



Elektronischer Geschäftsverkehr

Verordnung des EFD
über elektronisch übermittelte Daten und Informationen
(EIDI-V)
vom 30. Januar 2002

Kommentar

01.07.2002

Kommentar zur Verordnung des EFD über elektronisch übermittelte Daten und Informationen

Einleitende Bemerkungen

Bei der zu kommentierenden Ausführungsverordnung des EFD handelt es sich um die **Detail**-Vorschriften, nach welchen die Umsetzung der in der MWSTGV festgehaltenen Grundsätze betreffend Übermittlung und Aufbewahrung elektronischer Daten zu erfolgen hat. Diese auch zahlreiche Einzelheiten regelnden Vorschriften werden es der Wirtschaft erlauben, weitgehend ohne, jedenfalls aber mit zumutbaren Ungewissheiten bezüglich der mehrwertsteuerlichen Konsequenzen zum elektronischen Datenaustausch und zur ebensolchen Datenaufbewahrung überzugehen. Deren umfassende Regelung, namentlich auch das Erfordernis einer ausreichend abgesicherten digitalen Signatur, liegt somit nicht nur im Interesse der Steuerverwaltung, sondern genau so in demjenigen der Wirtschaftsbeteiligten. Denn es dürfte klar sein, dass die Sicherheit der elektronischen Übermittlung von Rechnungen so oder so gewährleistet sein muss. Zudem trägt die Formulierung gewisser Anforderungen an die Sicherheit dazu bei, Missbräuchen vorzubeugen, was für die weitere Entwicklung des elektronischen Datenaustausches und der elektronischen Datenaufbewahrung mit Bestimmtheit nur förderlich sein kann.

Sodann ist zu unterstreichen, dass wichtige Anliegen der Wirtschaft im Zusammenhang mit der mehrwertsteuerlichen Regelung der elektronischen Datenübermittlung bei der Erarbeitung der Ausführungsverordnung gebührend berücksichtigt werden. Ausdrücklich erwähnt seien vor allem die Zulassung der sog. Delegation und die doppelte Datenfernübertragung.

Ferner kann die vorliegende Verordnung des EFD Eurokompatibilität beanspruchen. Gemäss einer kürzlich erfolgten Änderung der entsprechenden EG-Richtlinie wird in den Mitgliedländern der EU die Gewährleistung der Authentizität und Integrität elektronisch übermittelter Rechnungen ebenfalls mittels elektronischer Signatur sichergestellt. Aufgrund einer diesbezüglichen Änderung sieht das deutsche Umsatzsteuergesetz beispielsweise vor, dass ab 1.1.2002 auch eine mit einer digitalen Signatur nach deutschem Signaturgesetz versehene (vergleichbar mit der vom EFD verlangten digitalen Signatur) elektronische Abrechnung als Rechnung gilt. Am Rande sei noch bemerkt, dass die EU-Staaten bezüglich der elektronischen Aufbewahrung von Daten zusätzliche Anforderungen stellen können, wenn die Aufbewahrung in einem Land erfolgt, mit dem keine dem einschlägigen Instrumentarium der Gemeinschaft entsprechende Vereinbarung über die gegenseitige Unterstützung besteht. In der Schweiz wird dagegen bloss verlangt, dass, wo immer im Ausland Daten aufbewahrt

werden, deren Zugriff, deren Lesbarmachung und deren Auswertung trotzdem jederzeit gewährleistet bleiben.

Schliesslich sei noch darauf hingewiesen, dass die Mitgliedländer der EU die Möglichkeit haben, die Anerkennung elektronisch übermittelter Rechnungen für MWST-Zwecke aus Ländern, mit denen keine entsprechende Amtshilfevereinbarung besteht, von der Erfüllung zusätzlicher Anforderungen abhängig zu machen. Würden für den elektronischen Datenaustausch mehrwertsteuerlich weniger strenge Anforderungen gestellt als dies in der EU der Fall ist, könnte dies für die ausgesprochen exportorientierte Schweizer Wirtschaft mit Nachteilen verbunden sein. Letztere muss deshalb grösstes Interesse daran haben, dass ihre ausländischen Kunden elektronisch übermittelte Daten (insbesondere Rechnungen) erhalten, die den international geltenden Standards - vor allem jenen der EU - entsprechen.

Art. 1 Gegenstand und Zweck

Artikel 1 umschreibt, was die vorliegende Ausführungsverordnung zu regeln hat, nämlich die Festlegung der technischen, organisatorischen und verfahrenstechnischen Anforderungen an die Beweiskraft sowie die Kontrolle elektronisch oder in vergleichbarer Weise übermittelter und aufbewahrter Daten und Informationen (elektronische Daten) nach den Bestimmungen der Artikel 43 und 44 der MWSTGV. Das heisst, sie hat insbesondere festzulegen, welche Voraussetzungen elektronisch übermittelte und aufbewahrte Daten erfüllen müssen, damit ihnen die Eidg. Steuerverwaltung (ESTV) anlässlich von Kontrollen hinsichtlich Vorsteuerabzug, Steuererhebung oder Steuerbezug die gleiche Beweiskraft zuerkennt wie Daten und Informationen, die ohne Hilfsmittel lesbar sind.

Zweck dieses Rechtserlasses ist somit nicht etwa zu versuchen, mittels entsprechender Bestimmungen sicherzustellen, dass elektronisch oder in vergleichbarer Weise übermittelte und aufbewahrte Daten und Informationen nicht manipuliert oder verfälscht werden können. Eine wirksame Verhinderung von Manipulationen oder Verfälschungen ist im Bereich der elektronisch übermittelten und aufbewahrten Daten und Informationen genau so wenig möglich wie bei auf Papier festgehaltenen Texten und Zahlen. Mittels Erlass entsprechender Rechtsvorschriften kann bloss die Feststellung von Verletzungen der Voraussetzungen sichergestellt werden, denen elektronisch oder in vergleichbarer Weise übermittelte Daten und Informationen genügen müssen, um die gleiche Beweiskraft zu haben wie Daten und Informationen, die ohne Hilfsmittel lesbar sind.

Der Klammervermerk „elektronische Daten“ erlaubt es, die Umschreibung des Gegenstandes nicht immer im vollen Wortlaut wiedergeben zu müssen. Sodann ist darauf hinzuweisen, dass das Bindewort „und“ in der Wendung „übermittelte und aufbewahrte Daten“ nicht kumulativ zu verstehen ist. Die Bestimmungen der vorliegenden Verordnung gelten somit nicht nur für elektronisch aufbewahrte Daten, die ein Steuerpflichtiger übermittelt erhalten hat, sondern ebenso für durch den letzterwähnten elektronisch aufbewahrte Daten, die er auf die nämliche Art selbst generiert hat. Das Scanning von Dokumenten in Papierform beispielsweise stellt somit keine Generierung von elektronischen Daten im Sinne der vorliegenden Verordnung dar und fällt deshalb auch nicht unter die durch diesen Rechtserlass zu regelnden Sachverhalte.

Art. 2 Begriffe

In diesem Artikel geht es darum, einige in den nachfolgenden Artikeln verwendete Begriffe näher zu definieren, deren Sinnbedeutung nicht ohne weiteres eindeutig ist.

