle umfasst die Weiterdelegation (nur) „den standardisierten Export aus dem Speichermedium und die Anbindung der zertifizierten technischen Sicherheitseinrichtung an das elektronische Aufzeichnungssystem" (§ 5 S. 1 Nr. 1 KassenSichV) im Unterschied zu den auf Basis von § 4 KassenSichV vom Steuerpflichtigen im Rahmen des Datenzugriffs in einem standardisierten Format nach den DSFinV-K-Vorgaben „als selbstständiger Bestandteil der Einheitlichen Digitalen Schnittstelle" zur Verfügung zu stellenden Daten sind (vgl. DSFinV-K 2.4, Tz. 1.1.3, veröffentlicht vom Bundeszentralamt für Steuern).

38 Im Gegensatz zum Verordnungsgeber, der – unabhängig von seiner verfassungsrechtlichen Verpflichtung (vgl. dazu *Remmert*, in: Dürig/Herzog/Scholz, GG, Stand: 102. EL August 2023, Art. 80, Rn. 131) – eine Verordnungsbegründung vorgelegt hat, hat das BSI seine Motive für die einzelnen Regularien, insbesondere etwa eine Begründung der Erforderlichkeit der einzelnen Vorgaben, nicht offengelegt bzw. rechtfertigt.

39 § 5 S. 1 KassenSichV sieht nur ein „Benehmen" mit dem BMF vor.

40 Vgl. Wortprotokoll der 89. Sitzung des Finanzausschusses des Bundestages, S. 17 (Thomas Eigenthaler, Deutsche Steuer-Gewerkschaft e. V.): „Ich habe meine großen Probleme damit, dass wir solche Dinge aus den Händen der Finanzverwaltung geben. Mir ist nicht klar, wie die Richtlinien zur Zertifizierung aussehen werden. Auch das steht nicht im Gesetz. Wir hatten vorhin gehört, dass mit unbestimmten Rechtsbegriffen gearbeitet wird. Aber meine Damen und Herren, ist das besser, dass wir etwas noch weiter vom Gesetzgeber wegführen, indem wir zunächst Dinge im Gesetz nur andeuten und in eine steuerliche Rechtsverordnung geben? Dann geht es rüber in das BSI, dort gibt es auch ein Gesetz, dort gibt es Richtlinien – ich weiß nicht, ob wir da nicht viel mehr Bürokratie mit ungewissem Ausgang erzeugen."

41 Vgl. *Achilles*, DB 2019, 1920, 1921: „Bereits an dieser Stelle ist kritisch zu hinterfragen, ob die KassenSichV hinreichend detaillierte Regelungen enthält, die die Verordnungsermächtigung fordert. So enthält z. B. § 5 KassenSichV keinen Regelungsrahmen für technische Anforderungen an die TSE, sondern verweist auf noch zu erstellende Technische Richtlinien und Schutzprofile."

42 Insbesondere die TR-03153, die aber auch auf andere technische Richtlinien verweist.

43 BSI, Häufig gestellte Fragen und Antworten (FAQ), abrufbar unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Schutz-vor-Manipulation-an-digitalen-Grundaufzeichnungen/Fragen-und-Antworten/fragen-und-antworten_node.html (Abruf: 25.9.2024).

44 Vgl. § 9 Abs. 4 S. 1 Nr. 1 BSI-Gesetz.

45 „Common Criteria Protection Profile Security Module Application for Electronic Recordkeeping Systems (SMAERS)", BSI-CC-PP-0105-V2-2020, welches nach wie vor als Version 1.0 vorliegt.

46 Vgl. BT-Drs. 18/9535, 14 unten und 17 („technologieneutral").

47 Vgl. Schutzprofil zur SMAERS-Komponente, Kap. 1.2: „In case of the client-server architecture, where the TOE [d. h. die SMAERS-Komponente] can not directly rely on the CSP platform, a platform with secure storage must be used. The platform that executes the TOE has to provide mechanisms to preserve the integrity, confidentiality (when required), and to prevent rollback of stored sensitive objects, including the TOE software itself. […] In addition the TOE must rely on the platform in case of update code package verification."

48 Für Kassensysteme, obwohl diese nicht zertifiziert werden müssen, empfiehlt beispielsweise *Kowllik*, DB 2022, 2697, 2698, noch 2022 die Verlängerung der Frist für die Umstellung auf Nr. 7.2 AEAO zu § 146a bis zum 31.12.2024 hinsichtlich des Umgangs mit einem Ausfall oder einer Störung der TSE „im Hinblick auf die Praxiserfahrungen mit der Cloud-TSE", „damit die Kassenhersteller hierzu eine aktualisierte oder neue Software entwickeln oder betroffene Unternehmen auf neue Kassensysteme umstellen können".

49 Bußgeldverfahren auf dieser Basis hat es aber, soweit ersichtlich, bislang nicht gegeben.

Anforderungen der TSE-Hersteller an den im Schutzprofil angelegten, aber nicht ausdefinierten Umgebungsschutz festgelegt werden mussten, um eine Zertifizierung zu erhalten, war lange intransparent. Erst ab 2023 – dazu unten noch genauer – wurde dies schriftlich vom BSI definiert, obwohl gerade die Vorgaben zum Umgebungsschutz in die bestehende IT-Infrastruktur des Steuerpflichtigen eingreifen und in vielen Fällen erhebliche Neu- und Folgeinvestitionen in Hard- und Software notwendig machen. Auf die damit verbundenen Probleme ist im Rahmen der Würdigung noch zurückzukommen.

Unabhängig von den tatsächlich erlassenen Vorgaben des BSI ist aus formaler Sicht schon unklar, welche „Rechtsakte" das BSI auf Basis der Weiterdelegation genau erlassen durfte. Nach § 5 S. 1 KassenSichV sollen die technischen Vorgaben vom BSI „im Benehmen mit dem BMF" in Form von Technischen Richtlinien und Schutzprofilen festgelegt werden. FAQs auf der Website des BSI, die Zweifelsfragen adressieren, Testfälle und andere Arten von Dokumenten finden sich hingegen in der Aufzählung dieser technischen Vorgaben in § 5 KassenSichV nicht.[50]

Der Vollständigkeit halber sei hier noch erwähnt, dass der Anwendungserlass des BMF zu § 146a AO, soweit er sich auf die TSE und deren Komponenten bezieht, nur eine grobe Zusammenfassung der BSI-Vorgaben wiedergibt, also insoweit ebenfalls keine eigenständige Ausfüllung der oben genannten Gesetzesbegriffe enthält – was ohnehin für die Gerichte auch nicht bindend wäre.[51] Der zentrale Begriff des „elektronischen Aufzeichnungssystems" hingegen, den weder der Gesetzgeber noch der Verordnungsgeber definiert haben, wird nur im Anwendungserlass zu § 146 AO definiert,[52] also außerhalb der Gesetze im materiellen Sinn.[53] Hinzu treten – als weitere „Rechtsquelle" im Kontext von § 146a AO neben dem Anwendungserlass – die diesbezüglichen FAQ des BMF.[54]

