Verfahrensdokumentation elektronische Rechnungsabwicklung für [XY-GmbH]

Mustervorlage

Das Dokument und alle im Dokument gegebenen Informationen sind Copyright-geschützt. Alle Rechte zur Vervielfältigung einschließlich Kopieren in elektronischer oder gedruckter Form, Neuerstellung, Übersetzung, Mikroverfilmung, Speichern auf elektronischen Medien sowie die Weiterverarbeitung des Dokuments oder von Teilen des Dokuments in elektronischer Form ist strengstens untersagt und obliegt ausdrücklich allein der XXX.

Copyright © 2014 XXX. Alle Rechte vorbehalten.

***** Legende für dieses Musterdokument (im finalen Dokument zu löschen) *****

Dieses Musterdokument wurde durch den Arbeitskreis Qualitätssicherung des VeR e.V. erarbeitet. Beteiligt waren die Firmen B&L Management Consulting, Peters, Schönberger & Partner.

Fragen können gerichtet werden an: ??

Dieses Musterdokument verwendet Farben und Sonderzeichen zur Verdeutlichung der Bedeutung der Texte. Die Elemente haben folgende Bedeutung:

Xyz = Schwarzer Text ist Mustertext und kann – wenn passend – so übernommen werden

Xyz = *Blauer, kursiver Text enthält Hinweise über die, unter der entsprechenden Überschrift, vorgesehenen Inhalte. Er muss durch die eigenen Inhalte ersetzt werden*

[Xyz] = *Eckige Klammern kennzeichnen Platzhalter, die durch eigene Inhalte zu füllen sind, z.B. [Grafik: Beteiligte Organisationseinheiten] erwartet das Einfügen einer entsprechenden Grafik*

[X_Yz] = Hellblauer Platzhalter bezeichnet eine Variable, die im Tabellenanhang gepflegt wird und im Text automatisch gefüllt wird. Z.B. [V_VFD] enthält den Verantwortlichen für diese Verfahrensdokumentation. Variable sind teilweise über Anfangsbuchstaben gruppiert, z.B. „V_“ für alle Verantwortlichkeiten. Die Verwendung von Variablen ist optional.

Xyz = Unterstrichener, farbiger Text verfügt über einen HyperLink (innerhalb dieses Dokumentes)

IKS! = Ist ein Hinweis auf das interne Kontrollsystem. Die so gekennzeichneten Stellen sind auch Bestandteil des IKS, werden dort aber nicht wiederholt.

Es handelt sich insgesamt um eine Mustervorlage. D.h. die Vorlage ist auf jeden Fall anzupassen. Da typischerweise Teile der hier geforderten Dokumentationen schon anderweitig vorliegen, können Unterkapitel entfallen oder primär aus externen Verweisen bestehen. Verweise sollten aber immer möglichst zielgenau spezifiziert sein (z.B. mit Kapitel- oder Seitennr.).

***** Ende der Legende für dieses Musterdokument (im finalen Dokument zu löschen) *****

Mustervorlage

Änderungsnachweis für das Musterdokument

Datum	Version	Autor	Änderung
14.01.2010	0.9	Holger Werner, VeR e.V.	Erstellung des Dokumentes
28.01.2010	0.91	Oliver Berndt	Überarbeitung und Ergänzung
16.03.2010	0.97	Oliver Berndt	Einarbeitung Kommentare A. Kauffmann
06.04.2010	0.99	Oliver Berndt	Einarbeitung Kommentare H. Werner und M. Lamm
13.03.2010	1.1	Oliver Berndt	Überarbeitung gemäß aktueller Gesetzeslage, z.B. keine Signaturpflicht mehr
20.08.2014	1.2	Tobias Lieb, PSP Oliver Berndt, B&L	Qualitätssicherung und Finalisierung

Verantwortlich für dieses Dokument

Die Verantwortung für die Inhalte und die Pflege dieses Dokumentes liegt bei: [V_VFD]

Gültigkeit dieses Dokuments

Die vorliegende Dokumentation beschreibt die organisatorisch-technische Lösung im Gültigkeitszeitraum von [Gültig_von] bis [Gültig_bis].

Mustervorlage

Inhaltsverzeichnis

0 VORBEMERKUNG 10

1 BESCHREIBUNG DES EINSATZGEBIETES 12

1.1 Unternehmen und eInvoice-Leistungsangebot 12

1.2 Rechtliche Grundlagen 12

1.2.1 Umsatzsteuergesetz 12

1.2.2 Aufbewahrung und Prüfbarkeit 12

1.3 Organisationsbeschreibung 13

1.3.1 Allgemeine Organisation 13

1.3.2 Lösungsbezogene Organisation 13

1.3.3 Vertretungsregelungen 14

1.3.4 Betriebsvereinbarung 14

1.4 Vertragliche Grundlagen 15

1.4.1 VeR-Vereinbarungen 15

1.4.2 Vereinbarungen mit Rechnungsausstellern 15

1.4.3 Vereinbarungen mit Rechnungsempfängern 15

2 SACHLOGISCHE LÖSUNG 16

2.1 Aufgabenstellung und Lösungsansatz 16

2.2 Prozess für Rechnungssteller 16

2.2.1 Einholung Einverständnis RE 16

2.2.2 Einrichtung des Rechnungsempfängers 17

2.2.3 Prozessüberblick und Prozessteuerung 17

2.2.4 Rechnungserstellung bzw. Dokumenten/Daten–Eingang 18

2.2.5 Konvertierung und Auslese der Verarbeitungsinformationen 18

2.2.6 *Optional:* Signaturerstellung 18

2.2.7 Transport zwischen den Systemen 19

2.2.8 *Optional:* Signaturverifikation und Prüfprotokoll 19

2.2.9 Dokumenten – Ausgang 19

2.2.10 Archivierung 20

2.2.11 Monitoring und Protokollierung 20

Mustervorlage

2.2.12 Fehlerhandling 21
2.2.13 Zurückziehen des Einverständnisses 21

2.3 Prozess für Rechnungsempfänger 21
2.3.1 Verantwortung Prozess Rechnungsempfänger 21
2.3.2 Einrichtung des Rechnungssteller 21
2.3.3 Prozessüberblick 22
2.3.4 Rechnungseingang 22
2.3.5 Konvertierung und Auslese der Verarbeitungsinformationen 22
2.3.6 *Optional:* Signaturverifikation und Prüfprotokoll 22
2.3.7 Transport zwischen den Systemen 22
2.3.8 Dokumenten – Ausgang 23
2.3.9 Archivierung 23
2.3.10 Monitoring und Protokollierung 23
2.3.11 Fehlerhandling 23
2.3.12 Zurückziehen des Einverständnisses 23

2.4 Mandantenfähigkeit 24

2.5 Auslagerung/Entsorgung gemäß BDSG 24

3 TECHNISCHE SYSTEMLÖSUNG 25

3.1 Technische Lösung für Rechnungssteller 25
3.1.1 Eintreffen der Daten im Unternehmen 25
3.1.2 Konvertierung 25
3.1.3 *Optional:* Signierung 26
3.1.4 Transport zwischen den Systemen 26
3.1.5 *Optional:* Verifikation 26
3.1.6 Indizierung und Datenbank 26
3.1.7 Visualisierung und Reproduktion 26
3.1.8 Protokollierung 27

3.2 Technische Lösung für Rechnungsempfänger 27
3.2.1 Eintreffen der Daten im Unternehmen 27
3.2.2 Konvertierung 27
3.2.3 *Optional:* Signierung 27
3.2.4 Transport zwischen den Systemen 27

Mustervorlage

3.2.5 *Optional:* Verifikation 28
3.2.6 Indizierung und Datenbank 28
3.2.7 Visualisierung und Reproduktion 28
3.2.8 Protokollierung 28

3.3 Systembeschreibung 28
3.3.1 Standard-Softwarekomponenten 29
3.3.2 Individuelle Programmteile 29
3.3.3 Netzwerke 29
3.3.4 Hardware 29
3.3.5 Schnittstellen 29
Schnittstelle zur Übergabe von Rechnungen vom Kunden 29
Schnittstelle zur Übergabe von Rechnungen eingehend 29
Schnittstelle zur Übergabe von Rechnungen ausgehend 30
Schnittstelle zur Übergabe von Rechnungen an das Archiv 30

3.4 Migration 30
Applikationen 30
Optional: Signatur-Systeme 30
Archiv 30

4 SICHERHEIT (PHYSISCH UND LOGISCH) 31

4.1 Allgemeines IT-Sicherheitskonzept 31
4.1.1 IT-Versicherungen 31
4.1.2 Datenschutz BDSG 31
4.1.3 Netzzugriffe 31

4.2 Benutzerverwaltung und Berechtigungskonzept 32
4.2.1 Authentifizierung und Passwort-Handling 32
4.2.2 Zuordnung Zugriffsrechte zu Benutzergruppen 32
4.2.3 Schutz sonstiger Ressourcen 32

