Herr
Mag. Alfred Hacker
BMF - IV/2 (IV/2)

Johannesgasse 5
1010 Wien

Fax: +43 1514335904050
e-Mail: Alfred.Hacker@bmf.gv.at

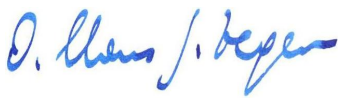
Wien, 13. Juli 2015

Betreff: Ihr Zeichen: BMF-010100/0010-IV/1/2015 /
Unser Zeichen: RECHT11976-RKS-V
Registrierkassensicherheitsverordnung, RKS-V [Verordnung]

In der Anlage finden Sie die Stellungnahme der
ARGE DATEN - Österreichische Gesellschaft für Datenschutz
mit dem Ersuchen um Kenntnisnahme und Berücksichtigung.

Für allfällige Fragen stehen wir gerne zur Verfügung.

Mit vorzüglicher Hochachtung



Mag. Dr. Hans G. Zeger, Vertretung ARGE DATEN als Obmann
cn=Mag. Dr. Hans G. Zeger, Vertretung ARGE DATEN als Obmann, c=AT, l=Wien, st=Wien, o=ARGE DATEN - Österreichische Gesellschaft für Datenschutz, email=hans.zeger@argedaten.at
2015.07.13 18:54:16 +02'00'

Dr. Hans G. Zeger (Obmann)

Anlage:
Stellungnahme

Alle Stellungnahmen werden unter ftp://ftp.freenet.at/privacy/gesetze veröffentlicht.

Stellungnahme der ARGE DATEN vom 13. Juli 2015 zu:

Registrierkassensicherheitsverordnung, RKS-V

Einleitung

Die Bekämpfung von Steuerbetrug und Abgabenhinterziehung stellt eine wesentliche Voraussetzung für eine funktionierende Gemeinschaft dar und dient letztlich allen ehrlichen Staatsbürgern.

Grundsätzlich begrüßt die ARGE DATEN den Versuch Steuerbetrug und Abgabenhinterziehung nicht nur organisatorisch-rechtlich zu bekämpfen, sondern die modernen Technologien der Informationsgesellschaft, insbesondere Zertifizierungsdienste heranzuziehen.

Leider erweist sich die vorgelegte Verordnung nicht konsequent genug und führt daher zu ungeklärten Sicherheitsfragen, erlaubt weiterhin - wenn auch unter erschwerten Bedingungen - Umgehungsmöglichkeiten und es ist fraglich, ob die Verordnung EU-konform ist.

Generelle Feststellungen

Grundsätzlich positiver Ansatz

Die Grundsatzentscheidung der Verordnung Barumsätze mit einer elektronischen Signatur iS § 2 Z 1 SigG zu versehen wird ausdrücklich begrüßt.

Begrüßt wird die Entscheidung das standardisierte und EU-weit geregelte Verfahren der "qualifizierten Zertifikate" im Sinne der EU-Richtlinie 1999/93/EG und dem österreichischen Signaturgesetz (SigG) zur Signatur zu verwenden.

Dieses Verfahren garantiert ausreichende Sicherheit in der Identifikation der Zertifiaktsinhaber, ausreichend sichere Signaturen gemäß Stand der Technik und einen EU-weit einheitlichen Sicherheitsstandard. Weiters existiert eine breite Zahl akkreditierter Anbieter, damit ausreichender Wettbewerb und im Ergebnis niedrige Kosten für die Unternehmen.

Alle alternativen Sicherungs-, Signatur- und Verschlüsselungsverfahren würden im Ergebnis entweder zu propriäteren Lösungen führen mit der Gefahr, dass bestimmte Kassenanbieter bevorzugt werden oder zu zusätzlichen aufwändigen Zulassungs- und Prüfverfahren führen, deren Kosten letztlich auf die Unternehmer überwälzt würden.

Die Gefahr erhöhter Kosten durch Zulassungsverfahren von Sonderlösungen findet sich schon im Verordnungsentwurf im Abschnitt "Geschlossene Gesamtsysteme", auf die in einem eigenen Abschnitt eingegangen wird.