III. Änderungen der BSI-Vorgaben 2023

Nach Wirksamwerden der gesetzlichen Regelungen 2020 entspann sich vielfältige Kommunikation zwischen BMF, BSI, (Unternehmens-) Verbänden und auch einzelnen Unternehmen (sowohl Steuerpflichtige als auch Systemanbieter) zu den Details der Regelungen. Entwürfe von Änderungen der AEAO[55] und BSI-Regularien kursierten in Fachkreisen und wurden umfangreich insbesondere von Verbänden – woran die *Verfasser* seinerzeit punktuell mitgewirkt haben – kommentiert und kritisiert, wenn auch in einem Verfahren, das kaum geordnet oder transparent genannt werden kann.[56] Dem Vernehmen nach ging die Kommunikationsbereitschaft der Behörden auf diese Kritik hin zurück. Die Unsicherheit über Zeitpunkt und Inhalt bevorstehender Änderungen der Rechtsquellen wuchsen und erschwerten Investitions- und Produktdesign-Entscheidungen. Allerdings sehen auch weder § 146a AO noch die KassenSichV die Anhörung von (beispielhaft) Herstellern und Verbänden vor.[57]

Mitte 2023 wurden die BSI-Regularien inhaltlich wesentlich geändert und erweitert. Die Änderungshistorie der TR-03153 spricht unter dem 30.5.2023 lapidar von einer „Überarbeitung". Die Änderungen sind – im Unterschied zu Gesetzes- oder Verordnungsänderungen – nicht als solche ersichtlich und können nur aufgrund eines umfangreichen Dokumentvergleichs aufgespürt werden. Ergänzend wurde ein neuer Anhang A vorgegeben, der erstmals im Detail die Anforderungen an die „Sicherheitszertifizierungen der TSE" vorgibt, darunter auch (im Rahmen der Zertifizierung) die Vorlage von „Schutzprofilen" einschließlich des Umgebungsschutzkonzepts. Ein neuer Anhang B stellt ein Leer- bzw. Vorratsdokument zu „Anforderungen an den ordnungsgemäßen Betrieb der TSE in bestimmten Nutzungsszenarien" dar, dessen Text lautet: „Aktuell werden in diesem Dokument keine zusätzlichen Anforderungen festgelegt". Der Sinn dieses Dokuments ist unklar.[58] Auch wenn das „Inkrafttreten" bzw. die Anwendbarkeit der überarbeiteten Fassung nicht ausdrücklich geregelt wurde, sind die Vorgaben der überarbeiteten TR-03153 nach § 5 Abs. 2 KassenSichV erst – insbesondere auf Zertifizierungsverfahren – seit Veröffentlichung im Bundessteuerblatt Teil 1[59] anwendbar. Eine rückwirkende Anwendung auf bereits erteilte Zertifizierungen (und deren einzelne Teile wie etwa ein Umgebungsschutzkonzept) ist weder vorgegeben noch wäre sie rechtlich rechtfertigbar.

Die in der TR-03153 vorgenommenen Änderungen sind durchaus gewichtig. Beispielhaft wurde die TR-03145-5 für sichere „Certification Authorities" neu geschaffen,[60] welche neuartige Anforderungen an die für TSEs zu betreibende PKI („public key infrastructure", in deren Rahmen der TSE-Hersteller den öffentlichen Schlüssel der TSE für die Prüfwertverifikation bereitstellt)[61] formuliert und welche in die TR-03153 ausdrücklich mit einbezogen wird.[62] Weiter wird die Fehlerbehandlung in das Kassensystem verlagert.[63] Die Einbindungsschnittstelle ist mit der bisherigen Definition inkompatibel,[64] was zu Funktionsverlust und der Notwendigkeit der Neuintegration in Kassensysteme führt. Aufrufe der Funktionen der Einbindungsschnittstelle müssen künftig sequenziell erfolgen, was zu Performance-Verlusten führt.[65] Die Liste ließe sich fortsetzen.

Zusätzlich „erließ" das BSI (erstmalig) eine Art Ergänzungsdokument zum bisherigen SMAERS-Schutzprofil, das konkrete Vorgaben zum Umgebungsschutz enthält.[66] Dieses „unterstützende Dokument" wurde bislang – im Gegensatz z. B. zur neuen Fassung der TR-03153 – nicht im Bundessteuerblatt Teil 1 veröffentlicht. Es ist deshalb – unge-

50 Natürlich wäre es für das BSI ein Leichtes, sämtliche anders titulierten Dokumente (einschließlich der FAQs) in „Technische Richtlinie" umzubenennen, um die formalen Anforderungen des § 5 S. 1 KassenSichV zu erfüllen. Gleichwohl geht das BSI selbstverständlich davon aus, dass auch die übrigen Vorgaben „bindend" sind.

51 Vgl. instruktiv auch zu den entsprechenden folgenden Ausführungen *Nonnenmacher/Peterich/Reifarth-Belli*, DStR 2024, 329.

52 Vgl. AEAO zu § 146, Abschnitt 2.1.4. Dies gilt auch für andere, in der KassenSichV nicht definierte Begriffe wie die „aufzeichnungspflichtigen Geschäftsvorfälle" oder die „anderen Vorgänge".

53 Zur fehlenden formalen und existenten faktischen Bindungswirkung weiterer Rechtsquellen s. noch unten.

54 BMF, Das Kassengesetz für mehr Steuergerechtigkeit: Belegausgabepflicht stärkt Transparenz und hilft gegen Steuerbetrug, abrufbar unter https://www.bundesfinanzministerium.de/Content/DE/FAQ/FAQ-steuergerechtigkeit-belegpflicht.html (Abruf: 25.9.2024).

55 Vgl. *Kowallik*, DB 2022, 2697, 2698.

56 Dementsprechend wurden auch keine Protokolle derartiger Besprechungen veröffentlicht und Ansprüche nach dem IFG wurden, soweit ersichtlich, in diesem Zusammenhang bislang nicht geltend gemacht.

57 § 47 GGO (auch in Verbindung mit § 62 Abs. 2 S. 1 GGO) findet auf Rechtsvorschriften „unterhalb" von Verordnungen keine Anwendung.

58 Das BSI hat im Rahmen seines Internetauftritts nichts unternommen, um der naheliegenden Unterstellung entgegenzutreten, dass hier ein „Container" geschaffen werden sollte, um unliebsame Lösungsansätze unter den schon „gehärteten" Vorgaben schnell durch Fortschreibung des Dokuments „verbieten" zu können.

59 BMF, 29.12.2023 – IV D 2-S 0316-a/19/10012 :005, BStBl. I 2024, 27.

60 Diese technische Richtlinie wurde bislang nicht nach § 5 S. 2 KassenSichV im Bundessteuerblatt veröffentlicht.

61 S. dazu auch noch unten.

62 Die TR-03153 (Version 1.1.1) enthält insgesamt 29 Verweise auf die TR-03145-5, insbesondere aber relevant Kap. 8.3.

63 Vgl. TR-03153 (Version 1.1.1), Kap. 9.4.

64 Vgl. TR-03153 (Version 1.1.1), Kap. 5, vs. TR-03153 (Version 1.0.1), Kap. 5.2.

65 Vgl. TR-03153 (Version 1.1.1), Kap. 5.1.2.

66 „Supporting Document for Common Criteria Protection Profile SMAERS", Version 1.0 vom 16.5.2023.

achtet anderer im Folgenden behandelter Aspekte – zweifelhaft, ob und welche Rechtswirkungen dieses Dokument derzeit entfaltet, auch wenn es die Zertifizierungspraxis des BSI entscheidend prägen wird.

Sowohl die Änderungen der TR-03153 als auch das „unterstützende Dokument" haben, wie noch zu zeigen sein wird, erhebliche Auswirkungen sowohl auf die TSE-Hersteller als auch auf die Anwender von TSE-Cloud-Lösungen mit lokaler SMAERS- und fernverbundener CSP-Komponente.

