

Verordnung des Bundesministers für Finanzen über die technischen Einzelheiten für Sicherheitseinrichtungen in den Registrierkassen und andere, der Datensicherheit dienende Maßnahmen (Registrierkassensicherheitsverordnung, RKS SV)

Aufgrund der §§ 131b Abs. 5 Z 1, 3 und 4 und § 132a Abs. 8 der Bundesabgabenordnung – BAO, BGBl. Nr. 194/1961, zuletzt geändert durch das Bundesgesetz BGBl. I Nr. 118/2015, wird verordnet:

Inhaltsverzeichnis

1. Hauptstück Allgemeiner Teil

- § 1. Anwendungsbereich
- § 2. Personenbezogene Bezeichnungen
- § 3. Abkürzungen und Begriffsbestimmungen

2. Hauptstück Technische Vorschriften

1. Abschnitt Allgemeines

- § 4. Beschreibung der Sicherheitseinrichtung

2. Abschnitt Anforderungen an die Registrierkasse

- § 5. Allgemeine Anforderungen
- § 6. Inbetriebnahme der Sicherheitseinrichtung für die Registrierkasse
- § 7. Datenerfassungsprotokoll
- § 8. Summenspeicher
- § 9. Signaturerstellung durch die Signaturerstellungseinheit
- § 10. Aufbereitung des maschinenlesbaren Codes
- § 11. Belegerstellung

3. Abschnitt Anforderungen an die Signaturerstellungseinheiten

- § 12. Allgemeine Anforderungen
- § 13. Signaturschlüsselpaar und Signaturerstellung
- § 14. Verifizierbarkeit der Signaturen

3. Hauptstück Beschaffung und Registrierung der Signaturerstellungseinheit; Kontrolle

- § 15. Beschaffung der Signaturerstellungseinheit
- § 16. Registrierung der Signaturerstellungseinheit
- § 17. Bekanntgabe der Außerbetriebnahme der Sicherheitseinrichtung für die Registrierkasse
- § 18. Datenbank über Sicherheitseinrichtungen für die Registrierkassen
- § 19. Kontrolle und Prüfung der Datensicherheit für die Registrierkassen

4. Hauptstück Geschlossene Gesamtsysteme

- § 20. Technische und organisatorische Anforderungen
- § 21. Sachverständige Begutachtung geschlossener Gesamtsysteme
- § 22. Feststellungsbescheid
- § 23. Änderung der tatsächlichen Verhältnisse
- § 24. Kontrolle der Identität der Softwarekomponente laut § 21 Abs. 2

5. Hauptstück Schlussbestimmungen

- § 25. Inkrafttreten

1. Hauptstück Allgemeiner Teil

Anwendungsbereich

§ 1. Die Registrierkassensicherheitsverordnung regelt

1. die zur technischen Umsetzung der Manipulationssicherheit elektronischer Aufzeichnungssysteme erforderlichen technischen Merkmale
 - a) der Registrierkasse,
 - b) der Signaturerstellungseinheit,
 - c) der Kommunikation zwischen Registrierkasse und Signaturerstellungseinheit,
2. die zusätzlichen Anforderungen an den Beleg gemäß § 132a Abs. 8 BAO,
3. Einzelheiten über die Erlassung von Feststellungsbescheiden betreffend geschlossene Gesamtsysteme und
4. den Zugriff der Behörden auf die dafür erforderlichen Daten für aufsichts- und abgabenrechtliche Zwecke.

Personenbezogene Bezeichnungen

§ 2. Alle in dieser Verordnung verwendeten personenbezogenen Bezeichnungen gelten gleichermaßen für Personen sowohl weiblichen als auch männlichen Geschlechts.

Abkürzungen und Begriffsbestimmungen

§ 3. Im Sinne dieser Verordnung ist oder sind:

1. AES-256: Verschlüsselungsverfahren nach dem Advanced Encryption Standard (AES FIPS 197 26/11/2001) mit einer Schlüssellänge von 256 Bit
2. Barcode: Standard „Code 128“, definiert in ISO/IEC 15417:2007
3. Barumsatz: Umsätze im Sinne § 131b Abs. 1 Z 3 BAO
4. Datenbank über Sicherheitseinrichtungen in Registrierkassen: Datenbank des Bundesministeriums für Finanzen, in der die in § 18 Abs. 2 genannten Daten betreffend die Sicherheitseinrichtungen in Registrierkassen und Kontrollen der Sicherheitseinrichtungen festgehalten werden
5. Datenerfassungsprotokoll (DEP): eine im Speicher der Registrierkasse oder in einem externen Speicher mitlaufende Ereignisprotokolldatei, die in Echtzeit jeweils mit Belegerstellung vollständig, fortlaufend chronologisch die Barumsätze mit Beleginhalten dokumentiert
6. Eingabestation: Einrichtung zur Erfassung von Barumsätzen, die mit einer Registrierkasse insbesondere zur Signierung und Dokumentation der Barumsätze verbunden ist
7. Elektronische Aufzeichnung: vollständige, fortlaufend chronologisch geordnete Dokumentation von Bargeschäften in elektronischer Form
8. Elektronische (kryptographische) Signatur: elektronische Daten, die anderen elektronischen Daten beigefügt oder mit diesen logisch verknüpft werden und die der Authentifizierung dienen im Sinne des § 2 Z 1 SigG
9. FinanzOnline: elektronisches Verfahren der Abgabenbehörde nach der FinanzOnline-Verordnung 2006, BGBl. II Nr. 97/2006, in der jeweils geltenden Fassung
10. Geschlossenes Gesamtsystem: elektronisches Aufzeichnungssystem, in welchem Warenwirtschafts-, Buchhaltungs- und Kassensysteme lückenlos miteinander verbunden sind und das mit mehr als 30 Registrierkassen verbunden ist.
11. Global Location Number (GLN): von der Bundesanstalt Statistik Österreich unter der Bezeichnung „Sekundär ID“ vergebener Ordnungsbegriff
12. Hardware-Sicherheitsmodul (HSM): Signaturerstellungseinheit, die zur Erstellung (qualifizierter) elektronischer Signaturen verwendet wird und vor allem bei serverbasierten Lösungen zum Einsatz kommt
13. Homepage des Bundesministeriums für Finanzen (BMF): www.bmf.gv.at
14. Kassenidentifikationsnummer: über FinanzOnline gemeldetes Kennzeichen einer Registrierkasse, das auch die Unterscheidung verschiedener Registrierkassen mit gleicher Signaturerstellungseinheit ermöglicht
15. Maschinenlesbarer Code: Eingangswert für OCR-, Barcode- oder QR-Code-Repräsentation
16. Monatszähler: Summenspeicher in der Registrierkasse, der die Zwischenstände des Umsatzzählers zum Monatsende festhält