4.3 Optional: Zertifikatshandling 32
4.3.1 *Optional:* Verfahren zur Beantragung neuer Zertifikate 33
4.3.2 *Optional:* Verfahren bei Verlust Zertifikat 33
4.3.3 *Optional:* Verfahren bei Ablauf Zertifikat 33
4.3.4 *Optional:* Verfahren bei Wechsel Zertifikatsinhaber 33

Mustervorlage

4.4 Ausfallsicherheit 33
4.4.1 Generelles und Virenschutz 33
4.4.2 Maßnahmen zur Verfügbarkeitsoptimierung 33
4.4.3 Datensicherung und Recovery 34
4.5 Standorte und Zugangsregelung 34
4.5.1 Feuerschutz/Elementarschäden 34
4.5.2 Stromversorgung 34
4.5.3 Kühlanlagen 34
4.5.4 Zugangsregelung Gebäude 35
4.5.5 Zugangsregelung IT-Abteilung 35
4.5.6 Zugangsregelung Rechenzentrum 35
4.5.7 Vergabe von Zugangsberechtigungen 35
5 TECHNISCHER BETRIEB 36
5.1 Organisation des eInvoice-Betriebs 36
5.1.1 Service Level Management 36
5.1.2 Qualifikationsmaßnahmen 36
5.1.3 Sonstiges Training 36
5.2 Availability and Service Continuity 36
5.2.1 Monitoring und Health Check 36
5.2.2 Wartungsverträge 37
5.2.3 Vorbeugende Wartung 37
5.2.4 Anweisungen zum generellen Verhalten bei Störungen (Notfallhandbuch) 37
5.3 Incident and Problem Management 37
5.3.1 Notfall 37
5.3.2 Recovery bei Störungen der Komponenten dieses Prozesses 37
5.3.3 Probleme der Anwender 37
5.3.4 Fehlerhandling 37
6 INTERNES KONTROLLSYSTEM (IKS) 38
7 TEST 41
7.1 Testkonzept und Abnahme 41

Mustervorlage

7.2 Standardtests 41
7.2.1 Testbereich Dokumenteingang 41
7.2.2 Testbereich Importieren & Archivieren 41
7.2.3 Testbereich Retrieval, Anzeige und Reproduktion 41
7.2.4 Testbereich Configuration Management 41
7.3 Individuelle Tests 41
7.4 Testprotokolle 41
7.5 Change and Release Management 42
7.5.1 Änderungsprozess 42
7.5.2 Freigabeprozess 42
8 TABELLARISCHER ANHANG 43
8.1 Geltungsbereich und Kundenverträge 43
8.2 Relevante Dokumentationen, Handbücher, etc. 44
8.3 Interne Verantwortlichkeiten 44
8.4 Benutzer und Nutzergruppen 45
8.5 Zugriffsberechtigungen 46
8.6 Configuration Management 47
8.6.1 Datenblätter Applikationen 48
8.6.2 Datenblätter Infrastruktur-Software 51
8.6.3 Datenblätter Hardware 56

Mustervorlage

Liste der Abbildungen und Tabellen

Abb. 1 – Beteiligte Organisationseinheiten eInvoice-Prozesse 14
Abb. 2 – Beteiligte Personen eInvoice-Prozesse 14
Abb. 3 – Überblick Prozess Rechnungsstellung 17
Abb. 4 – Überblick Prozess Rechnungsempfänger 22
Abb. 5 – Netzwerkplan eInvoice-Systeme 25

Mustervorlage

0 Vorbemerkung

Diese Verfahrensdokumentation dokumentiert den gesamten Prozess „Rechnungsabwicklung“ wie er als Dienstleistung sowohl für Rechnungssteller als auch für Rechnungsempfänger durchgeführt wird. In diesem Dokument reden wir von „eInvoice-Prozess“, wenn wir Aussagen gesamtheitlich für den Versand- und den Empfangsprozess machen.

Da es sich um ein veränderbares System, inkl. veränderbarer Teilprozesse handelt, sind Änderungen jederzeit schriftlich festzuhalten und als neue Versionen der Verfahrensdokumentation zu archivieren.

Die Verfahrensdokumentation gehört zu den Arbeitsanweisungen und sonstigen Organisationsunterlagen im Sinne des § 257 Abs. 1 HGB, bzw. § 147 Abs. 1 AO und ist grundsätzlich 10 Jahre aufzubewahren. Zusätzlich ist die Verfahrensdokumentation stets aktuell zu halten, d.h. Veränderungen der beschriebenen Prozesse sind mit Zeitstempel einzupflegen.

Die Grundsätze können immer nur von Hardware, Software und den implementierten Kontrollen (manuell und maschinell) in Kombination erfüllt werden. Es ist also stets auf den gesamten Prozess abzustellen.

Um die Anforderungen zu Ordnungsmäßigkeit- und Sicherheit gerecht zu werden, sind folgende Punkte einzuhalten:

- **Vollständigkeit**

  Insbesondere vollständiger Empfang, Verarbeitung und Versand der Daten und Dokumente

- **Richtigkeit**

  Insbes. fehlerfreie Verarbeitung der Daten bei der Konvertierung

- **Nachvollziehbarkeit**

  Insbesondere Nachvollziehbarkeit und Prüfbarkeit der Daten über die Dauer der gesetzlichen Aufbewahrungsfrist, Dokumentation der Konvertierung

  Sowie Sicherstellung, dass evtl. Veränderungen und ursprünglicher Inhalt erkennbar sind.

- **Ordnung**

  Insbesondere nachvollziehbare Verarbeitungsschritte, zeitliche und sachliche Ordnung

- **Zeitgerechtigkeit**

  Insbesondere Protokollierung des Zeitpunkts jeder Verarbeitungsstufe, Sicherstellung

  der richtigen Periodenzuordnung der Daten

- **Unveränderlichkeit**

  Insbesondere Sicherstellung, dass „Originalbelege“, z.B. signierte PDFs, unverändert transportiert und archiviert werden.

Mustervorlage

- **Vertraulichkeit**

  Insbesondere Sicherstellung, dass Kenntnisnahme von Daten durch nichtberechtigte Personen ausgeschlossen ist.

- **Integrität**

  Insbesondere Sicherstellung, dass Daten und Systeme vollständig und richtig zur Verfügung stehen und Daten vor Manipulationen geschützt sind

  - von außen: Virenschutz

  - von innen: Berechtigungskonzept

- **Verfügbarkeit**

  Insbesondere Sicherstellung der dauerhaften Bereitstellung von Hardware, Software,

  Daten, inkl. Vorkehrungen für Notfall

- **Autorisierung**

  Insbesondere Sicherstellung, dass nur berechtigte Personen ihnen zugeteilte Funktionen ausüben dürfen

- **Authentizität**

  Insbesondere Sicherstellung der eindeutigen Zuordenbarkeit der Aktion zu seinem Verursacher

- **Verbindlichkeit**

  Insbesondere Sicherstellung, dass die Transaktionen Verbindlichkeitswirkung entfalten und nicht abstreitbar sind

Sofern die benötigten Informationen bereits in anderen Dokumenten vorliegen und hier zu detailliert wären, wird mit Verweisen gearbeitet. Dabei wird der Fundort der fraglichen Information genau spezifiziert.

Informationen, die sich typischerweise häufig ändern und innerhalb eines Fließtextes schwierig zu pflegen sind, werden im tabellarischen Anhang gelistet und im Text nur referenziert.

Mustervorlage

1 Beschreibung des Einsatzgebietes

1.1 Unternehmen und eInvoice-Leistungsangebot

Mit welchen Services für welche Kunden (Branchen) positioniert sich der Dienstleister im Markt?

Welche Rolle spielt dabei eInvoicing?

1.2 Rechtliche Grundlagen

Das Verfahren berücksichtig als rechtliche Grundlagen UStG,HGB,AO,GDPdU sowie die sich daraus ergebenden Vorgaben und Verordnungen soweit sie für die [O_Dokumentarten] relevant sind.

1.2.1 Umsatzsteuergesetz

Auf der Grundlage des § 14 UStG können Rechnungen, vorbehaltlich der Zustimmung des Empfängers auch auf elektronischem Weg übermittelt werden, wobei die Zustimmung auch stillschweigend durch konkludentes Handeln erfolgen kann. Entscheidend für die Anerkennung aus umsatzsteuerrechtlicher Sicht ist, dass die Echtheit der Herkunft, die Unversehrtheit und die Lesbarkeit des Inhalts gewährleistet ist (§ 14 Abs. 1 UStG). Es ist dem Unternehmer überlassen wie er dies erreicht. Zulässig sind sämtliche Verfahren, die einen verlässlichen Prüfpfad zwischen Rechnung und Leistung schaffen.