Fehlendes Gesamt-Sicherheitskonzept

Festzuhalten ist, dass elektronische Signaturen gemäß EU-Richtlinie 1999/93/EG und SigG alleine noch kein sicheres Gesamtsystem garantieren, sondern im Falle fortgeschrittener elektronischer Signaturen (iS § 2 Z 3) oder qualifizierter elektronischer Signaturen (iS § 2 Z 3a) bloß die Unverfälschbarkeit der Signatur nach dem Stand der Technik garantieren.

Dies ist für die Verhinderung von Abgabenmanipulationen, wie es Ziel der Registrierkassensicherheitsverordnung ist, nicht ausreichend. Es seien nur einige Manipulationsmöglichkeiten genannt, die typischerweise im Rechnungslegungsbetrug vorkommen:

- ein Umsatz wird nicht eingebucht, Kunde erhält keinen Beleg bzw. verlangt keinen Beleg oder es handelt sich um einen Scheinbeleg
- der Umsatz wird zwar eingebucht, aber der Kunde wünscht keinen Beleg oder der Beleg wird liegen gelassen
- Umsätze werden falschen Kassen, falschen Tagen bzw. Zeiten zugeordnet und nicht in die Gesamtumsätze aufgenommen
- technische Ausfälle verhindern das Aufbringen einer korrekten Signatur

Um diese und weitere Manipulations- und Störmöglichkeiten auszuschalten enthält der Verordnungsentwurf eine Reihe von zusätzlichen Maßnahmen, die im wesentlichen darauf abzielen, zu jeder Registrierkasse eine Belegkette zu schaffen, die fortlaufend nummeriert ist und von einem Beleg zum nächsten die bisherigen Tagesumsätze weitergibt. Dabei werden wesentliche Sicherheitsaufgaben an die Kassensysteme ausgelagert.

Dieses Verfahren ist unter optimalen Bedingungen tatsächlich geeignet zahlreiche Manipulationsfälle zu verhindern, ist jedoch nur bedingt praxistauglich.

[1] Schwachstelle Tagesumsatz

Die Verpflichtung auf den Rechnungsbelegen auch die Tagesumsätze auszuweisen stellt einen enormen und grundrechtlich problematischen Eingriff in die Erwerbsfreiheit der Unternehmen dar. Konkurrenten könnten feststellen, welche Umsätze ein Mitbewerber macht.

Dieser Eingriff soll durch eine hochwertige Verschlüsselung gemildert werden. Damit werden grundsätzlich die Bedürfnisse nach Schutz von Betriebsgeheimnissen gewahrt, die unmittelbare Kontrollmöglichkeit geht jedoch verloren.

Darüber hinaus werden die Daten mittels QR-Code dargestellt. Dies führt jedoch dazu, dass die Daten vom Rechnungsempfänger nicht unmittelbar (Augenschein) geprüft werden können. Ob sinnvolles im QR-Code enthalten ist oder nicht, wäre erst im Zuge der Belegsprüfung einer Betriebsprüfung feststellbar.

Selbst wenn im Zuge einer derartigen Prüfung fehlerhafte QR-Daten auftauchen und es der Prüfbehörde gelingt nachzuweisen, dass nicht nur eine Einzelrechnung fehlerhaft ist, darf

bezweifelt werden, dass der Nachweis gelingt, das ausstellende Unternehmen hätte vorsätzlich eine ganze Reihe von fehlerhaften Belegen produziert.

[2] Schwachstelle Kassen bzw. Kassensoftware

Der Entwurf übersieht, dass die Kassen selbst bzw. ihre Software nicht dieselbe Manipulationssicherheit haben, wie die Signaturerstellungseinheiten. Damit können technische Defekte vorfallen (oder auch vorgetäuscht werden), die das Sicherheitskonzept der Verordnung durchbrechen. Die Verordnung sieht für diese Fälle zwar Meldepflichten vor, diese können jedoch erst greifen, wenn ein Defekt tatsächlich als solcher erkannt wird

Es würde ein Vielfaches an Kosten und Aufwand bedeuten nur zertifizierte Kassensysteme (inkl. Software) zuzulassen. Die Alternative nur mehr zertifizierte Kassensoftware zuzulassen ist auf Grund der enormen Kosten daher nicht machbar.