17. Object Identifier (OID): weltweit eindeutiger Bezeichner nach ISO/IEC 9834-1 und A 2642, der benutzt wird, um ein Informationsobjekt zu benennen. In dieser Verordnung wird der OID verwendet, um die Verwendung des Signaturzertifikates nach § 5 Abs. 1 Z 8 des Signaturgesetzes – SigG, BGBl. I Nr. 190/1999 in der jeweils geltenden Fassung, auf den Zweck 'Österreichische Finanzverwaltung Registrierkasseninhaber' einzuschränken.
18. OCR (Optical Character Recognition): Standard OCR-A, definiert in ISO 1073-1:1976
19. Ordnungsbegriff des Unternehmers: ein der Abgabenbehörde bekannter Schlüssel zur Identifizierung des Unternehmers (Steuernummer, UID-Nummer, GLN)
20. QR-Code: zweidimensionales Symbol nach Standard JIS X 0510/2004
21. Registrierkasse (auch elektronische Registrierkasse): verallgemeinerte Form jedes elektronischen Datenverarbeitungssystems, das elektronische Aufzeichnungen zur Losungsermittlung und Dokumentation von einzelnen Barumsätzen erstellt, insbesondere elektronische Registrierkassen jeglicher Bauart, serverbasierte Aufzeichnungssysteme (auch zur Abwicklung von Online-Geschäften), Waagen mit Kassenfunktionen und Taxameter. Eine Registrierkasse kann mit Eingabestationen verbunden sein.
22. Seriennummer des Signaturzertifikates: eine durch den Zertifizierungsdiensteanbieter ausgegebene, im Zertifikat enthaltene, eindeutige Kennung des Zertifikates zum erleichterten Auffinden des Zertifikates im Verzeichnis des ZDA
23. Sichere Signaturerstellungseinheit: konfigurierte Software oder Hardware, die zur Verarbeitung der Signaturerstellungsdaten verwendet wird und die den Sicherheitsanforderungen des SigG sowie den dazu erlassenen Verordnungen entspricht (§ 2 Z 5 SigG)
24. Signaturprüfdaten: Daten wie Codes oder öffentliche Signaturschlüssel, die zur Überprüfung einer elektronischen Signatur verwendet werden (§ 2 Z 6 SigG)
25. Signaturwert: im Rahmen der Signaturerstellung ermittelter elektronischer Wert der Signatur
26. Startbeleg: erster Beleg, der unter Verwendung einer Kassenidentifikationsnummer erstellt wird und die vollständige Verkettung aller unter dieser Kassenidentifikationsnummer erzeugten und gespeicherten Belege sicherstellt
27. Summenspeicher: Speicher in der Registrierkasse, die Zwischen- oder einen aktuellen Endstand aufsummierter Beträge wiedergeben
28. Trust-List (vertrauenswürdige Liste gemäß der Entscheidung der Kommission 2009/767/EG über Maßnahmen zur Erleichterung der Nutzung elektronischer Verfahren über einheitliche Ansprechpartner gemäß der Richtlinie 2006/123/EG über Dienstleistungen im Binnenmarkt, ABl. Nr. L 274 vom 20.10.2009 S. 36): nach den Verpflichtungen aus Artikel 2 der Entscheidung 2009/767/EG von allen Mitgliedstaaten zu führende Liste der ZDAs für qualifizierte Zertifikate)
29. Umsatzzähler: Summenspeicher in der Registrierkasse, der die Barumsätze der Registrierkasse laufend aufsummiert
30. Verifikation: Überprüfung signierter Daten auf Integrität und Authentizität, dass die Daten nach der Signaturerstellung von der korrekten Signaturerstellungseinheit signiert und nicht verändert wurden
31. Zahlungsbeleg (Beleg): Bestätigung mit bestimmten formalen Inhalten, die in Papierform oder in elektronischer Form den wesentlichen Inhalt des Rechtsgeschäftes zwischen den Geschäftspartnern dokumentiert und bei Bezahlung übergeben bzw. elektronisch übermittelt wird
32. Zertifikat: eine elektronische Bescheinigung, mit der Signaturprüfdaten einer bestimmten Person zugeordnet werden und deren Identität bestätigt wird im Sinne des § 2 Z 8 SigG, BGBl. I Nr. 190/1999;
33. Zertifizierungsdiensteanbieter (ZDA): Organisation, die Zertifikate ausstellt oder anderweitige Dienste im Zusammenhang mit elektronischen Signaturen bereitstellt im Sinne der Richtlinie 1999/93/EG über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen.