Absatz 1 macht deutlich, dass Prüfungen der elektronisch oder in vergleichbarer Weise geführten Geschäftsbücher, Geschäftskorrespondenz und Buchungsbelege nicht wie bisher schon aus rein praktischen Gründen (Transport einer grossen Anzahl von Papierbelegen) ausschliesslich am Geschäftssitz der Steuerpflichtigen zu erfolgen brauchen. Dank der mit geringem Aufwand transportierbaren Daten und Informationen, können Prüfungen von elektronisch aufbewahrten Belegen etc. ebenso gut in den Räumlichkeiten der ESTV durchgeführt werden, wie dies am Geschäftssitz der Steuerpflichtigen der Fall ist. Zu denken ist an die Möglichkeit der Prüfung von Daten, die der ESTV auf ihr Verlangen durch die Steuerpflichtigen zu diesem Zweck (Prüfung in den Räumlichkeiten der ESTV) auf maschinell verwertbaren Datenträgern überlassen werden. Falls es die Steuerpflichtigen vorziehen, können der ESTV durch diese letztere zu Prüfungszwecken einverlangte Daten, anstatt durch die Abgabe von maschinell auswertbaren Datenträgern jedoch auch ohne weiteres on-line zugänglich gemacht werden.

Es versteht sich von selbst, dass es der ESTV nicht zusteht, sei es mittels maschinell auswertbarer Datenträgern oder on-line, Einsicht in alle durch die Steuerpflichtigen gespeicherten Daten zu nehmen. Dies trifft selbstverständlich nur auf für die Steuererhebung relevante Daten und Informationen zu. Sofern einem Steuerpflichtigen die Eingrenzung des direkten (on-line) Datenzugriffs durch die ESTV lediglich auf die für die Steuererhebung relevanten Daten nicht zumutbar ist, besteht ohne weiteres die Möglichkeit, eine solche Eingrenzung

mittels Abgabe der betreffenden Daten auf maschinell verwertbaren Datenträgern zu erreichen. Ebenso versteht es sich von selbst, dass es voll und ganz in der Kompetenz der ESTV steht zu bestimmen, welche Daten und Informationen für die Steuererhebung als relevant zu betrachten sind und in welche eine Einsichtnahme unterbleiben kann.

Absatz 2 besagt, was in dieser Verordnung unter einer digitalen Signatur verstanden wird. Andere „digitale Signaturen“, welche den im vorliegenden Absatz verlangten Voraussetzungen nicht entsprechen, werden somit zum vorneherein als nicht ausreichende Absicherung für die elektronische Übertragung und Aufbewahrung von Daten betrachtet. Beim Fehlen einer in diesem Absatz umschriebenen Eigenschaft, die eine digitale Signatur aufweisen muss, erübrigt sich deshalb eine Prüfung der weiteren Anforderungen gemäss Artikel 3: auch deren ausnahmslose Erfüllung könnte das Fehlen einer der in diesem Absatz umschriebenen Eigenschaften nicht wett machen.

Sobald das Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (ZertES) in Kraft gesetzt sein wird, werden an Stelle der in der ZertDV aufgeführten Bestimmungen für die Ausgabe von Zertifikaten und die Anerkennung von Zertifizierungsdiensteanbietern die entsprechenden Voraussetzungen des Bundesgesetzes massgebend sein.

Art. 3 Beweiskraft

Absatz 1 nennt die Bedingungen, die erfüllt sein müssen, damit die in Artikel 43 Absatz 1 der MWSTGV verlangten Voraussetzungen, nämlich Nachweis des Ursprungs, Nachweis der Integrität und Nichtabstreitbarkeit von Versand und Empfang für die Beweiskraft elektronisch übermittelter und aufbewahrter Daten und Informationen als gegeben betrachtet werden können. Es sind dies:

- a. Die Absicherung der elektronischen Übermittlung und Aufbewahrung von Daten mittels digitaler Signatur und zwar einer digitalen Signatur, wie sie in Artikel 2 Absatz 2 definiert wird. Mit dieser Bestimmung wird deutlich gemacht, dass hinsichtlich der elektronischen Übermittlung und Aufbewahrung von Daten für die Belange der Mehrwertsteuer im wesentlichen keine weitergehende Absicherung verlangt wird, damit ihnen die gleiche Beweiskraft zuerkannt wird wie ohne Hilfsmittel lesbaren, als dies auch im allgemeinen Geschäftsverkehr der Fall ist (vgl. Artikel 15a OR). Obschon auch eine qualifizierte digitale Signatur, wie sie die zur Diskussion stehende darstellt, keine hundertprozentige Sicherheit bietet – zu denken ist vor allem an das Erschleichen eines Zertifikats mit gefälschtem

Pass etc. –, würden sich weitergehende Anforderungen, als sie die betreffenden handelsrechtlichen Bestimmungen vorsehen, im Interesse der Rechtssicherheit kaum rechtfertigen lassen.

- b. Die Gültigkeit des durch einen Zertifizierungsdiensteanbieter gemäss den Bestimmungen von Artikel 2 Absatz 2 ausgestellten Zertifikats im Zeitpunkt der Signaturerstellung. Massgebend für die Prüfung der Gültigkeit eines Zertifikats im Zeitpunkt seiner Verwendung sind die durch die Anbieter von Zertifizierungsdiensten gemäss Artikel 12 ZertDV zu führenden Listen für ungültig erklärte oder suspendierte Zertifikate.
- c. Die Prüfung mittels Verifikation der digitalen Signatur auf Integrität, Authentizität und Signaturberechtigung sowie die Dokumentation des Ergebnisses. Digital signierte Daten können mit dem öffentlichen Schlüssel verifiziert werden. Die Integritätsprüfung bildet den Ausgangspunkt der weiteren Prüfung der Authentizität und Signaturberechtigung. Unterbleiben diese Prüfungen ist offen, ob die Daten die verlangten Voraussetzungen zu erfüllen vermögen. Dank der Dokumentationspflicht und der Festsetzung des Zeitpunktes der Verifikation besteht vor der Verwendung Klarheit darüber, ob die Daten die gestellten Anforderungen erfüllen. Ergeben die Prüfungen ein negatives Ergebnis, so sind die Bedingungen grundsätzlich nicht erfüllt, die an Daten gestellt werden, die den Leistungsempfänger zum Vorsteuerabzug berechtigen.

Die Signaturprüfung ist Bestandteil der Verifikation. Während des Signaturprüfungsvorgangs ist mit hinreichender Sicherheit zu gewährleisten, dass

- a) die zur Überprüfung der Signatur verwendeten Daten den Daten entsprechen, die dem Überprüfer angezeigt werden,
- b) die Signatur zuverlässig überprüft wird und das Ergebnis dieser Überprüfung korrekt angezeigt wird,
- c) der Überprüfer bei Bedarf den Inhalt der unterzeichneten Daten zuverlässig feststellen kann,
- d) die Echtheit und die Gültigkeit des zum Zeitpunkt der Überprüfung der Signatur verlangten Zertifikats zuverlässig überprüft werden,
- e) das Ergebnis der Überprüfung sowie die Identität des Unterzeichners korrekt angezeigt werden,
- f) die Nichtverwendung von Pseudonymen klar ersichtlich ist, und
- g) sicherheitsrelevante Veränderungen erkannt werden können.

Die für die Signaturprüfung notwendigen Daten, öffentlicher Schlüssel aus dem Zertifikat sowie die zu überprüfenden Daten, müssen der Signaturanwendungskomponente als Parameter übergeben werden können. Die Berechnung des Hashwertes und der Verifizieralgorithmus müssen nachweislich so implementiert sein, dass eine grösstmögliche Interoperabilität sichergestellt ist.