Man kann diese Überarbeitungen positiv dahingehend verstehen, dass das BSI bemüht ist, seine Vorgaben immer weiter zu präzisieren und transparent zu machen. Umgekehrt bildet sich hier aber ein „Pseudorecht" der Exekutive heraus, dessen Einhaltung immer höheren Aufwand erfordert und das – noch vor der verfassungsrechtlichen Dimension – an die verwaltungsrechtliche Thematik der „autonomen Rechtssetzung der Verwaltung" erinnert, der „nach wie vor nicht restlos geklärte rechtsdogmatisch schwierige und praktisch bedeutsame Fragen" nachgesagt werden.[67] Der Adressat steuerrechtlicher Normen ist solche Zustände gewohnt, denn bekanntermaßen herrscht im Steuerrecht durch Anwendungserlasse und Nichtanwendungserlasse der Finanzverwaltung ein „Wildwuchs" an Regelungsinstrumenten, die formal nur in eine Richtung – nämlich zulasten der Finanzverwaltung – rechtlich bindend sind, letztlich aber dennoch, selbst wenn sie (möglicherweise) vom Gesetzestext abweichen, von Steuerpflichtigen „aus Angst vor Scherereien" eingehalten werden.[68] In anderen Rechtsgebieten verhält es sich bisweilen ähnlich.[69] Auch die BSI-Vorgaben lassen sich materiell in diesem Sinne, d. h. insbesondere auch „von der Willensbildung des parlamentarischen Gesetzgebers weitgehend unbeeinflusst",[70] verstehen. Kein Hersteller einer TSE würde hier den rechtsstaatlichen Weg gehen,[71] d. h. eine Versagung einer Zertifizierung durch das BSI im Wege der verwaltungsgerichtlichen Verpflichtungsklage mit dem Argument fehlender formaler oder materieller Wirksamkeit von BSI-Zertifizierungsvorgaben angreifen, die absehbar folgenden drei Instanzenzüge durchleiden und nach Jahren des Rechtsstreits allein deshalb keine Zertifizierung mehr erhalten, weil sich die Rahmenbedingungen in der Zwischenzeit erheblich geändert haben. Ein solches Vorgehen ist – selbst unter Berücksichtigung möglicher Amtshaftungsansprüche[72] – wirtschaftlich sinnlos und entspräche nicht der von einem ordentlichen Geschäftsmann (§ 43 GmbHG) anzuwendenden Sorgfalt.

Wichtig ist daher im Rahmen des vorliegenden Beitrags zunächst, die mit derartigen Vorgaben einhergehenden praktischen Folgen für die Rechtsanwender transparent zu machen. Es handelt sich weder um Probleme des akademischen Elfenbeinturms noch um die Einführung lediglich eines neuen (Export-)Datenformats („Datensatzbeschreibungen") wie bei dem noch relativ jungen § 147b AO.[73] Durch volatile technische Vorgaben wird vielmehr erheblicher Investitionsbedarf (insbesondere in Form von Design- und Architekturänderungen), administrativer Aufwand und Zeitverzug bei Produktherstellern – und als Folge auch bei den Steuerpflichtigen – „mit einem Federstrich" ausgelöst. Eine gesetzgeberische inhaltliche Kontrolle, einschließlich einer Ermittlung bzw. Prognose der verbundenen (Implementierungs-)Kosten, findet nicht statt; die Vorgaben können willkürlich und ohne rechtsstaatliches Verfahren festgesetzt und erweitert bzw. geändert werden. Das ist Fluch und Segen zugleich: Positiv kann damit schnell auf technische Entwicklungen reagiert werden, negativ kann beständig „Flickschusterei" der technischen Vorgaben zulasten der Rechtsanwender betrieben werden. Ein „Verwerfen" der Regelungen im Rahmen gerichtlicher Verfahren ist zwar denkbar, findet aber in der Praxis aus den obengenannten Gründen nicht statt.

Anhand der Regelungen zum Umgebungsschutz, die hier wie gesagt einen Fokus bilden sollen und in den öffentlich zugänglichen Rechtsquellen vor 2023 nur sehr abstrakt formuliert worden waren, soll nachfolgend aufgezeigt werden, was die neuen Regelungen in der Praxis bewirken. Je höher die gestellten rechtlichen Anforderungen werden, desto mehr werden bestimmte TSE-Architekturen für Hersteller und/oder Steuerpflichtige in der Implementation bzw. in der Administration „unzumutbar", was bedeutet, dass auf andere TSE-Architekturen ausgewichen werden muss. Die vielzitierte Technologieoffenheit bestünde nur formal weiter, wenn die Anforderungen an einzelne Architekturen derart verschärft werden, dass ihr Einsatz nicht mehr wirtschaftlich sinnvoll ist.

IV. Neue Anforderungen beim Umgebungsschutz

Schon Anfang 2021 war in Fachkreisen ein internes Papier des BSI zu den Vorgaben für den Umgebungsschutz für die SMAERS-Komponente zirkuliert worden.[74] Das BSI erklärte seinerzeit daraufhin, der interne Entwurf habe keinen normativen Charakter. Schon dieser Entwurf zur „Operational Environment" wies darauf hin, dass die vom Steuerpflichtigen „gestellte" Ausführungsplattform (Hardware, Betriebssystem, andere Applikationen) für die SMAERS-Software-Komponente einer Cloud-TSE zwar nicht Teil der Zertifizierung selbst ist, dass aber die Verwendung einer Plattform ohne Einhaltung der diesbezüglichen Umgebungsschutzvorgaben einen Betrieb der SMAERS-Komponente in einem „nicht-zertifizierten Modus" bedeutet und damit die steuerrechtlichen Vorgaben nicht eingehalten werden.[75] Beispielhaft sollte schon nach diesem BSI-Entwurf der Einsatz einer hardwarebasierten Schutz-Technologie vorgegeben werden („secure hardware"), d. h. letztlich die Verwendung eines „Trusted Platform"-Moduls 2.0 (TPM 2.0), wie es von Microsoft auch für den Betrieb von Windows 11 – im Gegensatz zu den vorherigen Windows-Varianten – vorgegeben wird.[76] Viele aktiv genutzte PC-Systeme verfügen noch nicht über dieses Sicherheitsmodul, das im Wesentlichen einen Hardware-Anker darstellt, um bestimmte „physikalische Attacken" abzuwehren. Verkürzt gesagt kann damit „die Software wissen, auf welchem physischen System sie läuft", sodass z. B. eine Spiegelung des Systemabbilds auf eine andere Hardware (Cloning) bemerkt werden kann, und auch (Datenträger-)Verschlüsselungslogiken können