Die bis 30.06.2011 geforderten Verfahren der elektronischen Signatur bzw. der EDI-Vereinbarung zur Sicherstellung der Unversehrtheit und der Echtheit der Herkunft sind weiterhin zulässig. Es ist aber zu bedenken, dass damit der Zusammenhang mit der erbrachten Leistung, also der verlässliche Prüfpfad noch nicht sichergestellt ist. Außerdem ist damit die ebenfalls geforderte Lesbarkeit noch nicht sichergestellt.

Die Herstellung des verlässlichen Prüfpfades erfolgt somit primär durch die klassische Rechnungsprüfung, die neben den formalen auch inhaltliche Prüfungen und Abgleiche mit den vorhandenen Stamm- und Bestelldaten durchführt. Ob diese Prüfungen technisch oder organisatorisch erfolgen ist unerheblich. Es ist Aufgabe dieser Dokumentation zu zeigen, wie der verlässliche Prüfpfad hergestellt wird.

1.2.2 Aufbewahrung und Prüfbarkeit

Neben der Anerkennung elektronisch übermittelter Rechnungen sind insbesondere die Pflichten in Bezug auf die Aufbewahrung und Prüfbarkeit von praktischer Bedeutung. Auf der Grundlage des § 14b Abs. 1 UStG sind sowohl der leistende Unternehmer als auch der Leistungsempfänger verpflichtet, Rechnungen über einen Zehnjahreszeitraum aufzubewahren und die Lesbarkeit sicherzustellen. Wenn im Fall elektronisch übermittelter Rechnungen der Nachweis über die Echtheit und die Unversehrtheit der Daten über die Signaturtechnologie erfolgen soll, sind Signatur und Prüfprotokoll ebenfalls über diesen Zeitraum aufzubewahren, selbst wenn nach anderen Vorschriften die Gültigkeit dieser Nachweise bereits abgelaufen ist. Das bedeutet jedoch nicht, dass dies immer erfolgen muss, wenn die Rechnung eine Signatur enthält, sondern

Mustervorlage

nur wenn der Empfänger sich entscheidet diese Technologie als Teil seines Internen Kontrollsystems (IKS) zu nutzen.

Dabei müssen der Aufbau und der Ablauf des angewandten Verfahrens für das Finanzamt auf der Grundlage des § 145 AO innerhalb angemessener Frist nachprüfbar sein. Zur Sicherstellung einer behördlichen Überprüfung elektronisch generierter Dokumente sieht die Abgabenordnung über § 147 Abs. 6 AO ein ausgeprägtes Zugriffsrecht der Finanzverwaltung auf die Unternehmens-EDV im Rahmen von Außenprüfungen vor, welches im BMF-Schreiben vom 16. 7. 2001, Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU) seitens der Finanzverwaltung konkretisiert wurde.

In Anlehnung an die Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS) setzt die Finanzverwaltung bei elektronischen Abrechnungen insbesondere voraus, dass der Originalzustand des übermittelten und ggf. noch verschlüsselten Dokuments jederzeit überprüfbar sein muss. Hierzu ist es erforderlich, dass elektronische Rechnungen durch die Übertragung der Inhalts- und Formatierungsangaben auf einem entsprechenden Datenträger archiviert werden und eine Bearbeitung während des Übertragungsvorgangs ausgeschlossen ist. Neben einer zweifelsfreien Indexierung sind die Bearbeitungsvorgänge zu protokollieren und mit abzuspeichern. Die entsprechenden Vorgaben sind in den GDPdU spezifiziert. Dies wurde sowohl bei der organisatorischen und technischen Gestaltung der Prozesse als auch bei der Zusammenarbeit mit anderen Systemen, hier speziell der Archivierung, berücksichtigt.

Hinweis: Es wird erwartet, dass noch in 2014 die GoBS und die GDPdU durch die GoBD[1] des Bundesfinanzministeriums ersetzt werden. Bei den GoBD kommen jedoch keine wesentlichen Anforderungen neu hinzu, sondern es handelt sich primär um Klarstellungen bzgl. der Anwendung neuer Technologien. Eine Reihe dieser Klarstellungen beziehen sich konkret auf den Einsatz Elektronischer Rechnungen.Beispielsweise wird die hohe Bedeutung einer Verfahrensdokumentation sehr stark betont.

1.3 Organisationsbeschreibung

1.3.1 Allgemeine Organisation

Wie ist das Unternehmen/der Konzern insgesamt strukturiert (kurz)?

Welches Unternehmen bzw. welcher Geschäftsbereich trägt die Verantwortung für das beschriebene Verfahren?

1.3.2 Lösungsbezogene Organisation

In die eInvoice-Prozesse ist nur ein Ausschnitt des gesamten Unternehmens aktiv involviert. Diese Teilbereiche sind in der folgenden Grafik dargestellt.

[1] GoBD = **Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff,**

Mustervorlage

[Grafik: Beteiligte Organisationseinheiten eInvoice-Prozesse]

ABB. 1 – BETEILIGTE ORGANISATIONSEINHEITEN EINVOICE-PROZESSE

Die in den Organigrammen genannten Personen haben folgende Funktionen innerhalb der eInvoice-Prozesse:

Offizielle Position	Name	Verantwortung	Vertreten durch
	[V_Supplier]	Rechnungserstellung und Versand	[V_Supplier_subst]
	[V_Buyer]	Rechnungsempfang und Prüfung	[V_Buyer_subst]

ABB. 2 – BETEILIGTE PERSONEN EINVOICE-PROZESSE

Die eInvoice-Prozesse nutzen die RZ-Infrastruktur am Standort [L_Name]

1.3.3 Vertretungsregelungen

Um den Prozess der Rechnungserstellung, ggf. Signierung und Archivierung bei Ausfällen von verantwortlichen Mitarbeitern zu gewährleisten, ist die Benennung und Schulung von Vertretern zu regeln.

Die Dokumentation des Prozesses muss für den Vertreter ausreichend und zielführend angelegt sein. Der bzw. die Vertreter müssen bei wichtigen Projektmeetings, etc. anwesend sein.

Sollten trotz der Regelungen Probleme auftauchen, ist *[V_eInvoice]* zu benachrichtigen.

1.3.4 Betriebsvereinbarung

Unabhängig von der Mitarbeiterqualifikation in Bezug auf die eInvoicing-Lösung unterliegen alle Mitarbeiter den folgenden Betriebsvereinbarungen:

Typischerweise gibt es hier Vereinbarungen zur Einhaltung des Datenschutzes, des E-Mail-Managements oder ähnlichem. Am besten Titel und 1-2 Sätze zum Inhalt.

Mustervorlage

1.4 Vertragliche Grundlagen

1.4.1 VeR-Vereinbarungen

Als Mitglied im Verband elektronische Rechnung, VeR e.V. haben wir uns zur Einhaltung der folgenden Vereinbarungen verpflichtet:

- Code of Ethics
- Interoperabilitätsvereinbarung

Hinzu kommen die Vereinbarungen, die wir jeweils mit den Kunden als Rechnungssteller oder Rechnungsempfänger treffen (siehe Unterkapitel). Die Verträge und Vereinbarungen bzw. exakte Verweise finden Sie unter Verträge und Vereinbarungen.

Evtl. weitere Vereinbarungen, SLAs etc. mit Kunden (kurze Erläuterung und Verweise)

1.4.2 Vereinbarungen mit Rechnungsausstellern

Im Anhang finden Sie unter Verträge und Vereinbarungen die folgenden Dokumente, die auch den konkretem Tätigkeitsumfang beschreiben:

- Inhalte der Beauftragung durch den Rechnungsaussteller
- Bevollmächtigung zu sämtlichen Handlungen im Namen und für Rechnung des Rechnungsausstellers
- Befreiung von dem Verbot der Mehrvertretung nach § 181 BGB, soweit der Dienstleister gleichzeitig für Rechnungsaussteller und Rechnungsempfänger tätig wird
- Liste der Rechnungssteller, mit denen diese Vereinbarungen geschlossen wurden

1.4.3 Vereinbarungen mit Rechnungsempfängern

Im Anhang finden Sie unter Verträge und Vereinbarungen die folgenden Dokumente, die auch den konkretem Tätigkeitsumfang beschreiben:

- Inhalte der Beauftragung durch den Rechnungsempfänger
- Bevollmächtigung zur Handlung im Namen und für Rechnung des Rechnungsempfängers

Und soweit relevant:

- Befreiung von dem Verbot der Mehrvertretung nach § 181 BGB

Mustervorlage

2 Sachlogische Lösung

Verantwortlich für die organisatorisch-technische Gestaltung der Gesamtlösung ist:
[V_eInvoice]

2.1 Aufgabenstellung und Lösungsansatz

Soweit keine Differenzierung Rechnungssteller-Rechnungsempfänger erforderlich (sonst im Unterkapitel):

- *Welchen detaillierten Zielen unterliegt das beschriebene Verfahren (kurz)?*
- *Was soll durch das Verfahren genau erreicht werden? (Detaillierung zu oben)?*

Eventuell werden sowohl für den Rechnungsersteller (Sender) als auch für den Rechnungsempfänger (Empfänger Leistungen durch denselben Dienstleister erbracht. Wenn der Dienstleister beispielsweise des Rechnungserstellers im Auftrag des Erstellers signiert, aber auch im Auftrag des Empfängers die Gültigkeit der Signatur verifiziert. Damit werden Kompatibilitäts- und Interoperabilitätsprobleme von vorneherein vermieden. Für die Anerkennung eines solchen Verfahrens sind jedoch die organisatorische und technische Trennung beim Dienstleister sowie die klare Nachvollziehbarkeit des Sphärenübergangs erforderlich.