2. Hauptstück Technische Vorschriften

1. Abschnitt Allgemeines

Beschreibung der Sicherheitseinrichtung

§ 4. (1) Die Sicherheitseinrichtung gemäß § 131b Abs. 2 BAO besteht aus einer Verkettung der Barumsätze mit Hilfe der elektronischen Signatur der Signaturerstellungseinheit.

(2) Die Verkettung wird durch die Einbeziehung von Elementen der zuletzt vergebenen, im Datenerfassungsprotokoll gespeicherten Signatur in die aktuell zu erstellende Signatur gebildet. Bei der Erfassung des ersten Barumsatzes tritt an die Stelle der zuletzt vergebenen Signatur die Kassenidentifikationsnummer.

2. Abschnitt Anforderungen an die Registrierkasse

Allgemeine Anforderungen

§ 5. (1) Jede Registrierkasse muss über ein Datenerfassungsprotokoll und einen Drucker zur Erstellung oder eine Vorrichtung zur elektronischen Übermittlung von Zahlungsbelegen verfügen.

(2) Jede Registrierkasse muss über eine geeignete Schnittstelle zu einer Sicherheitseinrichtung mit einer Signaturerstellungseinheit verfügen. Mit einer Signaturerstellungseinheit können auch mehrere Registrierkassen verbunden sein.

(3) Jede Registrierkasse muss mit dem frei verfügbaren Verschlüsselungsalgorithmus AES 256 ausgestattet sein, um die für den maschinenlesbaren Code erforderlichen Verschlüsselungen durchführen zu können.

(4) Jeder Registrierkasse muss eine eindeutige Kassenidentifikationsnummer im Unternehmen zugeordnet werden.

(5) Die Registrierkasse darf keine Vorrichtungen enthalten, über die das Ansteuern der Sicherheitseinrichtung umgangen werden kann.

(6) Die Nutzung einer Registrierkasse durch mehrere Unternehmer ist nur unter der Voraussetzung zulässig, dass jeder Unternehmer ein ihm zugeordnetes Zertifikat verwenden und die Registrierkasse für jeden Unternehmer ein gesondertes Datenerfassungsprotokoll führen kann.

Inbetriebnahme der Sicherheitseinrichtung für die Registrierkasse

§ 6. (1) Die Inbetriebnahme der Sicherheitseinrichtung für die Registrierkasse besteht aus der Einrichtung des Datenerfassungsprotokolls (§ 7) und der Ablage der Kassenidentifikationsnummer als Bestandteil der zu signierenden Daten des ersten Barumsatzes mit Betrag Null (0) (Startbeleg) im Datenerfassungsprotokoll.

(2) Vor dem 1. Jänner 2017 kann die Inbetriebnahme der Sicherheitseinrichtung im Sinne Abs. 1 bereits vor der Registrierung (§ 16) vorgenommen werden. Die Registrierung muss bis zum 1. Jänner 2017 erfolgt sein.

(3) Wird eine Registrierung nach dem 31. Dezember 2016 vorgenommen, so hat die Inbetriebnahme binnen einer Woche nach Registrierung der Signaturerstellungseinheit (§ 16) zu erfolgen.

(4) Der Unternehmer hat vor Inbetriebnahme die Erstellung der Signatur (§ 9 Abs. 3) und die Verschlüsselung des Umsatzzählers (§ 9 Abs. 2 Z 5) unter Zuhilfenahme des Startbeleges zu überprüfen. Entspricht die Erstellung der Signatur bzw. die Verschlüsselung des Umsatzzählers nicht den Erfordernissen des § 9, so ist die Registrierkasse unmittelbar als Registrierkasse mit ausgefallener Signaturerstellungseinheit im Sinne § 17 Abs. 4 zu behandeln. Das Prüfergebnis ist zu protokollieren und mit dem ausgedruckten Startbeleg gemäß § 132 BAO aufzubewahren.

Datenerfassungsprotokoll

§ 7. (1) Jede Registrierkasse hat ein Datenerfassungsprotokoll zu führen, in dem jeder einzelne Barumsatz zu erfassen und abzuspeichern ist. Für jeden Barumsatz sind zumindest die Belegdaten gemäß § 132a Abs. 3 BAO festzuhalten.

(2) Trainings- und Stornobuchungen sind wie Barumsätze zu erfassen und im Datenerfassungsprotokoll abzuspeichern.

(3) Die Daten des Datenerfassungsprotokolls sind zumindest vierteljährlich auf einem elektronischen externen Medium unveränderbar zu sichern. Diese Sicherung ist gemäß § 132 BAO aufzubewahren.

(4) Die Inhalte des maschinenlesbaren Codes (§ 10 Abs. 2) der Barumsätze sind im Datenerfassungsprotokoll der Registrierkasse gemeinsam mit den zugehörigen Barumsätzen festzuhalten.

(5) Das Datenerfassungsprotokoll einer Registrierkasse muss ab 1. Jänner 2017 jederzeit auf einen externen Datenträger im Exportformat Datenerfassungsprotokoll laut Z 3 der Anlage exportiert werden können.

Summenspeicher

§ 8. (1) Die in der Registrierkasse erfassten Barumsätze sind laufend aufzusummieren (Umsatzzähler). Trainingsbuchungen dürfen sich nicht auf den Umsatzzähler auswirken.

(2) Zu jedem Monatsende sind die Zwischenstände des Umsatzzählers zu ermitteln (Monatzzähler) und als Barumsatz mit Betrag Null (0) und elektronischer Signatur der Signaturerstellungseinheit (Monatsbeleg) im Datenerfassungsprotokoll der Registrierkasse zu speichern.