Im deutschen INSIKA-Konzept werden zahlreiche Sicherheitsanforderungen auf die Signaturerstellungseinheit (dort Smartcard) ausgelagert. Auch diese Lösung ist problematisch, da die Smartcard-Technologie nicht ausfallssicher genug ist. Im übrigen wäre es noch wesentlich billiger "unerwünschte" Smartcards, solche mit hohen Tagesumsätzen, unauffällig so zu beschädigen, dass sie nicht mehr auslesbar sind, was neue Manipulationsmöglichkeiten eröffnet.

Die theoretischen Manipulationsmöglichkeiten der Kassen müssen daher anders verhindert werden.

[3] Schwachstelle Gesamtorganisation

Die Verordnung geht im wesentlichen von der heutigen Kassenorganisation aus, d.h. ein Unternehmen hat eine überschaubare Zahl physischer Kassen, deren Tagesumsätze zusammen gerechnet werden.

Das System erlaubt jedoch auch die Schaffung beliebig vieler "virtueller" Kassen, die auch mit ein und derselben Signaturerstellungseinheit verwaltet werden können. Im Extremfall könnte je Geschäftsfall eine eigene Kasse definiert werden, die Kettenbildung der Belege ginge ins Leere, da in jedem Fall der Vorumsatz 0,- Euro wäre. Zu Tagesende würden dann nur jene "Kassen" zusammengefasst werden, deren Belege tatsächlich ausgefolgt wurden.

Zur Verschleierung der Manipulation ist es realistisch, dass einige Ketten gebildet werden, einzelne Ketten bis zu einem "gewünschten" Tagesumsatz befüllt werden und anschließend alle weiteren Umsätze auf virtuellen Kassen mit Startwert 0,- landen. Die Aufdeckung einer derartigen Manipulation wäre nur durch systematische Prüfung eines Unternehmens möglich. Dies würde einen konkreten Verdacht voraussetzen. Für derartige verdachtsabhängige systematische Betriebsprüfungen ist aber das geplante System nicht notwendig.

[4] Zeitmanipulationen

Die Verordnung übersieht, dass die Registrierkassen "im Feld" keine gesicherte, garantierte Zeit haben. Vergleichbar einem Faxgerät oder einem Privatcomputer kann jeder Benutzer Datum und Uhrzeit nach seinen Bedürfnissen einstellen. Üblicherweise hat niemand ein Interesse an der Zeitmanipulation, aber etwa zum Nachweis der Zustellung eines Faxtextes wird - aus guten Gründen - nicht die Absendezeit verwendet, sondern die Eingangszeit beim Empfänger.

Auch Onlinebanking, E-Government oder alle E-Commerce-Lösungen funktionieren dadurch, dass nicht der Kunde/Klient die Transaktionszeit vorgibt, sondern das System, das er benutzt (der Bankenserver, der Onlineshop oder das Behördenportal).

Diesen Grundsatz - lokalen Zeitangaben grundsätzlich nicht zu vertrauen - vernachlässigt die Registrierkassensicherheitsverordnung völlig. Damit können beliebige Zeitketten geschaffen werden und es ist heute noch nicht absehbar, welche Manipulationsmöglichkeiten sich aus den Zeitmanipulationen ergeben werden.

Vertane Chance einer modernen, flächendeckend wirksamen Billing-Lotterie

Kunden dazu zu bringen, tatsächlich Rechnungsbelege zu verlangen, anzunehmen und aufzubewahren, ist die größte Schwachstelle im Bereich der Verhinderung von Rechnungsmanipulation.