Die Trennung der Leistungen für Sender und Empfänger erfolgt in unserem Unternehmen durch:

- Unterschiedliche Verantwortlichkeiten für die Prozesse
- Unterschiedliche Serversysteme für die Software-Komponenten zur Signierung und zur Verifizierung
- Automatische Protokollierung der Übertragung

2.2 Prozess für Rechnungssteller

Verantwortlich für die organisatorisch-technische Gestaltung des Prozesses ist:
[V_eInvoice_Outbound]

- *Welchen weitergehenden Zielen unterliegt dieser Prozess?*
- *Was soll durch das Verfahren für Rechnungssteller genau erreicht werden?*

2.2.1 Einholung Einverständnis RE

Das UStG verlangt das Einverständnis des Rechnungsempfängers (RE). Soweit die Dienstleistung im Auftrag des Rechnungsempfängers erbracht wird, sind die akzeptierten Rechnungen bereits in den Verträgen spezifiziert.

Soweit die Dienstleistung im Auftrag des Rechnungsstellers erbracht wird, ist es Aufgabe des Kunden das Einverständnis einzuholen. Zieht der Empfänger sein Einverständnis zurück, so ist dies ebenfalls zwischen Rechnungssteller und Rechnungsempfänger bilateral zu klären.

Mustervorlage

- *Wenn der Dienstleister beauftragt ist das Einverständnis der Empfänger einzuholen, ist hier zu beschreiben, wie das passiert.*

IKS!

Kontrollziel	Kontrolle
Es muss hinreichend gewährleistet sein, dass für jeden RE ein Einverständnis eingeholt wird.	[…]

2.2.2 Einrichtung des Rechnungsempfängers

- *Woher weiß der Dienstleister, welche RE einzurichten sind?*
- *Wie, in welchen Systemen, von wem werden diese eingerichtet?*
- *Wie muss darüber hinaus eine Parametrisierung erfolgen, welche Bestandteile sind für alle Kunden gleich, welche sind individuell (diese könnte man z.B. gesondert als Anlagen anhängen)?*
- *Wie werden Tests mit den Kunden durchgeführt?*
  Siehe dazu auch 6.1 "Abnahme Kunde", evtl. kann hier ein Verweis bzgl. des Test eingebaut werden.
- *Welche Kontrollen, Protokollierungen existieren, um den Prozess nachvollziehen zu können?*
- *Evtl. Verweis auf Arbeitsanweisungen*

2.2.3 Prozessüberblick und Prozessteuerung

Die folgende Grafik gibt einen Überblick über die organisatorische-technische Gestaltung des Prozesses. Eine genaue Erläuterung der technischen Abläufe und der beteiligten Komponenten erfolgt im Kapitel Technische Systemlösung.

[Grafik: Überblick Prozess Rechnungsstellung]

ABB. 3 – ÜBERBLICK PROZESS RECHNUNGSSTELLUNG

- *Hier wäre eine kurze Erläuterung des Verfahrens – im Sinne eines Überblicks – sinnvoll. Details kommen dann in den Unterkapiteln bzw. später im technischen Teil.*
- *Hier sollte auch die Steuerung des Prozesses, z.B. über Workflow, aus Anwendungssicht beschrieben werden. Details kommen dann in den Unterkapiteln bzw. später im technischen Teil.*
- *Soweit ein Abgleich bzw. eine Plausibilitätsprüfung mit Kundendaten erfolgt, sollte dies hier bzw. in den jeweiligen Unterpunkten beschrieben werden. Ggf. ist auf kundenspezifische Ergänzungen des generischen Prozess zu verweisen.*
- *Beim Handling von Daten&Dokument sowie ggf. konvertierten Kopien muss sichergestellt sein, dass nur EIN „Rechnungsoriginal“ existiert. Es sollte gezeigt werden, durch welche Prüfungen dies erreicht wird.*
- *Vor allem dürfen nicht mehr Rechnungen entstehen als Datensätze geliefert wurden.*
- *Wichtig ist auch aufzuzeigen (generell oder in den Unterkapiteln), wie vermieden wird, dass einzelne Datensätze/Rechnungen in einem Schritt hängen und unbearbeitet bleiben. Letztendlich muss zu jedem empfangenen*

Mustervorlage

Datensatz eine Rechnung versendet werden bzw. muss jede eingehende Rechnung eine ausgehende Rechnung zur Folge haben.

- *Wenn die Signatur weiterhin eingesetzt werden soll, ist auf Folgendes zu achten: Einige der nachfolgenden Punkte ergeben sich i.d.R. aus der Herstellererklärung bzw. dem Signaturgesetz, die für jede Signaturerzeugungskomponenten (SEK) oder Signaturprüfkomponenten (SPK) vorhanden sein muss und Bestandteil der Verfahrensdokumentation sein sollte. Sofern sich der Punkt aus der Herstellererklärung ergeben sollte, dann ist dies bei den nachfolgenden Aufzählungen kurz vermerkt.*

2.2.4 Rechnungserstellung bzw. Dokumenten/Daten–Eingang

- *Im Vordergrund stehen in diesem und den folgenden Unterkapiteln Prozess, Funktionsweise und Bedienung, aber alles kurz (keine detaillierte Bedienungsanleitung). Technische Details folgen im nächsten Kapitel.*
- *In welcher Form kommen die Daten und/oder Dokumente an und wie ist Integrität und Authentizität sichergestellt?*
    - *Bei Signatureinsatz, evtl. in Herstellererklärung*
- *Wie werden sie erstbearbeitet, z.B. Prüfungen auf Vollständigkeit der Daten gemäß EU-Mindestanforderung oder kundenspezifische Checks, z.B.*
- *Wie ist sichergestellt, dass das Abrechnungsdokument die richtigen Daten enthält und rechnerisch korrekt ist?*
- *Soweit Sammelrechnungen erstellt werden, ist sicherzustellen, dass die Angaben der Summe der Einzelrechnungen entsprechen.*

2.2.5 Konvertierung und Auslese der Verarbeitungsinformationen

- *Was wird ausgelesen und aus welchem Grund konvertiert (wie das technisch erfolgt, wird später beschrieben)?*
- *Das konvertierte Format muss alle vereinbarten Informationen beinhalten*
- *Sofern Änderungen an den Daten vorgenommen werden, z.B. durch Konvertierung, muss dies klar nachvollziehbar sein und Ursprungsdaten sowie Konvertierungsverfahren sollten verfügbar bleiben. Verbindung zwischen konvertierten Daten und Ursprungsdaten muss gegeben sein.*

2.2.6 *Optional:* Signaturerstellung

- *Durch wen und welche Komponenten wird die Signatur erstellt und wie mit dem Beleg oder den Daten verbunden (wie das technisch erfolgt, wird später beschrieben)?*
    - *evtl. in Herstellererklärung*
- *Wichtig ist die Beschreibung des Massensignaturverfahrens mit den folgenden Aspekten*
    - *Wie ist die alleinige Kontrolle des Signaturinhabers umgesetzt?*
    - *Welche Parameter wurden für die Massensignatur gewählt?*
    - *Woher bezieht der Server die Zeit für die Signaturerstellung (NTP, Atomuhr, ..)?*
    - *Was passiert bei Störungen, z.B. wenn der Signaturinhaber außerplanmäßig seine PIN eingeben muss?*
    - *Wie ist sichergestellt, dass die erzeugten Signaturen auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen.*

Mustervorlage

- *Sofern unterschiedliche Verantwortlichkeiten existieren, ist wichtig nachzuvollziehen, wer für die formelle Erstellung der (Zeitpunkt der Signatur) verantwortlich zeichnet. Die anderen Verantwortlichkeiten sollten dann ebenfalls beschrieben werden. Dies kann auch über die Protokollierung erfolgen.*

IKS!