(3) Mit Ablauf jedes Kalenderjahres ist der Monatsbeleg, der den Zählerstand zum Jahresende enthält (Jahresbeleg), auszudrucken, zu prüfen und gemäß § 132 BAO aufzubewahren. Bei der Prüfung des Jahresbeleges ist § 6 Abs. 4 sinngemäß anzuwenden.

Signaturerstellung durch die Signaturerstellungseinheit

§ 9. (1) Zur Gewährleistung des Manipulationsschutzes im Sinne des § 131b Abs. 2 BAO müssen von der Registrierkasse über eine geeignete Schnittstelle zur Signaturerstellungseinheit elektronische Signaturen angefordert und übernommen werden können. Jeder einzelne Barumsatz und Monats-, Jahres- und Schlussbeleg sowie jede Trainings- und Stornobuchung sind elektronisch zu signieren.

(2) In die Signaturerstellung sind folgende Daten einzubeziehen:

1. Kassenidentifikationsnummer
2. Fortlaufende Nummer des Barumsatzes
3. Datum und Uhrzeit der Belegausstellung
4. Betrag der Barzahlung nach Steuersätzen gemäß § 10 Umsatzsteuergesetz 1994 (UStG 1994) in der jeweils geltenden Fassung getrennt
5. Mit dem Verschlüsselungsalgorithmus AES 256 laut Z 8 und Z 9 der Anlage verschlüsselter Stand des Umsatzzählers
6. Seriennummer des Signaturzertifikates
7. Signaturwert des vorhergehenden Barumsatzes des Datenerfassungsprotokolls (Verkettungswert laut Z 4 der Anlage)

(3) Die aufbereiteten Daten (Abs. 2) müssen nach dem Signaturformat laut Z 4 und Z 5 der Anlage durch die Signaturerstellungseinheit automatisiert elektronisch signiert werden.

(4) Die von der Signaturerstellungseinheit im Ergebnisformat der Signaturerstellung laut Z 6 der Anlage rückgemeldete Signatur ist auf dem zugehörigen Beleg nach den Vorgaben des § 10 als Teil des maschinenlesbaren Codes abzdrukken und im Datenerfassungsprotokoll mit den Belegdaten laut Z 11 der Anlage dauerhaft zu speichern (§ 7 Abs. 4).

Aufbereitung des maschinenlesbaren Codes

§ 10. (1) Nach Ermittlung jedes Signaturwertes hat die Registrierkasse für die Belegerstellung und die Speicherung im Datenerfassungsprotokoll einen maschinenlesbaren Code laut Z 12 der Anlage aufzubereiten.

(2) Der maschinenlesbare Code hat folgende Daten zu enthalten:

1. Kassenidentifikationsnummer
2. Fortlaufende Nummer des Barumsatzes
3. Datum und Uhrzeit der Belegausstellung
4. Betrag der Barzahlung nach Steuersätzen getrennt
5. Mit dem Verschlüsselungsalgorithmus AES 256 laut Z 8 und Z 9 der Anlage verschlüsselter Stand des Umsatzzählers
6. Seriennummer des Signaturzertifikates
7. Signaturwert des vorhergehenden Barumsatzes des Datenerfassungsprotokolls (Verkettungswert laut Z 4 der Anlage)

8. Signaturwert des betreffenden Barumsatzes.

(3) Trainings- und Stornobuchungen haben im maschinenlesbaren Code zusätzlich die Bezeichnung „Trainingsbuchung“ oder „Stornobuchung“ zu enthalten.

Belegerstellung

§ 11. (1) Auf dem Beleg sind neben den Belegdaten des § 132a Abs. 3 BAO folgende Daten auszuweisen:

1. Kassenidentifikationsnummer
2. Datum und Uhrzeit der Belegausstellung
3. Betrag der Barzahlung nach Steuersätzen getrennt
4. Inhalt des maschinenlesbaren Code.

(2) Sofern ein maschinenlesbarer Code nicht als QR-Code am Beleg aufgedruckt werden kann, sind die Daten nach Abs. 1 entweder

1. als ein vom Signaturwert des betreffenden Barumsatzes abhängiger Link in maschinenlesbarer Form als Barcode oder OCR zum Abruf der Daten bereitzuhalten und am Beleg auszuweisen oder
2. entsprechend der in Z 14 der Anlage festgelegten Codierung am Beleg auszuweisen.

(3) Belege für Trainings- und Stornobuchungen sind ausdrücklich als solche zu bezeichnen.

3. Abschnitt

Anforderungen an die Signaturerstellungseinheiten

Allgemeine Anforderungen

§ 12. Die technischen Anforderungen an die Signaturerstellungseinheit entsprechen den Anforderungen an Signaturerstellungseinheiten für qualifizierte Signaturen nach § 18 SigG in der jeweils geltenden Fassung und nach § 6 der Signaturverordnung 2008 – SigV 2008, BGBl. II Nr. 3/2008, in der jeweils geltenden Fassung BGBl. II Nr. 401/2010. Anstelle der in § 6 Abs. 3 letzter Satz SigV 2008 vorgesehenen Prüfung kann eine Prüfung in Bezug auf die inhaltlichen Anforderungen der Registrierkassensicherheitsverordnung erfolgen, wobei die Anforderung der alleinigen Kontrolle und deren Auswirkungen auf den Betrieb auf Grund der Verkettung nicht Gegenstand dieser Prüfung sind.