- d. Die Aufbewahrung des zur Überprüfung der digitalen Signatur notwendigen öffentlichen Schlüssels – ob mitgesandt oder nicht – und des durch einen anerkannten Anbieter von Zertifizierungsdiensten ausgestellten Zertifikats gemäss Buchstabe b., sofern letzteres nicht veröffentlicht wurde, mit den abgesicherten Daten. Mit dieser Bestimmung soll sichergestellt werden, dass die Hilfsmittel, welche für eine Überprüfung der Erfüllung der Voraussetzungen für die Beweiskraft der aufbewahrten Daten erforderlich sind, in jedem Fall zur Verfügung stehen.
- e. Die Aufbewahrung der Schlüssel zur Entschlüsselung verschlüsselter Daten bei Einsatz von Kryptographietechniken. Mit dieser Bestimmung soll vermieden werden, dass für die Steuererhebung relevante Daten in der Folge nicht mehr verfügbar sind, weil sie nicht mehr lesbar gemacht werden können.
- f. Keine Verwendung von Pseudonymen. Mit dieser Anordnung soll erreicht werden, dass die Identität der Zertifikateinhaber direkt feststellbar ist und nicht erst seitens des Zertifizierungsdiensteanbieters erfragt werden muss
- g. Die unzweifelhafte Sicherheit der Schlüssel im Zeitpunkt ihrer Verwendung. In Anbetracht der ständigen Weiterentwicklung der Computertechnik wird darauf verzichtet, eine gewisse Bitlänge der Schlüssel zu verlangen, um diese als unzweifelhaft sicher zu betrachten. Die ESTV geht davon aus, dass das Knacken einer bestimmten Bitlänge in der Tagespresse oder zumindest in der Fachliteratur sofort publik gemacht wird. Somit wird es ihr auch möglich sein, den Steuerpflichtigen innerhalb nützlicher Frist in angemessener Weise bekannt zu geben, bis zu welchem Datum eine spezifische Bitlänge bezüglich der Beweiskraft für die Steuererhebung relevanter Daten als unzweifelhaft sicher akzeptiert wird. Ohne eine solche Bekanntgabe des Verlusts der Sicherheit eines spezifischen Schlüssels durch die ESTV dürfen die Steuerpflichtigen davon ausgehen, dass derselbe als unzweifelhaft sicher angesehen werden darf.

Absatz 2 bestimmt, dass in gewissen Fällen elektronisch übermittelte Daten einer durch digitale Signatur abgesicherte Empfangsbestätigung durch deren Adressaten bedürfen. Einerseits ist dies der Fall, wenn der Leistungsempfänger bei der Fakturierung an Stelle des

nerseits ist dies der Fall, wenn der Leistungsempfänger bei der Fakturierung an Stelle des Leistungserbringers handelt, etwa weil der Leistungsempfänger eine sog. **Ab**-Rechnung über die empfangenen Leistungen erstellt, anstatt dass sie ihm vom Leistungserbringer in Rechnung gestellt werden oder er an Stelle des Leistungserbringers in dessen Namen und für dessen Rechnung die Fakturierung vornimmt (self-billing). Diese Anforderung ersetzt das bei Rechnungsstellung durch den Leistungserbringer sonst automatisch stattfindende „Cross-checking“ (Interessengegensatz zwischen Leistungserbringer und Leistungsempfänger bezüglich Rechnungsbetrag; für den ersten Berechnungsgrundlage der Steuer auf dem Umsatz, für den zweiten Berechnungsgrundlage des Vorsteuerabzugs).

Absatz 3 verlangt, dass eine solche Empfangsbestätigung ebenfalls vorliegt, wenn der Nachweis, dass der Leistungsempfänger seinen Wohn- oder Geschäftssitz im Ausland hat, einzig mit Hilfe elektronisch übermittelter Daten erbracht werden soll. Auch hier geht es darum, anlässlich von Kontrollen nicht nur auf Daten abstellen zu müssen, die durch den Steuerpflichtigen selbst generiert, sondern ebenfalls auf Informationen abstellen zu können, welche auf ausreichend abgesicherte Art und Weise durch die andere Partei des Leistungsaustauschverhältnisses übermittelt wurden. Bei der Auslegung, was als eine den Anforderungen von Artikel 3 Absatz 2 genügende Empfangsbestätigung gilt, wird sich die ESTV an den Normen orientieren, die gegenwärtig im Sub-Group on e-commerce des WP 9 der OECD zur rechtsgenügenden Festlegung des Status und der Jurisdiktion der Internet-Auftraggeber erarbeitet werden. In Anbetracht der Tatsache, dass es sich bei der Mehrzahl der im hiervor erwähnten Gremium der OECD vertretenen Ländern um Mitglied-Staaten der EU handelt, wird mit diesem Vorgehen ebenfalls sichergestellt, dass allfällige Unvereinbarkeiten mit den entsprechenden Regelungen in der EU vermieden werden.

Art. 4 Datensicherheit

Absatz 1 hält fest, dass bei elektronischer Führung der Buchhaltung die für eine „Ordnungsgemässe Buchführung“ geltenden Grundsätze genau so massgebend sind, wie dies bei einer auf konventionelle Art geführten Buchhaltung der Fall ist. Dies bedeutet, dass das verwendete Datenverarbeitungsverfahren Gewähr für eine fortlaufende, chronologische sowie lückenlose und systematische Erfassung sämtlicher Geschäftsvorfälle bieten muss. Ebenso muss es in der Lage sein sicherzustellen, dass Daten bezüglich der Verbuchung von Geschäftsvorfällen nicht unbemerkt verändert werden können. Dies bedeutet, dass deren ursprünglicher Inhalt, d.h. derjenige vor der Vornahme einer allfälligen Veränderung nicht mehr feststellbar ist; aber auch dass bei Vornahme von Veränderungen festgestellt werden kann,

wann diese letzteren erfolgt sind (ursprünglich oder erst später). Des weiteren muss hard- und softwaremässig gewährleistet sein, dass bei der blossen Übertragung von originären Daten auf ein Speichermedium keine Bearbeitung derselben möglich ist, ohne dass dies bei entsprechender Überprüfung nachträglich festgestellt werden kann.

Absatz 2 nennt die Voraussetzungen, denen die Sicherheitsvorkehrungen und -massnahmen zum Schutze der Datenbestände und Datenverarbeitungssysteme eines Steuerpflichtigen genügen müssen, um als ausreichend betrachtet werden zu können. Da zur Gewährleistung der Sicherheit der für die Steuererhebung relevanten Daten und Informationen während der Dauer der Aufbewahrungsfrist nicht nur die Verfügbarkeit der Daten und der Software, sondern auch der Hardware gehört, muss das Datensicherungskonzept auch die Sicherung der technischen Installationen (Hardware, Leitungen, Räume etc.) umfassen. Das soeben erwähnte Sicherungskonzept ist sowohl bezüglich des Verfahrens wie auch der Prozeduren der Datensicherung zu dokumentieren.