Diese Schwachstelle kann keine der technisch-organisatorischen Maßnahmen dieser Verordnung oder alternativer Systeme beheben. Dies ist nur durch ein Anreizsystem, wie es die Rechnungslotterie darstellt, zu schaffen

Ein zeitgemäßes Lotteriesystem sollte auf Basis generierter Nummern auf den Rechnungsbelegen funktionieren, Manipulationsmöglichkeiten könnten durch Verwendung qualifizierter Zeitangaben verhindert werden. Als Nebeneffekt könnten die in der Verordnung vorgesehenen Prüf- und Umsatzwerte tatsächlich manipulationssicher und unter Beachtung des Datenschutzes zentral verwaltet werden.

Eine derartige Billing-Lotterie würde jede Rechnung zum begehrten Gratislos machen, die Zusatzkosten wären minimal und könnten durch Vereinfachungen des vorliegenden Sicherheitskonzepts wettgemacht werden.

Ausufernde bürokratische Konzeption

Das Verfahren zur Inbetriebnahme einer Registrierkasse mit Sicherheitseinrichtung ist extrem bürokratisch und störanfällig. Die Inbetriebnahme erfordert fünf voneinander getrennte Schritte und dauert - auch bei optimaler Organisation - mehrere Tage. Tatsächlich könnte jedoch die Ausstellung wesentlich reduziert werden.

Problematische Konzeption der "geschlossenen Gesamtsysteme"

Die Bestimmungen für "Geschlossene Gesamtsysteme" sind in sich widersprüchlich. Offenbar sollen Systeme zugelassen werden, die über keine Signaturfunktion verfügen, gleichzeitig sollen die Verfahren "gleichwertig" sein.

Damit werden die Prüf- und Kontrollmöglichkeiten durch die Kunden drastisch reduziert. Der einzelne Kunde kann nicht erkennen ob er eine Rechnung aus einem "geschlossenen Gesamtsystem" erhalten hat oder nicht. Abhängig davon finden sich unterschiedliche Merkmale auf der Rechnung, damit fehlt für Kunden eine ausreichende Rechtssicherheit über die Gestaltung der Belege.

Weiters wird die Überprüfung an Bestätigungsstellen gemäß § 19 SigG übertragen. Es ist nicht nachvollziehbar, warum eine Bestätigungsstelle nach dem Signaturgesetz besondere Fachkenntnis bei einer Lösung hat, die keine Signatur verwendet, entsprechende gerichtlich beeidete Sachverständige oder akkreditierte Stellen nach der eIDAS-Verordnung, die es in Österreich ab Juli 2016 zwingend geben muss, jedoch nicht.

Es darf bezweifelt werden, dass diese Regelung EU-konform ist.

Es wird dringend empfohlen auch für die "geschlossenen Gesamtsysteme" angepasste Signaturlösungen zu finden, damit für Kunden alle Rechnungen denselben strukturellen Aufbau haben. Allenfalls sind für bestehende Lösungen längere Übergangszeiten vorzusehen.

Zusammenfassung

Der Entwurf ist ein wichtiger Schritt in die richtige Richtung, er sollte jedoch um folgende Punkte erweitert werden:

(a) Verpflichtung der Unternehmen ihre Kassenumsätze zum Schutz gegen nachträgliche Manipulationen mit einem qualifizierten Zeitwert (Zeitstempel) zu versehen und zu sichern. Diese Zeitstempel würden einige Manipulationsmöglichkeiten reduzieren und hätten gleichzeitig die Funktion der Datensicherung der wichtigsten Umsatzmerkmale bei einer sicherheitstechnisch besonders gut ausgestatteten akkreditierten Stelle.

(b) Jedenfalls sollte das Datenerfassungsprotokoll in regelmäßigen Abständen revisionssicher und zum Schutz gegen nachträgliche Manipulationen mit einem qualifizierten Zeitwert (Zeitstempel) versehen werden.

(c) Die Zuordnung der Signaturerstellungseinheiten zu bestimmten Kassen bzw. die Limitierung der Zahl der Kassen je Signaturerstellungseinheit (zB. auf maximal 10 Kassen je Einheit) sollte verbessert werden. Dies könnte durch die verpflichtende Aufnahme entsprechener Zertifikatseigenschaften in den Signaturerstellungseinheiten manipulationssicher umgesetzt werden.