Signaturschlüsselpaar und Signaturerstellung

§ 13. Bezüglich anwendbarer Signaturalgorithmen sowie Schlüssel sind die Regelungen der SigV 2008 zu den Algorithmen und Parametern für qualifizierte Signaturen aus dem Anhang zur SigV 2008, Punkte 1 bis 7 „Algorithmen und Parameter für qualifizierte elektronische Signaturen“ anzuwenden.

Verifizierbarkeit der Signaturen

§ 14. Der Signaturwert des betreffenden Barumsatzes muss an Hand des auf dem Beleg aufgebrachten maschinenlesbaren Codes verifizierbar sein. Dazu müssen insbesondere die in § 10 Abs. 2 enthaltenen Daten auf dem Beleg enthalten sein. Die Vorbereitung der dazu in komprimierter Form im maschinenlesbaren Code enthaltenen Daten hat gemäß Z 13 der Anlage zu erfolgen.

3. Hauptstück

Beschaffung und Registrierung der Signaturerstellungseinheit; Kontrolle

Beschaffung der Signaturerstellungseinheit

§ 15. (1) Unternehmer, die der Registrierkassenpflicht nach § 131b BAO unterliegen, haben die erforderliche Anzahl von Signaturerstellungseinheiten bei einem im EU-/EWR-Raum oder in der Schweiz niedergelassenen Zertifizierungsdiensteanbieter, der qualifizierte Signaturzertifikate anbietet, zu erwerben. Die Kosten für die Beschaffung der Signaturerstellungseinheit trägt der Unternehmer.

(2) Der Unternehmer hat zur Erlangung des Signaturzertifikates einen der Abgabenbehörde bekannten, dem Unternehmer zugeordneten Ordnungsbegriff und als Wert des OID „Österreichische Finanzverwaltung Registrierkasseneinhaber“ (Z 16 der Anlage) nach Maßgabe des § 5 Abs. 1 Z 8 SigG in seinem Signaturzertifikat eintragen zu lassen.

(3) Der Zertifizierungsdiensteanbieter vergibt für jede Signaturerstellungseinheit ein Signaturzertifikat, das folgende Angaben beinhaltet:

1. Typ und Wert des der Signaturerstellungseinheit zugeordneten Ordnungsbegriffs des Unternehmers,
2. Seriennummer des Signaturzertifikates und
3. Beginn und Ende der Gültigkeit des Zertifikats.

Eine Verwendung des Zertifikates über das Ende seiner Gültigkeit hinaus ist zulässig, sofern der im Zertifikat vorhandene Signaturalgorithmus laut Z 2 der Anlage als sicher gilt.

Registrierung der Signaturerstellungseinheit

§ 16. (1) Der Unternehmer oder sein bevollmächtigter Parteienvertreter hat über FinanzOnline den Erwerb seiner Signaturerstellungseinheiten zu melden. Dabei sind die Seriennummer des Signaturzertifikates, die Art der Signaturerstellungseinheit und die Kassenidentifikationsnummern der mit der Signaturerstellungseinheit zu verbindenden Registrierkassen bekannt zu geben. Zusätzlich hat der Unternehmer den frei wählbaren Benutzerschlüssel für die Entschlüsselung (Z 8 der Anlage) der mit dem Verschlüsselungsalgorithmus AES 256 verschlüsselten Daten im maschinenlesbaren Code über FinanzOnline bekannt zu geben. Ist dem Unternehmer die Meldung über FinanzOnline mangels technischer Voraussetzungen unzumutbar, hat die Meldung unter Verwendung des amtlichen Vordrucks zu erfolgen.

(2) Erst nach Prüfung, ob für jede gemeldete Signaturerstellungseinheit unter der angegebenen Seriennummer des Signaturzertifikates und dem gültigen Ordnungsbegriff des Unternehmers der ZDA in der öffentlichen Trust-List und das Signaturzertifikat im Verzeichnis des ZDA vorhanden sind, werden diese Daten an die Datenbank über Sicherheitseinrichtungen in Registrierkassen (§ 18) übergeben.

Bekanntgabe der Außerbetriebnahme der Sicherheitseinrichtung für die Registrierkasse

§ 17. (1) Der Unternehmer oder sein bevollmächtigter Parteienvertreter hat über FinanzOnline oder dem für die Erhebung der Umsatzsteuer zuständigen Finanzamt jeden nicht nur vorübergehenden Ausfall und jede Außerbetriebnahme der Sicherheitseinrichtung in der Registrierkasse bei

1. Diebstahl oder sonstigem Verlust der Signaturerstellungseinheit oder Registrierkasse,
2. Funktionsverlust der Signaturerstellungseinheit oder Registrierkasse oder
3. Außerbetriebnahme der Signaturerstellungseinheit oder Registrierkasse

ohne unnötigen Aufschub bekannt zu geben.

(2) Dazu hat der Unternehmer folgende Angaben zu machen:

1. Bezeichnung der betroffenen Komponenten der Sicherheitseinrichtung
2. Grund des Ausfalles oder der Außerbetriebnahme
3. Beginn des Ausfalles oder der Außerbetriebnahme

(3) Alle über FinanzOnline gemeldeten, nicht nur vorübergehenden Ausfälle und Außerbetriebnahmen werden in der Datenbank über Sicherheitseinrichtungen für die Registrierkassen vermerkt.