67 Vgl. *Schoch/Schneider*, Verwaltungsrecht, Stand: 4. EL November 2023, Einl., Rn. 31.
68 Vgl. bereits oben zu Anwendungserlassen sowie zum Nichtanwendungserlass aus jüngerer Zeit *Münch*, DStR 2023, 2321. Dasselbe gilt auch für Steuerrichtlinien auf Basis von Art. 108 Abs. 7 GG, vgl. *Kube*, in: BeckOK GG, 57. Ed., Stand: 15.1.2024, Art. 108, Rn. 8.
69 Vgl. etwa die verschiedenen „Merkblätter" der BaFin oder die Beschlüsse und Kurzpapiere der Datenschutzkonferenz (DSK).
70 So BVerwG, 17.6.2004 – 2 C 50/02, NVwZ 2005, 713, 714 zu den Beihilfevorschriften des Bundes.
71 Vgl. zu diesem Weg *Glade*, in: Kipker/Reusch/Ritter, Recht der Informationssicherheit, 2023, § 9 BSIG, Rn. 50. Die Details eines solchen Vorgehens liegen mangels Rechtsprechung im Dunkeln.
72 Vgl. dazu allgemein *Ehlers/Stadermann*, in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, Stand: 60. EL Oktober 2023, Teil 18.3, Rn. 51 ff.
73 Hier können sich im Rahmen der geplanten „Buchführungsdatenschnittstellenverordnung" allerdings ähnliche Probleme wie beim § 146a AO stellen.
74 „SMAERSOperationalEnvironment_V2" (undatiert, Dateierstellungsdatum 6.11.2020).
75 „The platform is not part of the certification itself, however, if SMAERS is operated on a platform that does not fulfill those requirements, it is operated in a non-certified mode, and thus, is not certified as required by the fiscal law".
76 Vgl. *Windeck*, heise online, 18.7.2021, abrufbar unter https://www.heise.de/ratgeber/Trusted-Platform-Module-2-0-in-Windows-11-6135986.html (Abruf: 25.9.2024).

auf diesen „unmanipulierbaren" Hardware-Anker zurückgreifen. Diese (Sicherheits-)Vorgabe führt dazu, dass eine große Anzahl von bestehenden Computer-Systemen nach dem Auslaufen des Supports für Windows 10 nicht mehr in der Lage sein wird, die dann aktuell gepflegte Windows-Version 11 auszuführen.[77] Millionen installierter PCs werden damit zu Elektroschrott deklariert und müssen – trotz grundsätzlich ausreichender Rechenleistung – vorzeitig ersetzt werden.

Anfang 2021 verwendeten große Filialisten mangels Bedarf und aus Kostengründen bei keiner Kasse und keinem Filial-Back-Office-Server ein TPM-2.0-Modul, und die Hersteller von Cloud-TSEs gingen zunächst davon aus, dass aufgrund der zulässigen Cloud-TSE-Technologie Eingriffe in die bestehende Hardware der Steuerpflichtigen (durch entsprechende Design-Vorgaben) gerade verhindert werden sollten. Schließlich ging es nicht nur um austauschbare Windows- und Linux-Systeme auf Standard-PC-Hardware-Basis, sondern auch um Stand-alone-Kassensysteme mit proprietärem Betriebssystem, die sich systembedingt nicht (nachträglich) mit einem entsprechenden Hardware-Anker ausstatten lassen. Das BSI empfahl den Herstellern von Cloud-TSE-Systemen im genannten Entwurfspapier daher, dem Steuerpflichtigen die lokale (Hardware-)Ausführungsplattform für die SMAERS-Komponente mitzuliefern, um diese selbst entsprechend validieren und konfigurieren zu können.[78] In der Folge enthielten die Umgebungsschutzvorgaben von Cloud-TSE-Herstellern die Forderung nach einem TPM-2.0-Modul in der Ausführungsplattform beim Steuerpflichtigen, da das BSI den Herstellern ansonsten keine Zertifizierung erteilt hätte. Die Herstellervorgabe als solche wurde also faktisch „erzwungen", auch wenn dies dann notwendigerweise zu einer Risikoabwägung bei den Steuerpflichtigen führen musste, wie mit dieser Vorgabe umzugehen war.

Die meisten Aspekte des ursprünglichen Papiers zur Umgebungsschutz, darunter auch die grundsätzliche Forderung nach dem skizzierten Hardware-Sicherheitsanker, hat das BSI trotz der damaligen „Rückzugsbewegungen" weiterverfolgt und seit August 2022 in verschiedenen Entwurfsstadien im oben genannten, im Juni 2023[79] finalisierten „unterstützenden Dokument" ausformuliert. Dieses Dokument legt zusätzliche Anforderungen sowohl an die CSP- als auch an die SMAERS-Komponente nieder. Neben Gesetz, Verordnung, technische Richtlinie bzw. Schutzprofil tritt damit noch eine vierte, weder in §§ 146a Abs. 3, 5 S. 1 KassenSichV noch in § 9 BSI-Gesetz genannte Ebene: Ein „unterstützendes Dokument", welches nach seiner eigenen Definition „guidelines" (also keine „Kriterien"?) enthält, wie eine SMAERS-Komponente im Rahmen der Zertifizierung zu evaluieren ist. Mit anderen Worten: Ohne Veränderung des Rahmendokuments „SMAERS-Schutzprofil" wurde auf nachgelagerter Regelungsebene der Umgebungsschutz kodifiziert, anhand dessen letztlich Hersteller und Rechtsanwender entscheiden müssen, ob ein bestimmtes TSE-Produkt bzw. eine bestimmte TSE-Architektur überhaupt noch wirtschaftlich sinnvoll betreibbar ist. Auch im „unterstützenden Dokument" wird – wie zuvor im internen Entwurf (s. o.) – darauf hingewiesen, dass der Bereich der zertifizierten TSE verlassen und mithin die steuerlichen Vorgaben nicht eingehalten werden, wenn die Umgebungsschutzvorgaben des „unterstützenden Dokuments" nicht eingehalten werden.[80] Nach den neuen BSI-Vorgaben muss der Integrator – also meist der TSE-Hersteller oder dessen Beauftragter, der zugleich als einziger Administrator der SMAERS-Ausführungsplattform fungieren soll – die Erfüllung der Umgebungsschutzvorgaben durch den Steuerpflichtigen bestätigen.[81] Durch die Auslagerung in ein Dokument „unterhalb" des Schutzprofils war formal nicht einmal mehr ein „Benehmen mit dem BMF" nach § 5 S. 1 KassenSichV notwendig.[82]

Konzeptuell werden in diesem Dokument „Evaluationsaktivitäten" im Rahmen der Zertifizierung, basierend auf bestimmten Risikoszenarien (Angriffsvektoren), vorgegeben. Als Standard-Angriffsszenario auf die TSE definiert das BSI den „uneingeschränkten physikalischen Zugriff des Angreifers auf die SMAERS-Komponente und dessen Ausführungsplattform".[83] In diesem Zusammenhang wird insbesondere auch der Steuerpflichtige selbst als potenzieller Angreifer gesehen, sodass hinsichtlich des sicheren Betriebes der SMAERS-Komponente nicht auf diesen vertraut werden kann. Schon das SMAERS-Schutzprofil von 2020 enthielt diese Überlegung,[84] leitete daraus aber noch keine konkreten Hardware-Anforderungen ab. Das Angriffsszenario selbst ist zwar inhaltlich insoweit plausibel, als auch schon bisher Kassendatenmanipulationen kaum von außenstehenden Dritten (Hackerangriff etc.) verübt wurden, sondern vom Steuerpflichtigen bzw. dessen Mitarbeitern selbst, um (Umsatz-)Steuerverkürzung zu betreiben. Gleichwohl ist dieses Angriffsszenario zumindest bei Großunternehmen, die über entsprechend dimensionierte „systems and controls" im Rahmen eines ausgefeilten Tax Compliance Management Systems verfügen, nicht plausibel mit der Folge, dass der gewählte „one size fits all"-Ansatz legitime Interessen übergeht und im Widerspruch zur Rechtmäßigkeitsvermutung der Aufzeichnungen[85] steht; hierauf wird noch zurückzukommen sein. Unabhängig davon wird hier aber schon deutlich, dass dieselbe Grundannahme auch für das Kassensystem selbst gelten müsste, mit bzw. in dem noch weit relevantere Manipulationen betrieben werden können.[86] Eigentlich müsste also auch das Kassensystem selbst dem Zugriff des Steuerpflichtigen entzogen werden, was den gesamten Schutzgedanken *ad absurdum* führt. Auch auf diese Ungleichbehandlung wird noch zurückzukommen sein.