Kontrollziel	Kontrolle
Es muss hinreichend gewährleistet sein, dass nur signierte Dokumente im Prozess weiterverarbeitet werden dürfen.	Systeminternes Fehlerhandling. Fehlgeschlagene Signaturen werden ins ERROR-Verzeichnis verschoben. E-Mail-Benachrichtigung.

2.2.7 Transport zwischen den Systemen

- *Es ist zu zeigen, wie die Integrität, Vollständigkeit etc. bei dem Transport zwischen verschiedenen Systemen sichergestellt werden?*
- *Art und Umfang der Transaktionskontrolle, um undefinierte Zustände zu vermeiden bzw. aufzulösen?*

IKS!

Kontrollziel	Kontrolle
Es muss hinreichend gewährleistet sein, dass Daten zwischen den Systemen nicht verloren gehen dürfen.	[…]

2.2.8 *Optional:* Signaturverifikation und Prüfprotokoll

- *Durch wen und welche Komponenten wird die Signatur verifiziert und was passiert mit dem Prüfprotokoll (wie das technisch erfolgt, wird später beschrieben)?*
- *Welche Angaben werden wie verifiziert (lokal, online)?*
    - *evtl. in Herstellererklärung*

2.2.9 Dokumenten – Ausgang

- *Welche Dokumente werden organisatorisch wie zum Kunden (oder Roaming-Partner) weitergeleitet (wie das technisch erfolgt, wird später beschrieben)?*
- *Bei Portalen ist wichtig zu beschreiben, wie der Kunde über die Rechnung informiert wird?*
- *Empfang bzw. Zugriff des Kunden sollte möglichst nachvollziehbar sein.*
- *Wie ist sichergestellt, dass die Übertragung des originalen Abrechnungsdokuments nur einmalig stattfindet?*
- *Ist durch Verfahren und Maßnahmen sichergestellt, dass jedes für einen Empfänger bestimmte Abrechnungsdokument auch an diesen übertragen wird?*
- *Wie ist sichergestellt, dass auf dem Übertragungsweg keine Änderungen an den Abrechnungsdokumenten stattfinden?*

IKS!

Kontrollziel	Kontrolle

Mustervorlage

Es muss hinreichend gewährleistet sein, dass die Übertragung des Dokuments nur einmal stattfindet.	[…]

2.2.10 Archivierung

- *Erfolgt Archivierung für Kunden oder eigene Absicherung?*
- *Was wird wie (z.B. Indexierung) und wo archiviert?*
- *Welche Maßnahmen wurden getroffen, um die Verfügbarkeit, Unveränderbarkeit und Lesbarkeit der Daten und Dokumente über die erforderliche Archivfrist sicherzustellen (z.B. gewählte Langfristformate)?*
- *Sofern für die Archivierung eine eigene Verfahrensdokumentation vorliegt, kann bzgl. der Details entsprechend verwiesen werden.*

IKS!

Kontrollziel	Kontrolle
Es muss hinreichend gewährleistet sein, dass alle Dokumente vollständig archiviert und über einen eindeutigen Index wiedergefunden werden.	[…]

2.2.11 Monitoring und Protokollierung

- *Welches Prozess-Monitoring (nicht System-Monitoring) gibt es?*
  hier ein Beispiel mit IKS-Bezug:

IKS!

Kontrollziel	Kontrolle
Alle ausgehenden Rechnungen müssen archiviert werden	Sobald der Archivimport fehl schlägt, erfolgt automatisch eine eMail-Benachrichtigung an den [V_eInvoice_Outbound]

- *Wie wird die Vollständigkeit über den Gesamtprozess sichergestellt (s.a. „Transport...“)*
- *Sind Maßnahmen implementiert, die sicherstellen, dass für alle abzurechnenden Geschäftsvorfälle ein Abrechnungsdokument erzeugt wird?*
- *Was wird wo durch wen und wie protokolliert?*

Mustervorlage

- *Wer kontrolliert Protokolle?*
  hier ein Beispiel mit IKS-Bezug:

IKS!

Kontrollziel	Kontrolle
Auch unkritische Meldungen (Warnungen) müssen, z.B. als Indizien für zukünftige Probleme, ausgewertet werden.	Die Kontrolle der Protokolle erfolgt im Rahmen des Monitoring durch die jeweils Verantwortlichen. Die Verantwortlichen sind definiert in ??

- *Was geschieht mit den verschiedenen Protokollen (Archivierung wo, von wem?)*

2.2.12 Fehlerhandling

- *Wer kümmert sich um welche organisatorischen bzw. Prozess-Fehler, z.B. fehlgeschlagene Zuordnungen, Daten nicht verarbeitbar, Signatur nicht verifizierbar, Dokumente in Fehlerqueues, Empfänger nicht erreichbar?*
- *Rein technische Fehler/Probleme werden bei der technischen Systemlösung beschrieben.*

2.2.13 Zurückziehen des Einverständnisses

- *Was passiert (organisatorisch und technisch) wenn Empfänger für alle oder bestimmte Rechnungsarten/-typen ihr Einverständnis zurückziehen?*
- *Wo gib es entsprechende Verfahrensanweisungen?*

2.3 Prozess für Rechnungsempfänger

- *Welchen weitergehenden Zielen unterliegt dieser Prozess?*
- *Was soll durch das Verfahren für Rechnungsempfänger genau erreicht werden?*

2.3.1 Verantwortung Prozess Rechnungsempfänger

Verantwortlich für die organisatorisch-technische Gestaltung des Prozesses ist:
[V_eInvoice_Outbound]

2.3.2 Einrichtung des Rechnungssteller

- *Woher weiß der Dienstleister, welche Rechnungssteller einzurichten sind?*
- *Wie, in welchen Systemen, von wem werden diese eingerichtet?*
- *Wie muss darüber hinaus eine Parametrisierung erfolgen, welche Bestandteile sind für alle Kunden gleich, welche sind individuell (diese könnte man z.B. gesondert als Anlagen anhängen)?*
- *Wie werden Tests mit den Kunden durchgeführt?*
  Siehe dazu auch 6.1 "Abnahme Kunde", evtl. kann hier ein Verweis bzgl. des Test eingebaut werden.
- *Welche Kontrollen, Protokollierungen existieren, um den Prozess nachvollziehen zu können?*
- *Evtl. Verweis auf Arbeitsanweisungen*

Mustervorlage

2.3.3 Prozessüberblick

Die folgende Grafik gibt einen Überblick über die organisatorische-technische Gestaltung des Prozesses. Eine genaue Erläuterung der technischen Abläufe und der beteiligten Komponenten erfolgt im Kapitel Technische Systemlösung.

[Grafik: Überblick Prozess Rechnungsempfänger]

ABB. 4 – ÜBERBLICK PROZESS RECHNUNGSEMPFÄNGER

- *Hier wäre eine kurze Erläuterung des Verfahrens – im Sinne eines Überblicks – sinnvoll. Details kommen dann in den Unterkapiteln bzw. später im technischen Teil.*
- *Hier sollte auch die Steuerung des Prozesses, z.B. über Workflow, aus Anwendungssicht beschrieben werden. Details kommen dann in den Unterkapiteln bzw. später im technischen Teil.*

2.3.4 Rechnungseingang

Im Vordergrund stehen in diesem und den folgenden Unterkapiteln die Funktionsweise und die Bedienung, aber alles kurz (keine detaillierte Bedienungsanleitung). Technische Details folgen im nächsten Kapitel.

In welcher Form kommen die Daten und/oder Dokumente an und wie werden sie erstbearbeitet.

2.3.5 Konvertierung und Auslese der Verarbeitungsinformationen

Was wird ausgelesen und aus welchem Grund konvertiert (wie das technisch erfolgt, wird später beschrieben)?

2.3.6 *Optional:* Signaturverifikation und Prüfprotokoll

Auch wenn Rechnungsdokument und Prüfprotokoll bereits beim Dienstleister erstellt und an den Empfänger unverändert weitergereicht werden, ist die Eingangsbearbeitung und Archivierung darzustellen.

Über bilaterale Absprachen ist optional eine erneute Prüfung für den Empfänger vereinbar.