(4) Bei jedem Ausfall der Signaturerstellungseinheit sind die Barumsätze auf einer anderen Registrierkasse zu erfassen, die über eine aufrechte Verbindung zu einer Signaturerstellungseinheit verfügt. Sollte dies nicht möglich sein, hat der Unternehmer bei der Aufbereitung und Verwendung des maschinenlesbaren Codes (§ 10) an Stelle des Signaturwertes des betreffenden Barumsatzes (§ 10 Abs. 2 Z 8) die Zeichenkette „Sicherheitseinrichtung ausgefallen“ im Ergebnis der Signaturerstellung laut Z 6 der Anlage zu verwenden. Der Hinweis „Sicherheitseinrichtung ausgefallen“ ist zusätzlich gut sichtbar am Beleg (§ 11) anzubringen. Nach Wiederinbetriebnahme der Signaturerstellungseinheit ist zusätzlich über die Belege, die während des jeweiligen Ausfalles mit dem Hinweis „Sicherheitseinrichtung ausgefallen“ zu versehen waren, ein signierter Sammelbeleg mit Betrag Null (0) zu erstellen und im Datenerfassungsprotokoll zu speichern.

(5) Bei jedem Ausfall einer Registrierkasse sind die Barumsätze auf anderen Registrierkassen zu erfassen. Sollte dies nicht möglich sein, sind die Barumsätze händisch zu erfassen und Zweitschriften der Belege aufzubewahren. Nach der Fehlerbehebung sind die Einzelumsätze anhand der aufbewahrten Zweitschriften nach zu erfassen und die Zweitschriften dieser Zahlungsbelege aufzubewahren (§ 132 BAO).

(6) Wenn nach dem Ausfall einer Registrierkasse ein neues Datenerfassungsprotokoll eingerichtet werden muss, ist als Signaturwert des vorhergehenden Barumsatzes (§ 10 Abs. 2 Z 7) der Signaturwert des zuletzt verfügbaren Barumsatzes bzw. der Signaturwert des Startbeleges im Datenerfassungsprotokoll zu verwenden. Das Ende des Ausfalles oder der Außerbetriebnahme ist über FinanzOnline

bekanntzugeben. Ist dem Unternehmer die Meldung über FinanzOnline mangels technischer Voraussetzungen unzumutbar, hat die Meldung unter Verwendung des amtlichen Vordrucks zu erfolgen.

(7) Ist eine Wiederinbetriebnahme der Signaturerstellungseinheit (Abs. 4) nicht mehr möglich, hat der Unternehmer eine neue Signaturerstellungseinheit zu beschaffen (§ 15), zu registrieren (§ 16) und eine neuerliche Inbetriebnahme der Sicherheitseinrichtung im Sinne der § 6 Abs. 1 bis 4 durchzuführen. Ist der zuletzt getätigte Barumsatz aus dem Datenerfassungsprotokoll feststellbar, entfällt die Inbetriebnahme der Sicherheitseinrichtung im Sinne der § 6 Abs. 1 bis 4 und gelten die Bestimmungen zum Sammelbeleg des Abs. 4. Während des Ausfalles händisch erfasste Barumsätze sind jedenfalls nachzuerfassen.

(8) Im Fall einer planmäßigen Außerbetriebnahme der Registrierkasse (Abs. 1 Z 3) hat der Unternehmer einen Schlussbeleg mit Betrag Null (0) zu erstellen. Der Schlussbeleg ist auszudrucken und gemäß § 132 BAO aufzubewahren.

Datenbank über Sicherheitseinrichtungen für die Registrierkassen

§ 18. (1) Der Bundesminister für Finanzen führt zur internen Dokumentation über die einem Unternehmer zugeordneten Signaturerstellungseinheiten eine Datenbank über Sicherheitseinrichtungen für die Registrierkassen.

(2) Diese enthält folgende Daten:

1. Name der Unternehmer
2. Ordnungsbegriff der Unternehmer
3. Art der Sicherheitseinrichtung
4. Seriennummern der Signaturzertifikate
5. Identifikationsnummern der Registrierkassen
6. Anzahl der an die Sicherheitseinrichtungen angeschlossenen Registrierkassen
7. Benutzerschlüssel für die Entschlüsselung der mit dem Verschlüsselungsalgorithmus AES 256 verschlüsselten Daten
8. Datum der Registrierung
9. Beginn und Ende von Ausfällen oder Außerbetriebnahmen der Sicherheitseinrichtungen
10. Betroffene Komponenten von Ausfällen oder Außerbetriebnahmen der Sicherheitseinrichtungen
11. Grund des Ausfalles oder der Außerbetriebnahme der Sicherheitseinrichtungen
12. Daten aus Kontrollen.

(3) Der Bundesminister für Finanzen ist datenschutzrechtlicher Auftraggeber im Sinne des § 4 Z 4 des Datenschutzgesetzes 2000 – DSG 2000, BGBl. I Nr. 165/1999, für die Datenbank über Sicherheitseinrichtungen für die Registrierkassen. Er hat dessen Einrichtung und Betrieb zu gewährleisten. Die Bundesrechenzentrum Gesellschaft mit beschränkter Haftung (BRZ GmbH) ist für die Datenbank über Sicherheitseinrichtungen für die Registrierkassen gesetzliche Dienstleisterin im Sinne der § 4 Z 5 und § 10 Abs. 2 DSG 2000.

Kontrolle und Prüfung der Datensicherheit für die Registrierkassen

§ 19. (1) Der Unternehmer hat auf Verlangen der Organe der Abgabenbehörde einen Barumsatz mit Betrag Null (0) zu erfassen und den dafür von der Registrierkasse ausgefertigten Beleg zu Kontrollzwecken zu übergeben. Bei Registrierkassen mit einer Vorrichtung zur elektronischen Übermittlung von Zahlungsbelegen ist der Beleg elektronisch zur Verfügung zu stellen.