Während das BSI nun ausdrücklich im Grundsatz vorgibt, dass für Windows- (und auch Linux-)Umgebungen die zugrundeliegende Hardware – unabhängig von der verwendeten Windows-Version – über ein TPM-2.0-Modul als „Anker" verfügen muss, lässt es gleich-

77 Vgl. golem.de, Windows 11 startet bald nicht mehr auf alten CPUs, abrufbar unter https://www.golem.de/news/betriebssystem-windows-11-startet-bald-nicht-mehr-auf-alten-cpus-2402-182168.html (Abruf: 25.9.2024).

78 „It is therefore RECOMMENDED that the manufacturer delivers SMAERS together with a suitable platform. In this case, the validation of the platform and its configuration is already performed within the evaluation".

79 Das Dokument selbst weist ein Veröffentlichungsdatum vom 16.5.2023 aus, während es tatsächlich erst im Juni 2023 auf der Website des BSI veröffentlicht wurde.

80 Vgl. „Unterstützendes Dokument" zum SMAERS-Schutzprofil, Kap. 1: „A TOE [d. h. SMAERS-Komponente] that is not operated adhering to these requirements is not operated as certified, and in such a case, the taxpayer is not meeting the legal requirements. Therefore, the manufacturer must provide additional documentation […] that describes how the TOE must be operated in order to meet all requirements. Adherence to this documentation is mandatory for all parties concerned".

81 Vgl. „Unterstützendes Dokument" zum SMAERS-Schutzprofil, Kap. 1: „The integrator must confirm in writing that he obliged to all these configuration documents and must provide this document to the taxpayer." Nach Kap. 3.2 ist der „Integrator" derjenige, der die SMAERS-Komponente (vor Ort) integriert, personalisiert und initialisiert. Das kann entweder der TSE-Hersteller sein oder ein vertrauenswürdiger, vom Hersteller eingesetzter Dienstleister.

82 Ob dieses (dennoch) stattgefunden hat, ist nicht öffentlich dokumentiert, letztlich aber auch irrelevant.

83 Vgl. Schutzprofil zur SMEARS-Komponente, Kap. 2.3: „it has to be assumed that the attacker has unrestricted physical access to the TOE or its platform".

84 Vgl. Schutzprofil zur SMAERS-Komponente, Kap. 3.2: „The taxpayer is however also considered as potential attacker, who may use a manipulated CTSS [d. h. TSE] or manipulates logs after they were produced by the CTSS."

85 § 158 Abs. 1 AO.

86 Vgl. etwa den Fall „Löschung von Daten in Cloudsystemen" bei *Teutemacher*, AO-StB 2020, 123, 124, wenn Umsätze innerhalb eines Cloud-Kassensystems gelöscht werden, bevor sie in die Cloud übertragen werden.

wohl eine Ausnahme zu. Das genannte Angriffsszenario auf die TSE, so das BSI, sei irrelevant, wenn ein physikalischer und logischer Zugang zur SMAERS-Ausführungsplattform plausibel verneint werden kann.[87] Das BSI stellt im Anschluss selbst allerdings fest, dass diesen Vorgaben nur dann Genüge getan werden kann, wenn die SMAERS-Komponente und ihre gesamte Laufzeitumgebung von einer vertrauenswürdigen dritten Partei, die unabhängig vom Steuerpflichtigen ist, in einer auditierten Umgebung mit implementierter sicherer Kundentrennung betrieben wird.[88] Wollte ein Steuerpflichtiger, der Ladenfilialen mit Kassensystemen betreibt, die SMAERS-Komponente als lokalen Teil einer Cloud-TSE vor Ort betreiben,[89] müsste er also in jeder Filiale einen verschlossenen Raum mit Zutrittsberechtigung nur für konzernfremde Dritte einrichten, in dem sich ein PC mit der SMAERS-Komponente befindet, und auch sämtliche „logischen" (Fern- und Administrations-)Zugriffsmöglichkeiten des eigenen Personals unterbinden. Praktikabel ist diese letztlich „zur Wahl gestellte" Alternative nicht.

Weiter fordert das BSI in diesem Zusammenhang unter anderem – auch bei Einsatz eines TPM-2.0-Moduls –, dass auf dem zugrundeliegenden System ausschließlich die SMAERS-Komponente, Applikationskomponenten des elektronischen Aufzeichnungssystems (Kassensoftware) und ansonsten nur eine notwendige Minimal-Applikationskonfiguration betrieben wird, weiter dass der lokale Standard-Administrator-Account deaktiviert werden muss und schließlich dass die Ausführung administrativer Funktionen dem „SMAERS-Plattform-Operator" (d. h. in der Regel dem TSE-Hersteller bzw. dessen Beauftragtem) vorbehalten bleiben muss. Jegliche Services von Dritten auf dem System müssen daraufhin geprüft werden, warum ihre „Anwesenheit" auf dem System notwendig ist.

Im Ergebnis führen die neuen Vorgaben dazu, dass der Betrieb einer lokalen SMAERS-Komponente mit fernverbundener CSP-Komponente für die Steuerpflichtigen in den weitaus überwiegenden Fällen aufgrund der notwendigen Investitionen und des Verlusts der administrativen Kontrolle über „eigene" Systeme letztlich nicht mehr in Frage kommt. Damit droht eine ganze Produktgruppe bzw. Architektur wegzufallen; die Investitionen der TSE-Hersteller in Cloud-TSEs mit lokaler SMAERS-Komponente werden weitgehend wertlos. Ob – und wenn ja, warum – es das Ziel des BSI war, durch die neuen Anforderungen mittelbar diese Architektur vom Markt zu nehmen, ist unklar.

V. Neue Anforderungen an die PKI

Das vom BSI definierte, in § 146a AO selbst nicht wiedergegebene und auch aus dem in § 2 S. 2 Nr. 7 KassenSichV verwendeten Wort „Prüfwert" nicht zwangsläufig herleitbare[90] Grundkonzept der TSE besteht darin, dass Daten über relevante (Kassen-)Vorgänge, welche das Kassensystem generiert, mithilfe einer sicheren Zeitquelle zeitgestempelt und über einen Transaktionszähler verkettet elektronisch signiert werden. Damit werden sie gegen spätere Veränderungen der einzelnen Datensätze, insbesondere auch gegen eine Veränderung der Vorgangszeit, und gegen Veränderungen in der Reihenfolge der Datensatz-Kette gesichert. Im Falle von Manipulationen ist zwar regelmäßig nicht der unmanipulierte Zustand rekonstruierbar, aber die Manipulation als solche kann (aufgrund einer nicht positiv nachprüfbaren Signatur) identifiziert werden. Die Signatur als Kernstück der Absicherung beruht, wie üblich, auf asymmetrischer Kryptographie mit einem privaten und einem öffentlichen Schlüssel.[91] Während der private Schlüssel sicher (d. h. unauslesbar) in der CSP-Komponente der TSE selbst enthalten ist, muss der öffentliche Schlüssel für die Nachprüfung, dass tatsächlich der private Schlüssel verwendet wurde, zugänglich und der individuellen TSE zuordenbar sein. Die Erstellung und Verwaltung der Schlüssel konnte schon nach der vormaligen TR-03153 der TSE-Hersteller übernehmen: „Betreibt ein Hersteller einer Technischen Sicherheitseinrichtung eine Public Key Infrastruktur (PKI) zur Sicherstellung der Authentizität der Prüfwerte, so ist der sichere Betrieb der PKI Bestandteil der CC-Zertifizierung des Sicherheitsmoduls."[92] Genauere Vorgaben für die „Sicherstellung der Authentizität der Prüfwerte" wurden seinerzeit nicht schriftlich niedergelegt. Damit war, vergleichbar der oben dargestellten „historischen" Situation beim Umgebungsschutz, unklar, welchen Anforderungen ein PKI-Konzept eines TSE-Herstellers genügen musste. Auch hier musste „iterativ" in Kommunikation mit dem BSI ein zertifizierungsfähiges Konzept erarbeitet werden, ohne dass die Anforderungen im Detail offengelegt, geschweige denn in technischen Richtlinien niedergelegt waren.