(d) Statt dem komplizierten und aufwändigen Sonderzulassungsverfahren für "Geschlossene Gesamtsysteme" sollten auch diese Systeme mit Signaturlösungen ausgestattet werden und die Akkreditierung durch eine Aufsichtstelle gemäß Artikel 17 eIDAS-Verordnung (910/2014 L 257/73) erfolgen.

(e) Die rechtliche Stellung von Zertifikat und Signatur sind, insbesondere in Hinblick auf die allgemeinen Feststellungen des SigG genauer zu definieren und zu verbessern.

Stellungnahme zu einzelnen Bestimmungen

§ 3 Z 20 Signatur

Das Signaturgesetz verwendet in § 2 Z 1 den Begriff "elektronische Signatur". Dieser Begriff wird EU-weit verwendet. Es wird daher empfohlen auch in der Verordnung diesen Begriff statt "*Signatur (auch kryptografische Signatur)*" zu verwenden.

§ 3 Z 23 Signaturzertifikat

Statt der Sonderdefinition sollten die Formulierungen des Signaturgesetzes § 2 Z 8,9 (Zertifikat und qualifiziertes Zertifikat) verwendet werden und an die Anforderungen der Bestimmungen der §§ 131, 131b angepasst werden.

Insbesondere steht die derzeitige Formulierung in § 3 Z 26 im Widerspruch zur Anforderung, dass die Zertifikate über die Trust-List der EU prüfbar sein sollen. Prüfbar mittels dieser Liste sind nur qualifizierte Zertifikate. Diese sind jedoch natürlichen Personen zugeordnet.

Offenbar soll die Formulierung in Z 23 zum Ausdruck bringen, dass qualifizierte Zertifikate zu verwenden sind, die natürlichen Personen als Steuersubjekt (Personengesellschaften, Einzelunternehmen) oder als berechtigte Organe eines Steuersubjekts (etwa bei juristischen Personen) zugeordnet sind. Das sollte in die Definition auch hineingeschrieben werden.

Weiters sollte klargestellt werden, dass die Festlegung, wer berechtigtes Organ eines Steuersubjekts ist vom Unternehmen zu treffen ist und an keine weiteren Anforderungen (etwa Zeichnungsberechtigung, Prokura, Eintrag im Firmenbuch usw.) gebunden ist.

§ 3 Z 26 Trust-List

Die Trust-List verwaltet nur Zertifikate zugelassener Zertifizierungsdiensteanbieter, die zur Ausstellung qualifizierter Zertifikate geeignet sind. Es ist daher klarzustellen, dass die Zertifikate im Rahmen der Registrierkassensicherheitsverordnung qualifizierte Zertifikate sein müssen.

§ 3 fehlende Festlegungen

Signaturen, die mittels qualifizierter Zertifikate ausgestellt werden, sind als eigenhändige Unterschriften des Zertifikatsinhabers anzusehen und entfalten eine entsprechende Rechtswirksamkeit. Es ist jedoch weltfremd anzunehmen, dass die in den Kassen installierten Signaturerstellungseinheiten ausschließlich von jener Person verwendet werden, auf deren Namen die Signaturerstellungseinheit ausgestellt wurde.

Dies würde im Ergebnis bedeuten, dass jeder Kellner, jeder Verkäufer eine persönliche Signaturerstellungseinheit zugewiesen hätte, Belege derselben Registrierkasse durch verschiedene Signaturerstellungseinheiten signiert würden und damit die § 16 geforderte Zuordnung von Signaturerstellungseinheit und Registrierkassa nicht möglich wäre.

Tatsächlich wird die Signatur vom Verkaufspersonal zwar angestoßen, ist aber nicht auf dessen Namen ausgestellt.

Es ist daher der Stellenwert dieser Signatur in der Registrierkassensicherheitsverordnung zu definieren. Es sollte klargestellt werden, dass Signaturen dieser Signaturerstellungseinheiten in Kassensystemen nicht eine qualifizierte Signatur darstellen, sondern einem Siegel im Sinne Abschnitt 5 der eIDAS-Verordnung entspricht, dass vom Unternehmen ausgestellt wurde. Dies könnte auch durch Vergabe einer geeigneten OID automationsunterstützt verwaltet werden.