(2) Auf Verlangen der Organe der Abgabenbehörde hat der Unternehmer das Datenerfassungsprotokoll für einen vom Organ der Abgabenbehörde vorgegebenen Zeitraum auf einen externen Datenträger zu exportieren und zu übergeben. Der Datenträger ist vom Unternehmer bereitzustellen.

4. Hauptstück Geschlossene Gesamtsysteme

Technische und organisatorische Anforderungen

§ 20. (1) Die Manipulationssicherheit in geschlossenen Gesamtsystemen gemäß § 131b Abs. 4 BAO ist durch eine Sicherheitseinrichtung zu gewährleisten, die aus einer Verkettung der Barumsätze mit Hilfe der aufbereiteten Daten nach § 9 Abs. 2 im Signaturformat laut Z 4 und 5 der Anlage besteht.

(2) Für geschlossene Gesamtsysteme gilt diese Verordnung mit Ausnahme der §§ 5 Abs. 2, 12, 15 und 17 Abs. 4. Die §§ 4 Abs. 1, 6 Abs. 4, 8 Abs. 2, 9, 16 Abs. 1 und 2, 17 Abs. 1 bis 3, 17 Abs. 7 und 18 sowie die Anlage sind mit der Maßgabe anzuwenden, dass weder eine Signaturerstellungseinheit noch ein Signaturzertifikat erforderlich sind und, dass einer Kassenidentifikationsnummer auch mehrere Registrierkassen mit einem gemeinsamen Datenerfassungsprotokoll zugeordnet werden dürfen. Absatz 4 bleibt hiervon unberührt.

(3) Bei geschlossenen Gesamtsystemen ist anstelle der Seriennummer des Signaturzertifikates (§ 9 Abs. 2 Z 6 und § 10 Abs. 2 Z 6) der Ordnungsbegriff des Unternehmers zu verwenden. Der Ordnungsbegriff des Unternehmers muss gegebenenfalls durch geeignete Zusätze (z.B.: Ziffern) ergänzt werden, um eindeutige Signaturprüfdaten zu ermöglichen. In der Datenbank gemäß § 18 sind anstelle der Seriennummer des Signaturzertifikates die Signaturprüfdaten zu erfassen. Der Ordnungsbegriff des Unternehmers sowie die Signaturprüfdaten müssen aus dem Gutachten gemäß § 21 hervorgehen.

(4) Antragsbefugt im Sinne § 131b Abs. 4 BAO sind nur Unternehmer, die ein geschlossenes Gesamtsystem als elektronisches Aufzeichnungssystem verwenden, das mit mehr als 30 Registrierkassen verbunden ist.

Sachverständige Begutachtung geschlossener Gesamtsysteme

§ 21. (1) Im Rahmen der Begutachtung geschlossener Gesamtsysteme sind insbesondere folgende Überprüfungen vorzunehmen:

1. das Vorliegen eines geschlossenen Gesamtsystems,
2. das Vorliegen der technischen und organisatorischen Voraussetzungen für die Manipulationssicherheit des geschlossenen Gesamtsystems.

(2) Im Gutachten sind insbesondere alle für den Betrieb der Sicherheitseinrichtung des geschlossenen Gesamtsystems gemäß § 20 Abs. 1 erforderlichen Softwarekomponenten anzugeben und Prüfberichte für diese Komponenten anzuschließen. Die Softwarekomponenten sind mit der mathematischen Hashfunktion Secure Hash Algorithm (SHA-256) mit einem Startwert, der Null (0000 0000 0000 0000) entspricht, für eine spätere Verifikation zu signieren. Aus den Prüfberichten muss nachvollziehbar hervorgehen, wie die einzelnen Komponenten geprüft wurden. Die Manipulationssicherheit und sicherheitstechnische Gleichwertigkeit mit einer Signaturerstellungseinheit sind zu bestätigen. Dem Gutachten sind ein Organigramm mit allen Hard- und Softwarekomponenten und Datenspeicher des geschlossenen Gesamtsystems sowie ein Überblick über die automatisch ablaufenden Verarbeitungsprozesse anzuschließen.

(3) Das Gutachten hat darüber hinaus Angaben darüber zu enthalten, welche organisatorischen Maßnahmen zur laufenden Überprüfung der Manipulationssicherheit vorgesehen sind. Dabei ist insbesondere darzulegen, welche betrieblichen Funktionen in der Organisationsstruktur des Unternehmens mit welchen Zugriffs- und Eingriffsrechten, die Veränderungen am Gesamtsystem herbeiführen können, ausgestattet sind, dass die Zugriffe protokolliert werden und durch welche Maßnahmen die Manipulationssicherheit des geschlossenen Systems laufend kontrolliert wird. Zudem ist darzulegen, wie im Falle eines Ausfalles des Systems die Einzelaufzeichnungspflicht, die Sicherung der Kassenumsätze und die Belegerteilung rechtskonform gewährleistet werden (Ausfallplan).

(4) Im Gutachten ist zu beurteilen, ob das geschlossene Gesamtsystem den Anforderungen des § 20 Abs. 1 und 2 entspricht und ob die technischen und organisatorischen Sicherungsmaßnahmen des Abs. 2 und 3 erfüllt werden.