Derartige PKIs unter Einsatz von Vertrauensdiensten wurden erstmals 1997 in Deutschland im Wege des Signaturgesetzes gesetzlich geregelt und seit 2016/2017 durch die eIDAS-VO der EU sowie das begleitende Vertrauensdienstegesetz (VDG) abgelöst.[93] Parallel hatte das BSI bereits vor 2017 „generelle Anforderungen an Trust Center, die eine Certification Authority mit Sicherheitslevel ‚hoch' betreiben" in Gestalt der TR-03145(-1) entwickelt, die selbst keinen Bezug auf die genannten gesetzlichen Rahmenbedingungen für elektronische Signaturen nimmt[94] und auf die in der ursprünglichen TR-03153 nur für die Zertifizierung externer (PKI-)Anbieter, deren Zertifikate für die Verifikation von Prüfwerten verwendet werden, verwiesen wurde.[95] Zwischenzeitlich wurden 2023 in der TR-03145-5[96] spezielle, konkretere und nochmals inhaltlich stark verschärfte Anforderungen für TSE-Hersteller niedergelegt, da das BSI hier – wie beim Umgebungsschutz – von „Hochrisiko"-Anforderungen ausgeht. Die hier behandelte TR-03153 für die SMAERS-Komponente nimmt in ihrer Fassung 2023 an verschiedenen Stellen Bezug auf die TR-03145-5, die eine TSE-spezifische Erweiterung der bisherigen TR-03145-1 darstellt. Sowohl die Vorgaben der TR-03145-1 als auch der neuen TR-03145-5 gehen über die gesetzlichen Vorgaben im Bereich der sicheren elektronischen Identifizierung bzw. Vertrauensdiensten weit hinaus. Das BSI hat hier, da es diese gesetzlichen Grundlagen nicht in seinem Sinne

87 Vgl. „Supporting Document", Ziff. 8: „determine if access to the SMAERS platform is not possible for an attacker, both logically and physically".
88 Vgl. „Supporting Document", Ziff. 8: „For this, SMAERS and its platform must be hosted by a trusted third party that is independent from the taxpayer in an audited environment implementing secure client separation".
89 S. zur Trennbarkeit von SMAERS- und CSP-Komponente noch unten.
90 Vgl. Begründung der KassenSichV in BR-Drs. 487/17, 10: „Der Prüfwert in § 2 Satz 2 Nummer 7 des KassenSichV dient der Sicherung der Integrität einer jeden Aufzeichnung. Die Funktion des Prüfwerts kann etwa (sic!) durch Signaturverfahren sichergestellt werden. Der Stand der Technik zur Eignung von Mechanismen zur Erstellung eines Prüfwerts ist gemäß § 5 den Technischen Richtlinien des BSI zu entnehmen".
91 Vgl. nur Wikipedia, Asymmetrisches Kryptosystem, abrufbar unter https://de.wikipedia.org/wiki/Asymmetrisches_Kryptosystem (Abruf: 25.9.2024).
92 Vgl. TR-03153 (Version 1.0.1), Kap. 7.4.
93 In diesem gesetzlichen Rahmen ist die Bundesnetzagentur Aufsichtsbehörde für elektronische Signaturen und Zeitstempel und das BSI für Webseiten-Zertifikate zuständig, vgl. § 2 VDG.
94 Allerdings erklärt das BSI in einem entsprechenden „Mapping"-Dokument hinsichtlich der technischen Voraussetzungen schon 2016, dass die Erfüllung der (damaligen) TR-03145 auch die (abstrakteren) Vorgaben der eIDAS-VO bedeutet.
95 Vgl. TR-03153 (Version 1.0.1), Kap. 7.4: „Externe Anbieter von Zertifikaten, welche zur Verifikation von Prüfwerten verwendet werden, MÜSSEN über ein Zertifikat nach [BSI TR-03145] verfügen."
96 Vgl. auch den Hinweis in BMF, 29.6.2023 – IV D 2 – S 0316-a/19/10012 :005, BStBl. I 2023, 1075, nach § 5 S. 2 KassenSichV.

modifizieren kann, insbesondere mit der TR-03145-5 eine „TSE-PKI-Parallelwelt" geschaffen.

Die „Nachschärfungen" in diesem Bereich haben zwar – wie beim Umgebungsschutz – den Vorteil größerer Klarheit und dürften damit zu weniger „Schleifen" im Rahmen der Zertifizierung führen, doch im Gegenzug wurden die Anforderungen inhaltlich strikter und führen damit zu erheblichem (Entwicklungs-) Aufwand aufseiten der TSE-Hersteller. Ein Beispiel hierfür ist die Sperrung von Zertifikaten in einem spezifischen, die entsprechenden (aber bislang nicht anwendbaren) Regelungen der TR-03145(-1) überschreibenden[97] Verfahren, gleich, ob deren private Schlüssel sich in einer Hardware- oder einer Cloud-TSE (bzw. deren CSP-Komponente) befinden.[98] Letztlich stellt eine Sperrung, deren Möglichkeit auch bislang schon ohne Grundlage in der TR-03153[99] vom BSI gefordert wurde, zunächst nur den Eintrag des Zertifikats in eine (insbesondere für die Finanzverwaltung zugängliche) Sperrliste dar, sodass das Zertifikat und damit auch die mit der zugehörigen TSE signierten Datensätze nicht mehr als vertrauenswürdig gelten.[100] Die TSE selbst wird dadurch nicht technisch unbrauchbar, kann aber nicht mehr für ihren fiskalischen Zweck eingesetzt werden. Nach den neuen Vorgaben der TR-03153 muss allerdings der zugeordnete private Schlüssel in der TSE, sofern technisch möglich, gelöscht und die TSE deaktiviert werden.[101] Wann genau eine Sperrung vorgenommen werden darf, insbesondere bei Vorliegen von Verdachtsmomenten (Stichwort Beweislast), ist angesichts der schlagwortartigen Fallgruppen in der Datensatzbeschreibung der TR-03145-5 (wie Kompromittierung, Diebstahl etc.) unklar.[102] Die (bislang in abgespeckter Form durch TSE-Hersteller genutzten) Standardprodukte der nach wie vor sehr wenigen PKI-Anbieter in Deutschland, die auf Basis der Anforderungen der eIDAS-VO der EU entwickelt und betrieben werden, müssen erheblich erweitert bzw. modifiziert werden, um diese neuen Anforderungen an TSE-Hersteller und deren PKI abzubilden. So muss beispielsweise, damit eine Sperrung nicht missbräuchlich geschehen kann, zumindest für Hardware-TSEs eine PIN zur Verfügung gestellt werden, um bei einer Sperranfrage die Identität des „Antragstellers" absichern zu können. Da die Sperrung in der nur für den TSE-Hersteller und die Finanzverwaltung zugänglichen Zertifikatsdatenbank letztlich nicht mehr aufgehoben werden kann, wird eine (Hardware-)TSE im Falle einer Sperrung des zugehörigen Zertifikats endgültig wertlos, und zwar unabhängig davon, ob die Sperrung in der TSE selbst durch Deaktivierung „nachvollzogen" wird. Wird die PIN missbräuchlich eingesetzt, würde der gutgläubige TSE-Eigentümer ggf. erst Jahre nach der Sperrung, insbesondere nämlich im Rahmen einer Kassen-Nachschau, von der Sperrung erfahren. Die Umsetzung dieser neuen Vorgaben erfordert neben der Implementierung BSI-spezifischer Sperrberechtigter und Sperrgründe auch den Betrieb einer öffentlich zugänglichen Sperrliste mit 99,99 % Verfügbarkeit (was technisch in der Regel nur durch den Einsatz eines sog. Hyperscalers und unter Inkaufnahme von Datenschutzrisiken[103] möglich ist) sowie bei Hardware-TSEs eine Personalisierung auf den Steuerpflichtigen, Änderungen der Logistik, einen PIN-Brief und eine neuartige TSE-Initialisierung.[104]