Zum Schutz der Datenbestände und Datenverarbeitungssysteme gegen unberechtigte Veränderungen haben die Steuerpflichtigen die hierzu erforderlichen Zugriffs- bzw. Zugangskontrollen vorzusehen. Zu denken ist insbesondere an Einschränkungen des Zugriffs auf Daten und Programme entsprechend dem Aufgabenbereich der grundsätzlich zugriffsberechtigten Personen. Zudem sind zu den Räumen, in denen die Datenbestände und Datenverarbeitungsprogramme aufbewahrt werden, Zugangskontrollen zu errichten. Diese müssen aber auch für Räumlichkeiten gelten, in welchen sich ausgelagerte Datenträger der Datensicherung befinden.

Zwecks Bewahrung der Datenbestände und Datenverarbeitungssysteme vor Verlust sind die Steuerpflichtigen gehalten, periodisch Datensicherungsprozeduren zu den für die Steuer relevanten Daten und Informationen durchzuführen. Auch ist es angezeigt, zu den aufbewahrungspflichtigen Datenbeständen und Datenverarbeitungssysteme zusätzliche Sicherungskopien zu erstellen und an einem anderen Standort (anderer Sicherheitsbereich) aufzubewahren. Nebst den soeben aufgeführten Massnahmen zum Schutz vor Verlust von Daten und Programmen als solchem darf aber auch die Gefahr des Verlusts der Lesbarkeit gespeicherter Daten mittels der zu einem gegebenen Zeitpunkt verfügbaren Textverarbeitungssysteme nicht vergessen werden. Die Erfüllung der Pflicht zur Vermeidung derartiger Datenverluste kann durch den Steuerpflichtigen insbesondere mittels der nachfolgend aufgeführten Massnahmen wahrgenommen werden:

- Das periodische Umkopieren der Daten auf neue Datenträger.
- Die periodische Konvertierung oder Migration, d.h. die Übertragung der Daten in ein neues Datenformat.
- Die Emulation, d.h. die Erhaltung der zum Lesen der Daten benötigten Systeme indem man diese letzteren auf neueren Systemen künstlich nachbaut.
- Die Speicherung der Daten in einem Format, das auf allgemein anerkannten Standards und öffentlich zugänglichen Spezifikationen basiert wie z.B. das Format XML (Extensible Markup Language).

Das Risiko der Unauffindbarkeit muss durch das Führen eines systematischen Verzeichnisses über die gespeicherten Datenbestände und Datenverarbeitungssysteme möglichst ganz vermieden oder zumindest stark reduziert werden. Das fragliche Verzeichnis hat dafür Gewähr zu bieten, dass der Standort der einzelnen Datenträger, deren Inhalt, das Datum der Sicherung sowie das früheste Datum des Löschens des Datenträgerinhalts ohne weiteres ersichtlich sind.

Um das Risiko der Vernichtung oder des Diebstahls der Datenträger rechtsgenügend auszuschliessen oder zu vermindern, sind diese letzterwähnten in gegen Einbruch, Feuer, Feuchtigkeit, Magnetfelder etc. genügend gesicherten Räumen bzw. Tresoren aufzubewahren.

Art. 5 Prüfbarkeit

Absatz 1 verlangt von den Steuerpflichtigen, dass sie für ein von ihnen betriebenes, für die Steuererhebung relevante Daten enthaltendes Datenverarbeitungssystem eine Verfahrensdokumentation erstellen. Diese letztere muss es einem buchführungskundigen Dritten erlauben, die Funktionsweise eines solchen Datenverarbeitungssystems unter angemessenem Zeitaufwand ausreichend zu begreifen, um die darin enthaltenen Daten hinsichtlich ihrer formellen und sachlichen Richtigkeit innerhalb nützlicher Frist prüfen zu können. Diese Anforderung im Falle z.B. des Buchführungssystems bezieht sich sowohl auf die Prüfbarkeit einzelner Geschäftsvorfälle als auch auf die Prüfbarkeit des Abrechnungsverfahrens als Ganzes. Des weiteren muss sich aus der fraglichen Dokumentation ergeben, dass das Verfahren auch effektiv entsprechend seiner Beschreibung durchgeführt worden ist. Wie die verlangte

Verfahrensdokumentation formal gestaltet und technisch geführt oder durch wen sie erstellt wird, bleibt den Steuerpflichtigen überlassen, solange die gewählte formale Ausgestaltung und technische Führung für einen buchführungskundigen Dritten ohne weiteres verständlich sind. Der Umfang der Verfahrensdokumentation schliesslich, der erforderlich ist, um den hievon umschriebenen Ansprüchen zu genügen, richtet sich nach der Komplexität des Datenverarbeitungssystems (z.B. Anzahl und Grösse der Programme, Struktur ihrer Verbindungen untereinander etc.).

Auch bei fremderworbener Software, bei der die Verfahrensdokumentation vom Software-Ersteller angefertigt wird, liegt die Verantwortung für deren Vollständigkeit und für deren Informationsgehalt beim Steuerpflichtigen. Dies trifft ebenso für die Teile der Verfahrensdokumentation zu, die ihm durch den Software-Ersteller nicht ausgehändigt worden sind, weshalb der Steuerpflichtige bei Bedarf auch dazu angehalten werden kann, der Eidg. Steuerverwaltung zu ermöglichen, Einsicht in diese Teile der Verfahrensdokumentation zu nehmen.

Die Verfahrensdokumentation muss mindestens folgende Elemente beinhalten, wobei die Beschreibung eines jeden der nachgenannten Bereiche den Umfang und die Wirkungsweise des internen Kontrollsystems erkennbar machen muss:

- Eine Beschreibung der sachlogischen Lösung.

Die sachlogische Beschreibung muss die Darstellung der fachlichen Aufgabe aus der Sicht des Anwenders enthalten, welche folgende Punkte umfassen sollte: eine generelle Aufgabenstellung, eine Beschreibung der Datenbestände, der Verarbeitungsregeln, des Datenaustauschs, der maschinellen und manuellen Kontrollen, der Fehlermeldungen sowie die Schlüsselverzeichnisse und Schnittstellen zu anderen Systemen.

- Eine Beschreibung der programmtechnischen Lösung.

Die Beschreibung der programmtechnischen Lösung hat zu zeigen, wo und wie die sachlogischen Forderungen in Programmen umgesetzt sind. Tabellen, über welche die Funktionen der Programme beeinflusst werden können, sind wie Programme zu behandeln.

Programmänderungen sind in der Verfahrensdokumentation unbedingt auszuweisen. Soweit die Programmänderungen nicht automatisch dokumentiert werden, muss durch zusätzliche organisatorische Massnahmen sichergestellt werden, dass Alt- und Neuzustand eines geänderten Programms nachweisbar sind. Änderungen von Tabellen mit Programmfunktion sind in der Weise zu dokumentieren, dass für die Dauer der Aufbewahrungsfrist der jeweilige Inhalt einer Tabelle festgestellt werden kann.

- Eine Beschreibung, wie die Programm-Identität gewährt wird.

In der Beschreibung, wie die Programmidentität gewährt wird, hat der Steuerpflichtige nachzuweisen, dass die sachlogischen Forderungen durch die eingesetzten Programme erbracht werden bzw. erbracht worden sind. Hierzu gehören die präzise Beschreibung des Freigabeverfahrens mit Regelungen bezüglich der Freigabekompetenzen, die durchzuführenden Testläufe und die dabei zu verwendenden Daten sowie Anweisungen für Programmeinsatzkontrollen. Somit gehört zum Nachweis der Programmidentität im wesentlichen die Freigabeerklärung in Verbindung mit vorhandenen Testdatenbeständen. Aus der Freigabeerklärung muss sich auch ergeben, welche Programmversion ab welchem Zeitpunkt für den produktiven Einsatz vorgesehen ist.