- *Wenn Prüfung stattfindet: Wie ist sichergestellt, dass für alle eingehenden elektronischen Abrechnungsdokumente eine zeitgerechte Prüfung der elektronischen Signatur stattfindet?*

2.3.7 Transport zwischen den Systemen

- *Wenn Leistungen gleichzeitig für Sender und Empfänger erbracht werden, ist hier die genaue Darlegung der organisatorische und technische Trennung wichtig.*
- *Weiterhin ist zu zeigen, wie die Integrität, Vollständigkeit etc. sichergestellt werden?*
- *Art und Umfang der Transaktionskontrolle, um undefinierte Zustände zu vermeiden bzw. aufzulösen?*

Mustervorlage

2.3.8 Dokumenten – Ausgang

- *Welche Dokumente werden organisatorisch wie zum Kunden (oder Roaming-Partner) weitergeleitet (wie das technisch erfolgt, wird später beschrieben)?*
- *Wie ist sichergestellt, dass der Kunde alle Rechnungen empfängt bzw. angezeigt bekommt?*
- *Wie ist sichergestellt, dass keine Rechnungen mehrfach geliefert wird?*

2.3.9 Archivierung

- *Erfolgt Archivierung für Kunden oder eigene Absicherung?*
- *Was wird wie (z.B. Indexierung) und wo archiviert?*
- *Welche Maßnahmen wurden getroffen, um die Verfügbarkeit, Unveränderbarkeit und Lesbarkeit der Daten und Dokumente über die erforderliche Archivfrist sicherzustellen (z.B. gewählte Langfristformate)?*
- *Sofern für die Archivierung eine eigene Verfahrensdokumentation vorliegt, kann bzgl. der Details entsprechend verwiesen werden.*

2.3.10 Monitoring und Protokollierung

- *Welches Prozess-Monitoring (nicht System-Monitoring) gibt es?*
- *Was wird wo durch wen und wie protokolliert?*
- *Wer kontrolliert Protokolle?*
  hier ein Beispiel mit IKS-Bezug:

IKS!	Kontrollziel	Kontrolle
	Auch unkritische Meldungen (Warnungen) müssen, z.B. als Indizien für zukünftige Probleme, ausgewertet werden.	Die Kontrolle der Protokolle erfolgt im Rahmen des Monitoring durch die jeweils verantwortlichen.

- *Was geschieht mit den verschiedenen Protokollen (Archivierung wo, von wem?)*

2.3.11 Fehlerhandling

- *Wer kümmert sich um welche organisatorischen bzw. Prozess-Fehler, z.B. fehlgeschlagene Zuordnungen, Daten nicht verarbeitbar, empfangene Signatur ungültig, Prüfprotokoll fehlt, Empfänger nicht erreichbar?*
- *Welche Verfahrensanweisungen gibt es für diese Fälle?*
- *Rein technische Fehler/Probleme werden bei der technischen Systemlösung beschrieben*

2.3.12 Zurückziehen des Einverständnisses

- *Was passiert (organisatorisch und technisch) wenn Rechnungssteller für alle oder bestimmte Rechnungsarten/-typen ihr Einverständnis für den elektronischen Rechnungsaustausch zurückziehen?*
- *Wo gib es entsprechende Verfahrensanweisungen?*

Mustervorlage

2.4 Mandantenfähigkeit

- *Wie differenzieren Sie zwischen den Mandanten?*
- *Für eine Dienstleistungslösung ist Mandantenfähigkeit essentiell, da Nachvollziehbarkeit, Zugriffsschutz etc. je Mandant separat zu zeigen sind. Dies umfasst daher nicht nur Zugriffsberechtigungen, sondern auch Protokolle, Archive und ggf. auch unterschiedliche Konfigurationen, z.B. aufgrund unterschiedlicher Service-Levels*

2.5 Auslagerung/Entsorgung gemäß BDSG

Verantwortlich für die Einhaltung des BDSG ist [V_BDSG].

- *Wie erfolgt die Löschung von Daten/Rechnungen/Protokollen etc. nach Ablauf der Aufbewahrungsfrist, z.B. wegen BDSG?*
- *Sofern der Prozess an den unterschiedlichen Systemen (oder unterschiedlichen Standorten) nicht gleichartig verläuft, ist entsprechend zu differenzieren.*

Die generellen Maßnahmen zur Einhaltung des BDSG bei den beteiligten Komponenten ist unter „Datenschutz BDSG“ beschrieben.

Mustervorlage

3 Technische Systemlösung

Nach dem wir den prinzipiellen und organisatorischen Ablauf aufgezeigt haben, widmet sich dieses Kapitel der technischen Umsetzung mit den IT-Systemen. Bevor die technische Beschreibung folgt, geben wir einen Überblick über die beteiligten Komponenten und ihr Zusammenspiel.

[Grafik: Netzwerkplan eInvoice-Systeme]

ABB. 5 – NETZWERKPLAN EINVOICE-SYSTEME

- *Hier dann kurze verbale Erläuterung der Grafik.*
- *Ggf. auch zwei Grafiken/Erläuterungen für R.steller und R.empfänger.*

Die Details der beteiligten Komponenten (Versionen etc.) finden sich in den Datenblättern im Anhang unter Configuration Management.

Für den Betrieb des eInvoicing ist verantwortlich: [V_Oper_eInvoice]

3.1 Technische Lösung für Rechnungssteller

Für die technische Umsetzung des Verfahrens für Rechnungssteller ist verantwortlich: [V_Oper_eInvoice_out]

- *Für R.steller und R.empfänger sind hier eigene Kapitel vorgesehen. Sofern die Überdeckung zu groß ist, kann das ggf. zusammen beschrieben werden. Es ist aber die geforderte „organisatorisch-technische Trennung“ (s.o.) zu bedenken.*
- *Auch für die Unterkapitel gilt:*
  - *Alle Details, wie Versionsangaben, Abhängigkeiten zu Betriebssystemen etc. sollten über die Datenblätter im Anhang dokumentiert werden. Hier sollten nur die Komponenten und ihr Zusammenspiel bzw. ihre Abhängigkeiten beschrieben werden.*
  - *Genutzte Formate, Schnittstellen etc. sollten hier ebenfalls genannt, aber über den Anhang (oder externe Dokumente) gepflegt werden.*

3.1.1 Eintreffen der Daten im Unternehmen

- *Übertragungsprotokolle, Schnittstellen, Formate in denen Daten empfangen werden (ggf. Verweise auf detailliertere Beschreibungen oder Standards, auch außerhalb dieses Dokumentes)*
- *Komponenten sowie benötigte Infrastruktur-Voraussetzungen?*

3.1.2 Konvertierung

- *Komponenten und Formate in denen Daten konvertiert werden (ggf. Verweise auf detailliertere Beschreibungen oder Standards, auch außerhalb dieses Dokumentes)*
- *Der Beleg darf keinen ausführbaren Code enthalten, da damit die Integrität nicht mehr gewährleistet wäre.*

Mustervorlage

3.1.3 *Optional:* Signierung

- *Hard- und Software-Komponenten und Formate mit denen Dokumente & Daten signiert werden (ggf. Verweise auf detailliertere Beschreibungen oder Standards, auch außerhalb dieses Dokumentes)*
- *Genutzte Formate und Schnittstellen sowie benötigte Infrastruktur-Voraussetzungen?*
- *Was genau wird signiert (z.B. muss bei PDF nicht zwangsweise der gesamte Inhalt signiert sein)?*
- *Nachweis der Zulässigkeit der Komponenten (z.B. über Verweise auf Herstellererklärung oder Web-Site der BNetzA)?*
- *Wie erfolgt die Zuordnung Signatur zu Rechnung?*

3.1.4 Transport zwischen den Systemen

- *Genutzte Protokolle, Formate und Schnittstellen sowie benötigte Infrastruktur-Voraussetzungen für den Datenaustausch zwischen den Systemen?*
- *Art und Umfang der Datenflusskontrolle*
- *Ggf. Workflow-Steuerung*

3.1.5 *Optional:* Verifikation

[Um sicherzustellen, dass die Signaturkarte nicht gesperrt wurde oder um dem Empfänger zusätzlich ein Verifikationsprotokoll zusenden zu können, kann die Verifikation bereits beim Rechnungssteller erfolgen]

- *Hard- und Software-Komponenten und Formate mit denen Signaturen verifiziert werden (ggf. Verweise auf detailliertere Beschreibungen oder Standards, auch außerhalb dieses Dokumentes)*
- *Genutzte Formate und Schnittstellen sowie benötigte Infrastruktur-Voraussetzungen?*
- *Nachweis der Zulässigkeit der Komponenten (z.B. über Verweise auf Herstellererklärung oder Web-Site der BNetzA)?*
- *Wie erfolgt die Zuordnung Prüfprotokoll zu Rechnung?*

3.1.6 Indizierung und Datenbank

- *Welche Daten werden in eigenen Systemen zu welchem Zweck, wie lange verwaltet?*
- *Hard- und Software-Komponenten, genutzte Formate und Schnittstellen sowie benötigte Infrastruktur-Voraussetzungen?*

3.1.7 Visualisierung und Reproduktion

- *Wie kann Visualisierung erfolgen?*
- *Hard- und Software-Komponenten, genutzte Formate und Schnittstellen sowie benötigte Infrastruktur-Voraussetzungen?*