Diese Erweiterungen der PKI-Vorgaben spezifisch für TSE-Hersteller gehen, was das Beispiel der Zertifikatssperrung und die Zertifikatsdatenbank anbelangt, noch über die entsprechenden gesetzlichen Grundlagen in Art. 24 Abs. 3, 28 Abs. 4 eIDAS-VO, § 14 VDG weit hinaus, wobei selbst deren Anwendbarkeit bislang nie vorgesehen war. Im Ergebnis sind hohe Investitionen von PKI-Anbietern für die Entwicklung einer „TSE-Sonderlösung" erforderlich, die mittelbar wirtschaftlich von den beauftragenden TSE-Herstellern zu tragen sind und von diesen an die Steuerpflichtigen – gleich, welche TSE-Architektur von diesen genutzt wird – weitergegeben werden müssen.

VI. Ermächtigungsgrundlage für die BSI-Vorgaben

Im Bereich des Umgebungsschutzes kann man, wie oben schon erwähnt, die Existenz des „unterstützenden Dokuments" des BSI positiv formulieren: Der bisherige, nie offengelegte und diffuse „interne" Zertifizierungsmaßstab des BSI im Bereich des Umgebungsschutzes, d. h. der Vorgaben, die TSE-Herstellern ihren Kunden – den Steuerpflichtigen – für die von diesen eingesetzten Ausführungsplattformen verbindlich an die Hand geben mussten, ist nun erstmals „offiziell" verschriftlicht worden. Damit kann dieser Maßstab einer formalen und inhaltlichen Prüfung unterzogen werden. Auf den (formalen) Umstand, dass das „unterstützende Dokument" bislang nicht im Bundessteuerblatt veröffentlicht wurde und daher dessen formale Bindungswirkung im Sinne von § 5 KassenSichV fraglich ist, wurde bereits hingewiesen.

Wichtiger ist aber, dass aus § 146a AO selbst keine formale (Ermächtigungs-)Grundlage für einen Umgebungsschutz als solchen, geschweige denn konkrete Vorgaben für dessen Ausgestaltung abgeleitet werden können. Derartige Versuche[105] scheitern, da die „Generalklausel" des § 146a Abs. 1 S. 1 AO aufgrund ihrer abstrakten Anforderungen nicht dahingehend ausgelegt werden kann, dass die Vorschrift nur ganz konkrete technische Umsetzungsmöglichkeiten zulasse. § 146a Abs. 3 AO wiederum sieht keine Verordnungsermächtigung für den Umgebungsschutz vor, d. h. für den Erlass von Vorgaben an den Steuerpflichtigen im Hinblick auf bereits bestehende IT-Systeme, auf denen Teilfunktionen einer (Software-)TSE ablaufen sollen. Sowohl § 146a Abs. 3 AO als auch § 5 KassenSichV nennen als Delegationsumfang lediglich die Anforderungen an das Sicherheitsmodul (§ 146a Abs. 3 S. 1 Nr. 2 a) AO), an das Speichermedium (§ 146a Abs. 3 S. 1 Nr. 2 b) AO) und an die einheitliche digitale Schnittstelle (§ 146a Abs. 3 S. 1 Nr. 2 c) AO), jeweils als Bestandteile der TSE als solcher (§ 146a Abs. 1 S. 3 AO).[106] Soweit die TSE als Softwarelösung abgebildet wird,[107] ist das „Sicherheitsmodul" der TSE die entsprechende Software-Komponente (Applikati-

97 Vgl. TR-03145-1, Kap. 5.7.
98 Vgl. TR-03145-5, Kap. 4.3.
99 Vgl. TR-03153 (Version 1.0.1), Kap. 7.4.
100 Vgl. TR-03145-1, Kap. 5.7: „revocation of certificates: revoked certificates are not trustable any more".
101 Vgl. TR-03153 (Version 1.1.1), Kap. 3.9.4.1.
102 Vgl. TR-03145-5, Anlage B, zu den möglichen Werten der Felder „RevokingPartys" und „RevocationReason", sowie TR-03153 (Version 1.1.1), Kap. 8.3.2.1.2: „Eine Sperrung eines Zertifikates DARF dabei nur aus Gründen erfolgen, die die Sicherheit der PKI beeinflussen wie zum Beispiel der Kompromittierung eines privaten Schlüssels."
103 Bei den zur Identifizierung einer TSE in der Sperr-Datenbank notwendigen IDs handelt es sich zumindest bei Einzelunternehmen um personenbezogene Daten.
104 Vgl. im Einzelnen TR-03145-5, Kap. 4.3.
105 Vgl. etwa *Bron/Schroeder*, BB 2022, 279.
106 § 146a Abs. 3 S. 1 Nr. 2 g) AO in Verbindung mit § 11 KassenSichV nennt daneben auch die Anforderungen an die Zertifizierung der TSE als Gegenstand der Delegation, insoweit hier aber ohne inhaltliche Relevanz, soweit man nicht unter „Anforderungen an die Zertifizierung" die inhaltlichen Zertifizierungskriterien verstehen möchte, die dann nicht vom BSI festgelegt werden dürften, da insoweit keine Weiterdelegation vorgesehen wurde.
107 Der Gesetzesbegriff der Sicherheits-„Einrichtung" und des Sicherheits-„Moduls" gibt letztlich nichts dazu her, ob eine TSE in Hardware- oder Software-Form erstellt werden kann oder als (Cloud-)Dienstleistung bezogen wird oder eine Mischform zur Anwendung kommt.

on), nicht aber die zugrunde liegende Hard- und Software (Ausführungsplattform). Im Ergebnis beschränkt sich die gesetzliche (Ermächtigungs-)Grundlage auf die TSE selbst, sodass auf dieser Basis schon rein formal keine (untergesetzlichen) Anforderungen an die Beschaffenheit „angrenzender" Systeme bzw. Systemteile bestimmt werden dürfen.