(5) Verwenden mehrere Unternehmer, die durch ein vertikales Vertriebsbindungssystem oder durch ein Waren- oder Dienstleistungsfranchising wirtschaftlich verbunden oder die Teil eines Konzerns im Sinne des § 244 UGB sind, gemeinsam ein geschlossenes Gesamtsystem mit insgesamt mehr als 30 Registrierkassen und beurteilt das Gutachten die Manipulationssicherheit dieses Systems für diese Unternehmer, so kann dieses Gutachten von mehreren Unternehmern ihrem Antrag auf Erlassung eines Feststellungsbescheides zugrunde gelegt werden. Für alle Verwender des geschlossenen Gesamtsystems ist Abs. 3 sinngemäß anzuwenden. Lieferungen und sonstige Leistungen, die außerhalb des geschlossenen Gesamtsystems im betreffenden Betrieb erfolgen, sind von der Wirksamkeit des Feststellungsbescheides nicht umfasst.

(6) Mit der Erstellung solcher Gutachten dürfen nur gerichtlich beeidete Sachverständige beauftragt werden. Die Vollständigkeit der sicherheitsrelevanten Überprüfungen im Gutachten ist durch eine Bestätigungsstelle gemäß § 19 SigG zu bescheinigen.

(7) Die Kosten für die Erstellung der Gutachten trägt der Unternehmer.

Feststellungsbescheid

§ 22. (1) Im Feststellungsbescheid der Abgabenbehörde gemäß § 131b Abs. 4 BAO sind die dem Gutachten zugrunde liegenden Softwarekomponenten der Sicherheitseinrichtung gemäß § 20 Abs. 1 mit Hilfe der Softwaresignatur (§ 21 Abs. 2) zu identifizieren.

(2) Mit Feststellungsbescheid bestätigte geschlossene Gesamtsysteme werden in der Datenbank über Sicherheitseinrichtungen (§ 18) registriert.

(3) Kann die Manipulationssicherheit des geschlossenen Gesamtsystems durch das Finanzamt nicht bestätigt werden, ist dem Unternehmer eine einmalige Nachfrist von einem Monat für die Nachholung der die Manipulationssicherheit gewährleistenden Maßnahmen unter Beibringung eines diese Maßnahmen bestätigenden Gutachtens einzuräumen. Das Finanzamt hat diesfalls unter Zugrundelegung des vorliegenden Sachverhaltes zu entscheiden.

(4) Wird die Manipulationssicherheit des geschlossenen Gesamtsystems mit rechtskräftigem Bescheid des Finanzamtes nicht bestätigt, hat der Unternehmer innerhalb von drei Monaten ab Eintritt der Rechtskraft die Manipulationssicherheit unter Verwendung einer Signaturerstellungseinheit (§ 131b Abs. 2 BAO) herbeizuführen, andernfalls mit Ablauf dieser Frist die Verpflichtungen nach § 131b Abs. 2 BAO als nicht erfüllt gelten.

Änderung der tatsächlichen Verhältnisse

§ 23. (1) Änderungen des mit Bescheid bestätigten geschlossenen Gesamtsystems sind vor ihrer Durchführung dem für die Erhebung der Umsatzsteuer zuständigen Finanzamt unter Vorlage eines neuen Gutachtens (§ 21) zu melden, wenn eine umfassende Umstellung des geschlossenen Gesamtsystems (z. B.: Technologiewechsel) oder eine Änderung der Softwarekomponenten der Sicherheitseinrichtung gemäß § 20 Abs. 1 geplant ist oder die Antragsvoraussetzungen im Sinne § 20 Abs. 4 oder 21 Abs. 5 nicht mehr vorliegen. Über solche Änderungen des geschlossenen Gesamtsystems ist mit Feststellungsbescheid abzusprechen.

(2) Die Meldung dieser beabsichtigten Änderungen hat über FinanzOnline zu erfolgen.

(3) Werden dem Unternehmer nach Erlassung des Feststellungsbescheides Tatsachen bekannt, die Zweifel an der Manipulationssicherheit des geschlossenen Gesamtsystems hervorrufen, hat er diese ohne unnötigen Aufschub über FinanzOnline zu melden.

Kontrolle der Identität der Softwarekomponente laut § 21 Abs. 2

§ 24. Die Organe der Abgabenbehörde sind berechtigt, die Übereinstimmung der im Gutachten ausgewiesenen Softwarekomponente laut § 21 Abs. 2 mit der im geschlossenen Gesamtsystem im Einsatz befindlichen Softwarekomponente zu überprüfen. Dazu muss das geschlossene Gesamtsystem eine Eingabemöglichkeit eines Startwertes zur lokalen Abfrage der Softwaresignaturwertes zur Verfügung stellen sowie den Softwaresignaturwert der Komponente berechnen und anzeigen.

5. Hauptstück Schlussbestimmungen

Inkrafttreten

§ 25. (1) Die Verordnung tritt mit 1. Jänner 2017 in Kraft.

(2) Abweichend von Abs. 1 treten § 1 bis 3, § 5 Abs. 1, § 7 Abs. 1, § 17 Abs. 5 und § 19 Abs. 2 mit 1. Jänner 2016 in Kraft.

(3) Abweichend von Abs. 1 und 2 treten die § 6, § 15, § 16, § 18, § 21 und § 22 mit 1. Juli 2016 in Kraft.

(4) Diese Verordnung wurde gemäß der Richtlinie 98/34/EG über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft, ABl. Nr. L 204 vom 21.07.1998 S. 37, zuletzt geändert durch die Verordnung (EU) Nr. 1025/2012 zur europäischen Normung, zur Änderung der Richtlinien 89/686/EWG und 93/15/EWG sowie der Richtlinien 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG und 2009/105/EG und zur Aufhebung des Beschlusses 87/95/EWG und des Beschlusses Nr. 1673/2006/EG, ABl. Nr. L 316 vom 14.11.2012 S. 12, bei der Europäischen Kommission unter der Notifikationsnummer **XXX** notifiziert.