Mustervorlage

3.1.8 Protokollierung

- *Welche Systemprotokolle sind zu Nachweiszwecken wo, für wen verfügbar?*
- *Was passiert mit diesen Protokollen (Prüfung, Archivierung. …)?*

3.2 Technische Lösung für Rechnungsempfänger

Für die technische Umsetzung des Verfahrens für Rechnungsempfänger ist verantwortlich: [V_Oper_eInvoice_in]

- *Für R.steller und R.empfänger sind hier eigene Kapitel vorgesehen. Sofern die Überdeckung zu groß ist, kann das ggf. zusammen beschrieben werden. Es ist aber die geforderte „organisatorisch-technische Trennung" (s.o.) zu bedenken.*
- *Auch für die Unterkapitel gilt:*
  - *Alle Details, wie Versionsangaben, Abhängigkeiten zu Betriebssystemen etc. sollten über die Datenblätter im Anhang dokumentiert werden. Hier sollten nur die Komponenten und ihr Zusammenspiel bzw. ihre Abhängigkeiten beschrieben werden.*
  - *Genutzte Formate, Schnittstellen etc. sollten hier ebenfalls genannt, aber über den Anhang (oder externe Dokumente) gepflegt werden.*

3.2.1 Eintreffen der Daten im Unternehmen

- *Übertragungsprotokolle, Schnittstellen, Formate in denen Daten empfangen werden (ggf. Verweise auf detailliertere Beschreibungen oder Standards, auch außerhalb dieses Dokumentes)*
- *Komponenten sowie benötigte Infrastruktur-Voraussetzungen?*

3.2.2 Konvertierung

- *Komponenten und Formate in denen Daten konvertiert werden (ggf. Verweise auf detailliertere Beschreibungen oder Standards, auch außerhalb dieses Dokumentes)*

3.2.3 *Optional:* Signierung

- *Hard- und Software-Komponenten und Formate mit denen Dokumente & Daten signiert werden (ggf. Verweise auf detailliertere Beschreibungen oder Standards, auch außerhalb dieses Dokumentes)*
- *Genutzte Formate und Schnittstellen sowie benötigte Infrastruktur-Voraussetzungen?*
- *Nachweis der Zulässigkeit der Komponenten (z.B. über Verweise auf Herstellererklärung oder Web-Site der BNetzA)?*
- *Wie erfolgt die Zuordnung Signatur zu Rechnung?*

3.2.4 Transport zwischen den Systemen

- *Genutzte Protokolle, Formate und Schnittstellen sowie benötigte Infrastruktur-Voraussetzungen für den Datenaustausch zwischen den Systemen?*
- *Art und Umfang der Datenflusskontrolle*
- *Ggf. Workflow-Steuerung*

Mustervorlage

3.2.5 *Optional:* Verifikation

- *Soweit Verifikation erforderlich, die gleichen Punkte wie bei Signierung*
- *Ansonsten muss hier nur die Verfügbarkeit des Prüfprotokolls sichergestellt werden*

3.2.6 Indizierung und Datenbank

- *Welche Daten werden in eigenen Systemen zu welchem Zweck, wie lange verwaltet?*
- *Hard- und Software-Komponenten und Formate mit denen Komponenten, genutzte Formate und Schnittstellen sowie benötigte Infrastruktur-Voraussetzungen?*

3.2.7 Visualisierung und Reproduktion

- *Wie kann Visualisierung erfolgen?*
- *Hard- und Software-Komponenten und Formate mit denen Komponenten, genutzte Formate und Schnittstellen sowie benötigte Infrastruktur-Voraussetzungen?*

3.2.8 Protokollierung

- *Welche Systemprotokolle sind zu Nachweiszwecken wo, für wen verfügbar?*
- *Was passiert mit diesen Protokollen (Prüfung, Archivierung. …)?*

3.3 Systembeschreibung

Nach der Beschreibung der Lösung, bei der die Systeme nur in ihrer Hauptfunktion und ihrem Zusammenwirken dargestellt wurden, erfolgt hier die technische Beschreibung der einzelnen Systeme so detailliert wie notwendig. Dazu gehören beispielsweise die folgenden Aspekte:

- *Um welche Art System handelt es sich, z.B. Linux-Server für Signaturerstellung?*
- *Welche Daten kommuniziert es wie mit anderen Systemen?*
- *Wie das System in das Betriebskonzept, z.B. Health Check, Datensicherung, Administration eingebunden?*
- *Wie ist das System in die Netzwerk- und Sicherheitsinfrastruktur eingebunden?*

Konfigurationsdetails, die sich schnell ändern können, z.B. Versionen der installierten Software, aber auch der verantwortliche Systembetreuer sollten im entsprechenden Datenblatt beschrieben werden, auf das hier verwiesen wird.

Die Beschreibung der einzelnen Systeme kann somit relativ kurz gehalten werden.

Bei eInvoice sind in jeden Fall zu beschreiben:

- *Genutzte Applikationen*
- *Wenn vorhanden: Signatur-Server + Verifikations-Server*

Mustervorlage

- *Kommunikations-Server*
- *Archiv*

3.3.1 Standard-Softwarekomponenten

Die o.g. Punkte sollten für alle am technischen eInvoice-Prozess beteiligten Standard-Software-Komponenten kurz dargestellt werden.

3.3.2 Individuelle Programmteile

Die o.g. Punkte sollten für alle am technischen eInvoice-Prozess beteiligten Individual-Komponenten kurz dargestellt werden.

Wichtig ist in diesem Zusammenhang vor allem auch die Regelungen zur Verantwortung bei Fehlern und für Weiterentwicklungen individueller Software.

3.3.3 Netzwerke

Die o.g. Punkte sollten für alle am technischen eInvoice-Prozess beteiligten Netzwerk-Komponenten kurz dargestellt werden.

Sofern das Standard-Netzwerk verwandt wird und dies bereits in einem anderem Dokument beschrieben ist, ist ein Verweis ausreichend.

3.3.4 Hardware

Die o.g. Punkte sollten für alle am technischen eInvoice-Prozess beteiligten Hardware-Komponenten kurz dargestellt werden.

Sofern, z.B. für Server, Standardkomponenten verwandt werden und diese bereits in einem anderen Dokument beschrieben sind, ist ein Verweis ausreichend.

3.3.5 Schnittstellen

Hier erfolgen die technischen Beschreibungen der Schnittstellen für den Dokumenten- und Datenaustausch, ggf. inkl. Signatur, Prüfprotokoll etc..

Schnittstelle zur Übergabe von Rechnungen vom Kunden

Schnittstelle zur Übergabe von Rechnungen eingehend

Mustervorlage

Schnittstelle zur Übergabe von Rechnungen ausgehend

Schnittstelle zur Übergabe von Rechnungen an das Archiv

3.4 Migration

- *Welche technischen Maßnahmen wurden getroffen, um die Verfügbarkeit, Unveränderbarkeit und Lesbarkeit der Daten und Dokumente über die erforderliche Archivfrist sicherzustellen (z.B. gewählte Langfristformate)?*
- *Welche Maßnahmen wurden getroffen, um eine evtl. später erforderliche Migration der Dokumente und Daten auf andere Server, Betriebssysteme, Applikationen problemlos zu gestalten?*
- *Dabei ist vermutlich zwischen den folgenden Hauptkomponenten zu differenzieren*

Applikationen

Optional: **Signatur-Systeme**

Archiv

Mustervorlage

4 Sicherheit (physisch und logisch)

Hier beschreiben wir die Maßnahmen, die physisch (z.B. baulich) und logisch (z.B. Zugriffsberechtigung) ergriffen wurden, um Änderungen und Verlust von Dokumenten und Daten vorzubeugen. Solche Verluste können verursacht sein durch technische Ausfälle oder auch durch fahrlässiges oder vorsätzliches Handeln.

Diese Maßnahmen werden ergänzt durch die diversen Kontrollen, die vor allem im Prozess zu finden sind. Die Gesamtheit aller Sicherheitsmaßnahmen wird auch als internes Kontrollsystem, IKS bezeichnet. Die einzelnen Kontrollen des IKS sind in dieser Verfahrensdokumentation durch „IKS!“ gekennzeichnet. Die entsprechende Zusammenfassung findet sich im nächsten Kapitel.

4.1 Allgemeines IT-Sicherheitskonzept

- *Wer ist für IT-Sicherheit verantwortlich?*
- *Wie ist generell die Sicherheit der Daten gegen Verlust und/oder Manipulation aufgrund von Vorsatz oder technischen Problemen konzipiert (Policies)?*
- *Welche Richtlinien sind verfügbar?*

4.1.1 IT-Versicherungen

- *Welche speziellen IT-Versicherungen wurden abgeschlossen?*
- *Was ist damit abgesichert?*
- *Wer ist dafür verantwortlich?*

4.1.2 Datenschutz BDSG

Verantwortlich für die Einhaltung des BDSG ist [V_BDSG].