Auch im Hinblick auf die PKI-Vorgaben gilt, dass der TSE-Hersteller selbst und dessen Organisation als Zertifizierungsstelle weder Teil des Sicherheitsmoduls, auf das sich die gesetzliche Ermächtigung in § 146a Abs. 3 S. 1 Nr. 2 a) AO bezieht, sind, noch Teil der „Protokollierung von digitalen Grundaufzeichnungen" im Sinne von § 146a Abs. 3 S. 1 Nr. 2 e) AO. Im Gegenteil: Im Gesetzestext findet sich kein Hinweis darauf, dass überhaupt elektronische Signaturen zu verwenden sind[108] bzw. der Hersteller einer TSE als Zertifizierungsstelle bzw. PKI-Anbieter – geschweige denn im Sinne der eIDAS-VO oder anderweitig – fungieren soll. Damit ist auch die Vorgabe bestimmter PKI-Strukturen, die bei den TSE-Herstellern aufzubauen und vorzuhalten sind, begrifflich nicht von der gesetzlichen (Ermächtigungs-)Grundlage gedeckt.

Dr. Axel-Michael Wagner, RA, ist Partner der Kanzlei Peters, Schönberger & Partner in München. Er berät Mandanten in den Bereichen Compliance, M&A-Transaktionen, Due Diligence-Prüfungen und Vertragsrecht. Seine Expertise erstreckt sich zudem auf das IT-Recht, den Datenschutz sowie die zivilprozessuale Prozessführung.

Stefan Groß, StB, CISA, ist Partner der Kanzlei Peters, Schönberger & Partner in München. Er berät vornehmlich an der Schnittstelle Steuerrecht und IT sowie rund um das Thema Tax Technologie und KI im Steuerbereich. Er ist Vorstand beim Institut für Digitalisierung im Steuerrecht (IDSt), Mitglied im Fachausschuss IT (FAIT) des IDW, Chefredakteur der REthinking: Tax sowie Initiator von TAXPUNK.de und den Tax Pioneers.

108 Der Begriff „Protokollierung" in § 146a Abs. 3 S. 1 Nr. 2 e) AO impliziert gerade keine elektronische Signatur und die dort genannte „Sicherstellung der Integrität und Authentizität sowie der Vollständigkeit der elektronischen Aufzeichnung" kann nicht nur durch eine elektronische Signatur, sondern durch entsprechende Verfahren erreicht werden. Die Forderungen nach Integrität, Authentizität und Vollständigkeit erheben beispielsweise auch die GoBD der Finanzverwaltung, ohne elektronische Signaturen zu fordern.

BFH: Abhilfebescheid während des Revisionsverfahrens

BFH, Beschluss vom 10.7.2024 – III R 18/24
ECLI:DE:BFH:2024:B.100724.IIIR18.24.0
Volltext der Entscheidung: **BB-ONLINE BBL2024-1942-5**
unter www.betriebs-berater.de

AMTLICHE LEITSÄTZE

1. NV: Setzt die Familienkasse während des Revisionsverfahrens Kindergeld in dem beantragten Umfang fest und hält der Kläger seinen Sachantrag aufrecht, wird die Revision wegen Wegfalls des Rechtsschutzbedürfnisses unzulässig.

2. NV: Ein Rechtsschutzbedürfnis folgt nicht aus dem Hinweis der Familienkasse, dass Erstattungsansprüche von Sozialbehörden einer Auszahlung des Kindergelds an den Kindergeldberechtigten entgegenstehen könnten.

AO § 218 Abs. 2; EStG § 62, § 74 Abs. 2; FGO § 90, § 96 Abs. 1 S. 2, § 126, § 138; SGB 10 § 102, § 104, § 107 Abs. 1

SACHVERHALT

Ursprünglich war in der Sache streitig, ob die Klägerin und Revisionsklägerin (Klägerin) einen Kindergeldanspruch gemäß §§ 62 ff. des Einkommensteuergesetzes (EStG) für ihren Sohn S hat. Der von der Klägerin im Revisionsverfahren gestellte Antrag betraf die Monate Juli 2010 bis einschließlich Juli 2014, von denen nach einer Verfahrenstrennung hier nur die Monate Mai 2012 bis einschließlich August 2012 streitgegenständlich sind.

Die Familienkasse X lehnte die Bewilligung von Kindergeld mit Bescheid vom 27.06.2012 ab. Einspruch (Einspruchsentscheidung vom 06.08.2012) und Klage waren erfolglos. Das Urteil ist in Entscheidungen der Finanzgerichte 2014, 1124 veröffentlicht.

Gegen das Urteil legte die Klägerin mit Schreiben vom 13.08.2013 Beschwerde wegen Nichtzulassung der Revision (§ 116 Abs. 1 der Finanzgerichtsordnung – FGO –) ein. Mit Beschluss des Bundesfinanzhofs (BFH) vom 05.02.2014 – XI B 84/13 wurde die Revision zugelassen. Das Verfahren wurde hierauf als Revisionsverfahren fortgesetzt (§ 116 Abs. 7 Satz 1 FGO), ruhte jedoch im Hinblick auf die beim Bundesverfassungsgericht (BVerfG) anhängigen Verfahren 2 BvL 9-14/14. Es ist während der Verfahrensruhe auf den III. Senat übergegangen (Geschäftsverteilungsplan 2023 des BFH, A., Ergänzende Regelungen, IV. Nr. 1 i.V.m. A., III. Senat, Nr. 2 Buchst. d) und wurde von diesem wieder aufgenommen, nachdem das BVerfG mit Beschlüssen vom 28.06.2022 – 2 BvL 9-10/14 und 13-14/14 (BVerfGE 162, 277, BGBl I 2022, 1450 – Entscheidungsformel –) und vom 15.06.2023 – 2 BvL 11-12/14, Zeitschrift für das gesamte Familienrecht 2023, 1636 – redaktioneller Leitsatz –; juris) entschieden hat. Die Beteiligten wurden hierüber im August 2023 informiert und hatten in der Folge Gelegenheit zur Stellungnahme. Es hat sich nur die Beklagte und Revisionsbeklagte (Familienkasse) in der Sache geäußert. Im Hinblick auf die Stellungnahme der Familienkasse wurde das Verfahren mit Senatsbeschluss vom 15.05.2024 – III R 22/23 (III R 47/14) getrennt.

Das Revisionsverfahren wegen Festsetzung von Kindergeld für S für die Monate Juli 2010 bis April 2012 und September 2012 bis Juli 2014 wurde unter dem Aktenzeichen III R 22/23 (III R 47/14) weitergeführt. Die Revision wurde insoweit mit Beschluss vom 11.06.2024 als unzulässig verworfen.

In dem hier streitgegenständlichen Verfahren III R 18/24 wegen Kindergeld für S hat die Familienkasse mit Bescheid vom 24.05.2024 zugunsten der Klägerin Kindergeld für S für die Monate Mai 2012 bis einschließlich August 2012 festgesetzt; das Schreiben ging der Klägerin (beziehungsweise ihren Prozessbevollmächtigten) zeitnah zu. Mit Schreiben vom 31.05.2024 und vom 04.06.2024 hat die Familienkasse den BFH unterrichtet und erklärt, dass ihrer Auffassung nach damit der Rechtsstreit in der Hauptsache erledigt sei. Die Schreiben der Familienkasse wurden der Klägerin am 08.06.2024 mit Zustellungsurkunde zugestellt. Sie wurde aufgefordert, innerhalb einer Frist von zwei Wochen ab Zustellung mitzuteilen, ob sie den Rechtsstreit in der Hauptsache (gleichfalls) für erledigt erklärt. Diese Frist ist ergebnislos abgelaufen.

Die Klägerin beantragt sinngemäß,