- Eine Beschreibung, wie die Integrität von Daten gewahrt wird.

Zur Wahrung der Datenintegrität sind alle Vorkehrungen zu beschreiben, durch welche erreicht wird, dass Daten und Programme nicht von Unbefugten geändert werden können. Hierzu gehören neben der Beschreibung des Zugriffsberechtigungsverfahrens der Nachweis der sachgerechten Vergabe von Zugriffsberechtigungen.

- Arbeitsanweisungen für den Anwender.

Schliesslich gehören zur Verfahrensdokumentation ebenfalls die schriftlich festgehaltenen Arbeitsanweisungen, die für den Anwender zur sachgerechten Erledigung und Durchführung seiner Aufgaben unabdingbar vorhanden sein müssen. Es ist dies insbesondere die Beschreibung der im Verfahren vorgesehenen manuellen Kontrollen und Abstimmungen, wobei auch die Schnittstellen zu vor- und nachgelagerten Systemen gebührend zu berücksichtigen sind.

Die Verfahrensdokumentation darf nebst den Landessprachen Deutsch, Französisch und Italienisch auch in Englisch abgefasst sein.

Absatz 2 hält fest, dass es unerlässlich ist, alle Stammdaten zu dokumentieren und insbesondere sämtliche Änderungen derselben lückenlos festzuhalten und zu kommentieren (z.B. die Änderung des Steuersatzes für eine bestimmte Kategorie von Leistungen zufolge der Optierung für deren Besteuerung). Ebenso darf es nicht möglich sein, dass beispielsweise Lieferantenstammdaten vorübergehend verändert und wieder zurückverändert werden können, ohne dass dies bei entsprechenden Kontrollen ersichtlich wäre (z.B. Bankverbindung eines Mitarbeiters an Stelle derjenigen des Lieferanten, nach erfolgter Zahlung wieder zurück zur alten Bankverbindung). Das gleiche gilt für alle Steuer- und auch andere Tabellen, die

einen Wertefluss begründen oder erklären, wie dies etwa für Tabelleneinstellungen der Fall ist, welche die automatisierten Buchungen für Umsatzsteuerzwecke bestimmen.

Sodann wird erstmals verlangt, wie dies in den nachfolgenden Verordnungsbestimmungen noch mehrmals der Fall sein wird, dass die Steuerpflichtigen für die Steuererhebung relevante Daten und Informationen in elektronischer oder vergleichbarer Weise so aufbewahren, dass diese während der Aufbewahrungsfrist verfügbar bleiben und ohne unzumutbare zeitliche Verzögerung lesbar gemacht werden können. Von den Steuerpflichtigen wird somit verlangt, dass sie bei der Konzipierung der Aufbewahrung von elektronischen Daten darauf achten, dass die Daten nicht nur auf für sie zweckdienliche Art und Weise jederzeit verfügbar und unverzüglich lesbar sind, sondern die Speicherung von Daten auch unter Berücksichtigung der Abrufbedürfnisse der ESTV in der hievor umschriebenen Art und Weise erfolgt. Andernfalls haben die Steuerpflichtigen die seitens der ESTV anlässlich von Kontrollen verlangten Daten zu ihren Lasten so aufzubereiten, dass der Zeitbedarf für deren Prüfung nicht höher ausfällt, als dies bei einer den Anforderungen der vorliegenden Bestimmung genügenden Aufbewahrung der Fall wäre.

Absatz 3 schränkt die Verwendung von Schlüsselzahlen und Codes ausschliesslich auf Artikelbezeichnungen ein. Auch bei dieser eingeschränkten Anwendung wird sodann verlangt, dass die Bedeutung einer bestimmten Schlüsselzahl oder eines bestimmten Codes sowohl beim Absender als auch beim Empfänger der entsprechenden Daten aufgrund einer lückenlosen Dokumentation und einer genauen Kommentierung eindeutig festgestellt werden kann. Sofern ein gewisser Codes zu verschiedenen Zeitperioden eine unterschiedliche Bedeutung besitzt, muss dies aus der entsprechenden Dokumentation unmissverständlich hervorgehen (z.B. der gleiche Code steht im Monat Dezember für Christbäume und in den Monaten März und April für Schokoladehasen). Um die soeben umschriebenen Anforderungen an die Bestimmbarkeit der Bedeutung von Schlüsselzahlen und Codes erfüllen zu können, ist es unerlässlich, dass diese (die fragliche Bedeutung) beim Absender und beim Empfänger zu einem gegebenen Zeitpunkt oder während einer gegebenen Zeitperiode identisch ist bzw. war. Dies setzt wiederum voraus, dass die vom Absender und Empfänger benutzte Datenbasis oder zumindest deren Root, auf der die Definition der verwendeten Schlüsselzahlen oder Codes beruhen, die gleiche ist. bzw. war.

Art. 6 Wiedergabe

Absatz 1 hält die Steuerpflichtigen dazu an, die für die Steuererhebung relevanten Daten ohne unzumutbare zeitliche Verzögerung lesbar machen zu können. Dies bedeutet, dass die

betreffenden Aufzeichnungen jederzeit verfügbar sein müssen und ohne Erschwernis gelesen werden können. Sodann muss das jeweilige Archivierungsverfahren Gewähr dafür bieten, dass der Inhalt der Wiedergabe mit den auf den maschinell lesbaren Datenträgern gespeicherten Daten übereinstimmt. Zudem ist das Verfahren für die Wiedergabe der sich auf Datenträgern befindenden Daten durch den Steuerpflichtigen in schriftlich festgehaltenen Arbeitsanweisungen niederzulegen. Hinsichtlich der Sicherstellung der längerfristigen Erhaltung der Lesbarkeit der für die Steuererhebung relevanten gespeicherten Daten sei auf die in Artikel 4 Absatz 2 dritter Abschnitt gemachten Ausführungen bezüglich des Verlusts der Lesbarkeit wegen Änderungen der zur Verfügung stehenden Textverarbeitungssysteme verwiesen.

Absatz 2 besagt, welche Anforderungen die Wiedergabe der gespeicherten Daten erfüllen muss. Dieselbe muss richtig d.h. inhaltlich unverändert, vollständig und leicht verständlich sein. Damit die beiden erstgenannten Anforderungen (inhaltlich unverändert und vollständig) als erfüllt betrachtet werden können, muss die Wiedergabe gespeicherter Daten im EDIFACT-Format ohne jegliche Aufbereitung möglich sein, d.h. die Editierfunktion muss sich auf reines Scrollen durch die Message beschränken. Damit ebenfalls die Anforderung „leicht verständlich“ als erfüllt betrachtet werden kann, muss die Wiedergabe gespeicherter Daten zudem auch noch folgende Voraussetzungen erfüllen:

- Es werden Überschriften verwendet und die Daten werden kommentiert (z.B. Nennung des Rechnungsempfängers, der Lieferadresse, der Menge etc.).
- Die Daten werden gruppiert (z.B. Lieferanschrift, Adresse des Rechnungsausstellers).
- Die Daten werden gegliedert (Kopf-, Rechnungs-, Fussteil; Spaltenbildung für Mengen, Artikelbezeichnungen, Beträge etc.).