Weiters sind die Aufbewahrungspflichten der Signaturerstellungseinheit auf den tatsächlichen Anwendungsfall anzupassen. § 2 Z 3 lit a SigG verlangt die "ausschließliche Zuordnung des Zertifikates dem Signator", eine Anforderung, die bei den Registrierkassen nicht erfüllt ist. Zweck der Registrierkasse im Sinne dieser Registrierkassensicherheitsverordnung ist es eben, dass verschiedenste Personen Umsätze einbuchen können und alle Umsätze mit derselben Signaturerstellungseinheit unterfertigt werden, im Normalfall jedoch ohne Zutun oder Anwesenheit des Signators, auf den das Zertifikat ausgestellt wurde.

Die Verantwortung des Signators sollte daher soweit begrenzt werden, als er verpflichtet wird die für Zwecke der Sicherheit der Registrierkassen ausgestellten Signaturerstellungseinheiten im Sinne dieser Verordnung korrekt installiert sind.

§ 6 fehlende Regelung bei Neustart bzw. Reset von Kassen

Es kann aus zahlreichen Gründen notwendig sein, eine Kassa neu zu initialisieren (defekte Bauteile, Updates, Upgrates, Bedienfehler, sonstige Hard- oder Softwarefehler).

Die Verordnung enthält keinerlei Hinweise, wie in diesen Fällen vorzugehen ist. Dieser Punkt ist zu ergänzen.

§ 7 Datenerfassungsprotokoll

Es fehlen Angaben zur revisionssicheren Erstellung des Datenerfassungsprotokolls. So sollte jedenfalls gefordert werden, dass die gesicherte Version (Abs. 3) zu signieren ist und mit einem garantierten Zeitwert (Zeitstempel) zur Verhinderung nachträglicher Manipulationen zu versehen ist.

§§ 15, 16 Beschaffung und Registrierung der Signaturerstellungseinheit

Der beschriebene Ablauf ist zu bürokratisch und könnte durch Restrukturierung im Sinne des One-Stop-Shop-Prinzips bei den ausstellenden Zertifizierungsdienstanbietern erfolgen.

§§ 20ff Geschlossene Gesamtsysteme - gleichheitswidrige Konzeption

Es ist zwar nachvollziehbar, dass Betreiber großer Registrierkassennetze eigene Lösungen wünschen. Aus Sicht der Gesamteffizienz des Systems und auch aus Transparenzgründen gegenüber Kunden sollten derartige Lösungen jedoch nicht umgesetzt werden oder nur die absolute Ausnahme darstellen.

Es wird daher vorgeschlagen statt eigener Zulassungsverfahren für diese Systeme längere Anpassungsfristen vorzusehen, etwa bei Systemen zwischen 500-2000 Kassen ein Jahr länger, bei Systemen über 2000 Kassen zwei Jahre länger.

Im übrigen sind die Bestimmungen in sich widersprüchlich, so wird etwa in § 21 Abs. 2 gefordert, dass die Systeme "*sicherheitstechnisch mit einer Signaturerstellungseinheit gleichwertig*" sind.

Sind sie tatsächlich gleichwertig, dann entsprechen sie den Vorgaben des SigG bzw. der SigV und es können auch entsprechende Zertifikate ausgestellt werden, die mittels der Trust-List geprüft werden. Sind sie nicht gleichwertig, dürften sie nicht zugelassen werden.

Das im Abschnitt beschriebene Zulasssungsverfahren entspricht, wird es ernst genommen, einem Zulassungsverfahren im Sinne der Zertifizierungsdiensteanbieter.

Soll es jedoch die Möglichkeit darstellen, für priviligierte Unternehmen ein Zulassungsverfahren "light" zu schaffen, dann wäre das als gleichheitswidrig, sachlich unbegründet und EU-widrig abzulehnen.