Die Steuerpflichtigen sind des weiteren gehalten, in den Arbeitsanweisungen das Ordnungsprinzip für die Wiedergaben zu beschreiben sowie das Verfahren zu regeln, das für die Feststellung der Vollständigkeit und der Richtigkeit der Wiedergabe gespeicherter Daten verbindlich ist.

Art. 7 Zugriff auf die Daten

Absatz 1 verleiht der Eidg. Steuerverwaltung die Kompetenz, nicht nur vor Ort, d.h. am Geschäftssitz des Steuerpflichtigen Einsicht in sämtliche für die Steuer relevanten gespeicherten Daten zu nehmen und diese mit Hilfe des Datenverarbeitungssystems des Steuerpflichtigen zu prüfen, sondern die Prüfung der fraglichen Daten auch in ihren eigenen Räumlichkeiten vorzunehmen. Die direkteste Art, eine solche Prüfung in den Räumlichkeiten der ESTV durchzuführen, stellt die on-line Kontrolle dar (sog. remote auditing). Wie schon unter Art. 2 Absatz 1 erwähnt, setzt ein solches Vorgehen voraus, dass der Steuerpflichtige in der Lage ist, den Datenzugriff durch die ESTV auf die seitens der letztgenannten Behörde für die Steuererhebung als relevant erklärten Daten einzuschränken.

Des weiteren wird angeordnet, dass die Steuerpflichtigen für die Durchführung von Steuerprüfungen durch die ESTV, sei es für Prüfungen vor Ort oder sei es für sog. remote auditing, ihr Datenverarbeitungssystem zur Verfügung zu stellen haben. Dies bedeutet auch, dass sie die dadurch allenfalls bedingten, vorübergehenden Einschränkungen des Datenzugriffs durch ihre Angestellten zu dulden haben.

Absatz 2 gibt der ESTV sodann die Möglichkeit zu verlangen, dass die zu prüfenden Daten entweder nach ihren Weisungen ausgewertet werden, d.h. dass sie vom Steuerpflichtigen gleich selbst in einer Art aufbereitet werden, die ihre Prüfung ermöglicht, oder dass ihr diese Daten auf einem durch sie bestimmten Datenträger zur eigenen maschinellen Auswertung zur Verfügung gestellt werden. In beiden Fällen kann die eigentliche Prüfung der für die Steuererhebung relevanten Daten sowohl in den Räumlichkeiten der ESTV wie auch vor Ort erfolgen und hat der Steuerpflichtige die Kosten zu tragen, die im Zusammenhang mit den hierzu erforderlichen Vorarbeiten entstehen. Die im vorliegenden Absatz umschriebenen beiden Arten der Einsichtnahme in die für die Steuererhebung relevanten Daten werden in jedem Fall immer zur Anwendung kommen, wenn es dem Steuerpflichtigen nicht möglich ist, den on-line Zugriff durch die ESTV, in der im vorangehenden Absatz umschriebenen Art im erforderlichen Ausmass einzuschränken.

Absatz 3 regelt die Tragung des Schadens, der durch den Datenzugriff durch die ESTV auf das Datenverarbeitungssystem der Steuerpflichtigen entstehen könnte. Da die Mitarbeitenden der ESTV mit den Besonderheiten des Datenverarbeitungssystems der Steuerpflichtigen in der Regel nicht vertraut sind, liegt es am Steuerpflichtigen dafür zu sorgen, dass derartige Schäden unterbleiben. Diese ausschliessliche Tragung des Schadens zufolge des Zugriffs durch die ESTV auf das Datenverarbeitungssystem der Steuerpflichtigen gilt sowohl bei

Zugriffen der Mitarbeitenden der ESTV vor Ort wie auch bei solchen, die on-line d.h. von den Räumlichkeiten der ESTV aus erfolgen.

Art. 8 Prüfpfad

Absatz 1 stellt klar, dass der Prüfpfad, d.h. das Verfolgen der Geschäftsvorfälle sowohl vom Einzelbeleg über die Buchhaltung bis zur Mehrwertsteuerabrechnung als auch in umgekehrter Richtung im Falle des mittels elektronisch übermittelter und aufbewahrter Daten abgewickelten Geschäftsverkehrs genau so gilt wie im Falle des auf konventionelle Art und Weise abgewickelten. Diese Anforderung bezieht sich nicht nur auf eine fortlaufende Kontrolle der Geschäftsvorfälle, sondern auch auf die Durchführung stichprobenweise vorgenommener Prüfungen. Aber auch der Anspruch auf eine Verfolgung des Prüfpfads ohne unzumutbare zeitliche Verzögerung behält im Bereich elektronisch aufbewahrter Daten seine Gültigkeit.

Absatz 2 verlangt, dass auch bei der zusammengefassten Verbuchung von gleichen Geschäftsvorfällen eine nachträgliche und übersichtliche Aufgliederung in die Einzelposten innerhalb nützlicher Frist gewährleistet bleibt.

Absatz 3 hält die Steuerpflichtigen dazu an, auch bei elektronischer Aufbewahrung der für die Steuererhebung relevanten Daten periodische Abstimmungen zwischen den Vorsteuern gemäss EDI-Eingängen wie z.B. Eingangsfakturen in der Form ihrer Absendung bzw. ihres Empfangs und dem elektronisch geführten und gespeicherten Vorsteuerkonto vorzunehmen.

Absatz 4 schreibt ein Transaktionsjournal vor, das analog dem Journal der Geschäftsbuchhaltung, wo sämtliche Geschäftsvorfälle festgehalten werden, sämtliche elektronisch ein- und ausgegangenen Nachrichten lückenlos festhält. Wie die Bezeichnung Journal deutlich macht, handelt es sich bei diesem Transaktionsjournal um eine chronologische Aufzeichnung sämtlicher ein- und ausgegangenen EDIs, welche bloss deren für den Prüfpfad relevanten Angaben, nicht aber deren vollständigen Inhalt festhält. Sofern das Archiv gleichzeitig auch die hievordieschriebene Funktion eines Transaktionsjournals vollumfänglich wahrnimmt, erübrigt sich eine spezielle Führung desselben.

Absatz 5 hält fest, dass Protokollierungen notwendig sind, um den Prüfpfad lückenlos zu gewährleisten. Das Erfordernis dieser Protokollierung beginnt mit dem Inkrafttreten der vorliegenden Verordnung.

Art. 9 Einschaltung Dritter

Absatz 1 nennt die Voraussetzungen, die erfüllt sein müssen, damit die Einschaltung eines Dritten in den für die Steuererhebung relevanten Datenfluss zwischen Leistungserbringer und Leistungsempfänger zulässig ist. Es sind dies:

- a. Die Sicherstellung der Beachtung der in Artikel 3 Absatz 1 Buchstaben a. bis g. aufgeführten Massnahmen bei der Weitergabe der durch Datenfernübertragung oder durch Datenträgeraustausch erhaltenen Daten ohne Weiterverarbeitung. In diesem Falle wird das durch den Absender mittels digitaler Signatur angebrachte „Siegel“ an weiterzuleitenden Daten durch den eingeschalteten Dritten zwischen Empfang und Weiterleitung nicht gebrochen. Der letztgenannte kann jedoch gegebenenfalls an die durch den Absender mittels digitaler Signatur abgesicherten, weiterzuleitenden Daten zusätzliche durch ihn (den eingeschalteten Dritten) generierte und digital signierte Daten anhängen.
- b. Die Überprüfbarkeit einer allfälligen Weiterverarbeitung der erhaltenen Daten vor der Weiterleitung sowie deren Lesbarmachung innerhalb nützlicher Frist. Sofern das mittels digitaler Signatur angebrachte „Siegel“ um die weiterzuleitenden Daten durch den eingeschalteten Dritten zwecks deren Weiterverarbeitung gebrochen wird, muss dies klar erkennbar sein. Und genau so muss auch ersichtlich sein, wie der eingeschaltete Dritte die von ihm erhaltenen Daten vor deren Weiterleitung weiterverarbeitet hat. Mit der Präzisierung „weiter“(verarbeiten) wird zum Ausdruck gebracht, dass eine eigentliche Veränderung der erhaltenen und weiterzuleitenden Daten nicht zulässig ist. Der eingeschaltete Dritte darf die erhaltenen Daten vor deren Weiterleitung lediglich auf eine - unter Wahrung der Erkennbarkeit ihrer ursprünglichen Elemente - andere Art darstellen wie etwa ein Total oder ein Produkt (z.B. aus Menge und Preis pro Einheit) bilden etc. In Anbetracht der durchgeführten Bearbeitung der mittels digitaler Signatur seitens des Auftraggebers abgesichert erhaltenen Daten muss die anschliessende Weiterleitung derselben ihrerseits mit einer den Anforderungen des Artikels 3 Absatz 1 Buchstaben a. bis g. genügenden digitalen Signatur des eingeschalteten Dritten erneut abgesichert werden.
- c. Die Ermächtigung des eingeschalteten Dritten durch den Auftraggeber zur Datenweiterleitung aufgrund einer entsprechenden Vereinbarung. In dieser Vereinbarung ist genau zu regeln, wie die Weiterleitung der an den eingeschalteten Dritten übermittelten Daten zu geschehen hat, welche allfälligen (Weiter)verarbeitungen der letztgenannte vornehmen muss oder welche zusätzlichen Daten an die vom Auftraggeber erhaltenen noch anzuhängen sind. Bei der Weiterleitung von Daten zwecks Rechnungs- oder Abrechnungser-

stellung sowie Gutschriftserteilung muss der eingeschaltete Dritte für jede einzelne diesbezügliche Datenübermittlung vom Auftraggeber implizit oder explizit ermächtigt werden und zwar so, dass es für deren Empfänger deutlich ersichtlich ist. Aus der Überprüfung beim Eingang von Daten im Zusammenhang z.B. mit einer Rechnung muss deshalb ganz klar hervorgehen, dass es sich hierbei nicht um eine solche seitens des eingeschalteten Dritten, sondern eines bestimmten Leistungserbringers als ursprünglichem Gläubiger handelt. Name und Adresse des Leistungserbringers müssen deshalb deutlich im Vordergrund stehen und leicht erkennbar sein. Der eingeschaltete Dritte als Datenverarbeitungsbetrieb darf allenfalls bloss ganz am Rande durch einen Vermerk wie z.B. „Rechnung erstellt durch X. Y.“ aufgeführt sein. Der Empfänger der soeben erwähnten Daten (Rechnungen, Abrechnungen, Gutschriften) muss im Interesse der Rechtssicherheit im Geschäftsverkehr in jedem Fall sofort erkennen können, in wessen Auftrag ihm Daten seitens eines eingeschalteten Dritten übermittelt werden.

Absatz 2 legt fest, dass in Sammelabrechnungen an einen bestimmten Leistungsempfänger über die Leistungen mehrerer Leistungserbringer nur die Leistungen ein und desselben Leistungserbringers in einer Summe zusammengefasst werden dürfen. Hieraus folgt, dass die elektronische Rechnungsstellung für die Leistungen verschiedener Leistungserbringer je mittels individuellem Schlüssel digital signiert sein muss. Damit wird erreicht, dass Sammelabrechnungen vom Leistungsempfänger im Hinblick auf die Vornahme des Vorsteuerabzugs wie Einzelrechnungen verschiedener Lieferanten verwendet werden können. Sammelabrechnungen, in welchen die Leistungen mehrerer Leistungserbringer in einer Summe zusammengefasst ausgewiesen werden, erfüllen die Voraussetzungen für den Nachweis des Anspruchs auf Vorsteuerabzug nach Artikel 37 Absatz 1 MWSTG jedenfalls nicht. Dies gilt ebenso (kein Nachweis des Anspruchs auf Vorsteuerabzug) für Sammelabrechnungen, die nicht ausdrücklich im Namen des Leistungserbringers als ursprünglichem Gläubiger ausgestellt werden, wie dies insbesondere für Kreditkartenabrechnungen immer der Fall ist. Auch versteht es sich von selbst, dass die im Rahmen einer Sammelabrechnung für die Leistungen eines bestimmten Leistungserbringers erstellten Daten zwecks Rechnungsstellung je für sich die in Artikel 37 Absatz 1 MWSTG verlangten Angaben vollumfänglich enthalten müssen, damit sie für deren Empfänger gegebenenfalls einen Anspruch auf Vorsteuerabzug zu begründen vermögen.

Absatz 3 stellt klar, dass sich beispielsweise ein Leistungserbringer nicht dadurch vor einer Steuernachforderung seitens der ESTV schützen kann, indem er mit dem eingeschalteten Dritten vereinbart, dass dieser letztere der ESTV gegenüber für dem Leistungsempfänger zu Unrecht nicht belastete Steuern alleine haften werde. Solche Abmachungen gelten nur unter

den Parteien, d.h. der fragliche Leistungserbringer wird sich für die von ihm durch die ESTV nachgeforderten Steuern beim eingeschalteten Dritten gegebenenfalls schadlos halten können.

Absatz 4 verfügt, dass eingeschaltete Dritte der gleichen Auskunftspflicht unterliegen wie die in Artikel 61 MWSTG aufgeführten Personen. Die eingeschalteten Dritten erbringen wohl ihrem Auftraggeber Dienstleistungen, nicht aber an dessen Gegenpartei, so dass der soeben erwähnte Artikel des MWSTG aufgrund seines Wortlauts hinsichtlich der an die Gegenpartei des Auftraggebers weitergeleiteten Daten keine eindeutige Auskunftspflicht begründet.

Art. 10 Aufbewahrung

Absatz 1 verpflichtet den Versender und den Empfänger elektronischer Daten dazu, diese in ihrer ursprünglichen Form der Übermittlung und in ihrem ganzen Umfang auf maschinell verwertbaren Datenträgern zu archivieren. Diese Archivierungspflicht bezieht sich nicht nur auf die für die Steuererhebung relevanten Daten im engeren Sinne wie z.B. Rechnungen, Gutschriften etc., sondern auch auf Daten, die bloss dazu dienen, den Zugriff auf die soeben aufgezählten überhaupt zu ermöglichen wie z.B. Verfahrensdokumentationen, Arbeitsanweisungen, Organisationsunterlagen etc. Aber auch die von den Steuerpflichtigen selbst generierten Daten wie z.B. die elektronisch geführte Buchhaltung (Journal, Hauptbuch, Hilfsbücher wie etwa die Debitorenbuchhaltung, Betriebsrechnung) sind wie hievor umschrieben zu archivieren. Die Bestimmung schliesslich, dass eine Aufbewahrung elektronisch übermittelter, empfangener oder selbst generierter Daten nur gerade in ausgedruckter Form oder auf Mikrofilm **nicht** zulässig ist, bezweckt den sog. Medienbruch und die mit dessen Überbrückung verbundenen Probleme (Sicherstellung einer vollständigen und unveränderten Übertragung von einem Medium auf das andere) zu vermeiden.

Absatz 2 stellt klar, dass die Umwandlung (Konvertierung) von Daten insbesondere bei der interventionslosen Kommunikation zwischen Computeranwendungen auftritt. Während die Daten in strukturierter Form in einem standardisierten Format übermittelt werden, wird für die automatisierte Verarbeitung durch die beidseitigen Applikationen ein Inhouse-Format verwendet. Für diese Übersetzungen werden Konverter verwendet. Der Umfang der Daten kann ändern. Überall, wo die für die Verarbeitung verwendeten Datenformate nicht mit denjenigen der Übermittlung übereinstimmen, sind beide zu archivieren und mit dem gleichen Index zu verwalten. Die konvertierte Version ist als solche zu kennzeichnen.

Absatz 3 verlangt, dass die elektronisch gespeicherten Daten während der ganzen gesetzlich vorgeschriebenen Aufbewahrungsdauer für den Steuerpflichtigen jederzeit zugänglich sind und von einem einzigen Ort im Inland aus ohne unzumutbare zeitliche Verzögerung lesbar und maschinell auswertbar gemacht werden können. Mit dieser Vorschrift wird sichergestellt, dass Prüfungen vor Ort durch die ESTV möglich sind, ohne dass sich deren Mitarbeiter an verschiedene Orte begeben müssen. Die vorgeschriebene Aufbewahrungsdauer bezieht sich selbstverständlich auf alle in Absatz 1 hievord erwähnten Arten von für die Steuererhebung relevanten Daten, d.h. sowohl auf diejenigen im engeren wie auch diejenigen im weiteren Sinne. Da das Archiv der elektronisch gespeicherten Daten die eigentliche Rechnungsablage der Steuerpflichtigen darstellt, hat es den für diese letztere geltenden Bestimmungen bezüglich der Ordnungsmässigkeit zu genügen. Dies bedeutet, dass der Zugriff auf die fraglichen Daten aufgrund der nämlichen Kriterien möglich sein muss, wie dies für eine konventionelle Rechnungsablage auch der Fall ist. Sodann sei ein weiteres Mal auf die in Artikel 4 Absatz 2 gemachten Ausführungen betreffend der Pflicht zur Verhinderung des Verlusts der Lesbarkeit der archivierten Daten wegen Änderungen der zur Verfügung stehenden Textverarbeitungssysteme verwiesen. Schliesslich ist zu erwähnen, dass sofern ein Dritter mit der Archivierung elektronischer Daten beauftragt wird, gegenüber der ESTV trotzdem der steuerpflichtige Auftraggeber für deren ordnungsgemässe Aufbewahrung und Wiedergabe voll verantwortlich bleibt.

Absatz 4 sieht gewisse Einschränkungen betreffend der Speicherung für die Steuererhebung relevanter Daten auf Hardware vor, die sich im Ausland befindet. Sofern die fraglichen Einschränkungen zwecks Gewährleistung des Zugriffs und der Lesbarmachung bezüglich elektronischer Daten, die auf im Ausland gelegener Hardware gespeichert sind, nicht beachtet werden, genügt der Steuerpflichtige seinen Archivierungsobligationen nicht. Falls eine Prüfung durch die ESTV nicht durchführbar wäre, weil der Zugriff auf Daten, die im Ausland gespeichert werden, wegen der Nichtbeachtung der genannten Einschränkungen nicht möglich ist, hätte der Steuerpflichtige für die sich hieraus ergebenden Folgen vollumfänglich einzustehen. Dies wäre beispielsweise dann der Fall, wenn Hardware mit steuerlich relevanten Daten in einem Land aufbewahrt würde, dessen Datenschutznormen den Zugriff auf diese Daten nicht zulassen würden.

Art. 11 Aufbewahrungsdauer

Der vorliegende Artikel besagt lediglich, dass für die Aufbewahrungsdauer und Löschung elektronisch aufbewahrter Daten und Informationen, die für die Erhebung der Mehrwertsteuer

er relevant sind, genau das gleiche gilt, wie für Geschäftsbücher, Belege, Geschäftspapiere und sonstige Aufzeichnungen, die auf Papier oder auf Mikrofilmen aufbewahrt werden.

Art. 12 Übergangsbestimmungen

Absatz 1 hält fest, was gilt, wenn es den Steuerpflichtigen (noch) nicht möglich ist, sich Zertifikate von anerkannten Zertifizierungsdiensteanbietern gemäss der ZertDV bzw. des ZertES ausstellen zu lassen. Die ESTV ist diesfalls bereit, im Sinne einer Ausnahmeregelung auch Zertifikate zu akzeptieren, die von einem Zertifizierungsdiensteanbieter ausgestellt wurden, von dem nachweisbar aus guten Gründen angenommen werden darf, dass er sich gemäss Art. 3 ff. ZertDV bzw. der entsprechenden Artikel im Gesetzesentwurf ZertES wird anerkennen lassen können, sobald die Möglichkeit hiezu bestehen wird.

Absatz 2 regelt die vorläufige Zulassung durch die ESTV der seitens ausländischer Zertifizierungsdiensteanbietern ausgestellten Zertifikate. Nachdem man bereit ist, von inländischen Zertifizierungsdiensteanbietern ausgestellte Zertifikate zu akzeptieren, wenn aus guten Gründen davon ausgegangen werden kann, dass diese die verlangten Voraussetzungen erfüllen, um sich dereinst – sobald die Möglichkeit hiezu überhaupt bestehen wird – anerkennen lassen zu können, ist es naheliegend, gegenüber ausländischen Zertifizierungsdiensteanbietern auf analoge Art und Weise vorzugehen. Demzufolge werden durch ausländische Zertifizierungsdiensteanbieter ausgestellte Zertifikate im Sinne einer vorläufigen Regelung durch die ESTV akzeptiert, sofern diese erstgenannten in der fraglichen Eigenschaft in einem Land anerkannt sind, das nachgewiesenermassen vergleichbare Anforderungen an die betreffende Anerkennung stellt wie die Schweiz.

Art. 13 Konsultation der Wirtschaft

Um der weiteren technischen Entwicklung bei der Übermittlung und Aufbewahrung für die Steuererhebung relevanter elektronischer Daten möglichst rasch Rechnung tragen zu können, wurden die zu deren Regelung erforderlichen (technischen) Detailvorschriften bewusst nicht in der MWSTGV, sondern in einer Ausführungsverordnung des EFD festgelegt. Dank diesem Vorgehen wird es der ESTV möglich sein, auf Grund ihrer Kontakte mit den Steuerpflichtigen, welche ihre für die Steuererhebung relevanten Daten elektronisch übermitteln und aufbewahren, über Änderungen des technischen Umfelds und der sich daraus ergebenden Bedürfnisse für Anpassungen der rechtlichen Regelung stets aus erster Hand informiert

zu sein und diese innerhalb kürzester Zeit zu veranlassen. Die vorliegende Verordnung des EFD regelt die Übermittlung und Aufbewahrung für die Steuererhebung relevanter elektronischer Daten somit ausdrücklich auf Grund des heutigen Standes der Informationstechnologien, deren Fortschreiten vielleicht sogar schon vor Ablauf eines Jahres unabdingbare Anpassungen derselben verlangen könnte.

Art. 14 Inkrafttreten

Kein Kommentar.