- *Welche Maßnahmen sind für die generelle Einhaltung des Datenschutzes gemäß BDSG getroffen?*

4.1.3 Netzzugriffe

Sofern das Standard-Sicherheitsnetzwerk verwandt wird und dies bereits in einem anderem Dokument beschrieben ist, ist ein Verweis ausreichend.

- *Wie ist sichergestellt, dass Unbefugte keinen Zugriff auf/über das Netzwerk erhalten (Firewall, VPN etc.?*
- *Wie erfolgt das Monitoring der Netzzugriffe (z.B. Auditing, Protokollierung)?*
- *Wer verfolgt wie evtl. Einbruchsversuche bzw. unbefugte Zugriffe?*
- *Bei der Nutzung von Web-Servern sind Maßnahmen gegen das Spoofing zu ergreifen und zu beschreiben.*

Mustervorlage

IKS!

Kontrollziel	Kontrolle
Es muss hinreichend gewährleistet sein, dass keine unbefugten Zugriffe auf das Netzwerk erfolgen.	[…]

4.2 Benutzerverwaltung und Berechtigungskonzept

Verantwortlich für die Einhaltung des BDSG ist [V_User].

- *Wie ist die Benutzerverwaltung im beschriebenen Verfahren organisatorisch und technisch geregelt?*

4.2.1 Authentifizierung und Passwort-Handling

- *Wie ist das Login-Verfahren?*
- *Werden zentrale Verzeichnisse genutzt?*
- *Welche Regeln (orga./techn.) gibt es für das Passwort-Handling?*
- *Wie erfolgt Vergabe und Entzug von Passwörtern?*

4.2.2 Zuordnung Zugriffsrechte zu Benutzergruppen

Hier wird das Verfahren zur Vergabe von Zugriffsrechten beschrieben. Die konkret vergebenen Rechte auf Applikationen und Server finden sich im Anhang.

- *Wie – und wie differenziert – werden in diesem Prozess Zugriffsrechte auf die Dokumente und Daten zugeordnet?*

4.2.3 Schutz sonstiger Ressourcen

- *Wie – und wie differenziert - ist der Zugriff auf andere relevante Ressourcen (z.B. SmartCard) geschützt?*

4.3 *Optional:* Zertifikatshandling

Die für die Signaturerstellung benötigten Zertifikate und Signaturschlüssel werden bezogen von dem Zertifizierungsdiensteanbieter *[Anbieter_SSEE]*

Zum Einsatz kommt das Produkt *[HW_SSEE],* das unter „Datenblätter Hardware“ genauer beschrieben wird.

Zertifikate sind verfügbar für die folgenden Personen:

[V_SigZert1]

Mustervorlage

[V_SigZert2]

[V_SigZert3]

4.3.1 *Optional:* Verfahren zur Beantragung neuer Zertifikate

Ggf. kann hier auf ein separates Dokument, z.B. eine bestehende Arbeitsanweisung verwiesen werden.

Neben dem Verfahrens selbst, sollte hier auch beschrieben werden, was genau beantragt wird, z.B. Werden Attribute, Pseudonyme im Zertifikat verwendet: Wenn ja, mit welchem Inhalt?

4.3.2 *Optional:* Verfahren bei Verlust Zertifikat

Sperrung von Zertifikaten: Wer im Unternehmen ist sperrberechtigt, Arbeitsanweisung (Ablauf) Sperrung, Aufbewahrung Sperrpasswort, ...

IKS!

Kontrollziel	Kontrolle
Es muss hinreichend gewährleistet sein, dass im Bedarfsfall Zertifikate umgehend gesperrt werden.	Arbeitsanweisung vorhanden, Sperrberechtigte identifiziert, Liste mit Karten + Nummern vorhanden, Vorgehen bekannt.

4.3.3 *Optional:* Verfahren bei Ablauf Zertifikat

4.3.4 *Optional:* Verfahren bei Wechsel Zertifikatsinhaber

4.4 Ausfallsicherheit

4.4.1 Generelles und Virenschutz

- *Welche Maßnahmen sind für die Erhaltung der Datenintegrität getroffen (z.B. Viren-Scanner, inkl. Update Policy)?*
- *Sofern die Informationen zu Virenschutz in Organisations- und Betriebshandbüchern enthalten sind, sollten hier exakte (mit Kapitelnr.) Referenzen/Verweise eingebaut werden.*
- *Soweit differenzierte Verfahren, z.B. für Client- bzw. Server-Systeme eingesetzt werden, sind die hier relevanten klar zu spezifizieren.*

4.4.2 Maßnahmen zur Verfügbarkeitsoptimierung

- *Welche Maßnahmen sind für die Verfügbarkeit der Funktionalität bei Ausfall einzelner Komponenten getroffen (z.B. Cluster, Spiegelung, …)?*

Mustervorlage

4.4.3 Datensicherung und Recovery

Verantwortlich für die Datensicherung ist [V_Backup].

- *Welche Maßnahmen sind für die Erhaltung der Datenintegrität nach Ausfall einzelner Komponenten getroffen?*
- *Nimmt die Gesellschaft eine Auslagerung wichtiger Sicherungsbestände außerhalb des Rechnerbereichs vor? Backup und Recovery / Disaster Recovery:*
- *Sind die zu sichernden Daten auf Basis ihrer Notwendigkeit für den Betrieb der Lösung identifiziert worden?*
- *Sind angemessene Datensicherungs- und Auslagerungsverfahren definiert, um sicherzustellen, dass die Daten im Bedarfsfall verfügbar sind?*
- *Welche Systeme werden eingesetzt, welche Prozesse angewendet?*
- *Evtl. wieder Verweis auf Betriebshandbuch o.ä.*

IKS!

Kontrollziel	Kontrolle
Es muss hinreichend gewährleistet sein, dass Recoveries jederzeit fehlerfrei ablaufen.	Vorgehen dokumentiert, Verantwortliche festgelegt, Recovery-Tests für Systeme … monatlich, dokumentiert.

4.5 Standorte und Zugangsregelung

Die eInvoice-Prozesse nutzen die RZ-Infrastruktur am Standort [L_Name].

Verantwortlich für die Standorte und Zugangsregelung ist [V_Location].

4.5.1 Feuerschutz/Elementarschäden

- *Sind in der Betriebsstätte der Komponenten angemessene Maßnahmen zum Schutz der Systeme vor Elementarschäden (Feuer, Wasser) installiert?*
- *Welche Maßnahmen zum Brandschutz wurden getroffen (ggf. je Standort)?*
- *Sofern die Informationen zu den folgenden Punkten in Organisations- und Betriebshandbüchern enthalten sind, sollten hier exakte (mit Kapitelnr.) Referenzen/Verweise eingebaut werden.*

4.5.2 Stromversorgung

- *Welche Maßnahmen für Stromausfälle wurden getroffen (ggf. je Standort)?*

4.5.3 Kühlanlagen

- *Welche Klimaanlagen für EDV- und Serverräume werden eingesetzt um einen störungsfreier Betrieb (z. B. redundantes-Klimasystem) zu gewährleisten (ggf. je Serverraum)?*

Mustervorlage

4.5.4 Zugangsregelung Gebäude

- *Wie ist der Zugang zu den Firmengebäuden im Detail geregelt, z.B. für Ausstellung Mitarbeiterausweise?*
- *Sind Verfahren zur Vergabe und Überprüfung der Zutrittsberechtigungen zur Betriebsstätte der IT-Systeme definiert und werden diese eingehalten?*

4.5.5 Zugangsregelung IT-Abteilung

- *Wie ist der Zugang zur IT im Detail geregelt?*

4.5.6 Zugangsregelung Rechenzentrum

- *Wie ist der Zugang zum RZ im Detail geregelt?*

4.5.7 Vergabe von Zugangsberechtigungen

- *Wer vergibt wie die entsprechenden Berechtigungen?*
- *Was passiert wenn Berechtigte ausscheiden?*

Mustervorlage

5 Technischer Betrieb

5.1 Organisation des eInvoice-Betriebs

- *Wie ist der Betrieb generell organisiert (Auf- und Ablauforganisation)?*
- *Ist ein geregelter IT-Betrieb anhand eines definierten Verfahrens zum geordneten Regelbetrieb gewährleistet*
- *Wer ist für die HW-/SW-Komponenten als Admin verantwortlich? Vertretungsregelung?*

5.1.1 Service Level Management

- *Welche Service Levels, z.B. Reaktionszeiten, Erreichbarkeiten werden angeboten?*
- *Welche Service Levels, z.B. Reaktionszeiten sind mit den Komponentenanbietern vereinbart?*

IKS!

Kontrollziel	Kontrolle
Es muss hinreichend gewährleistet sein, dass für jede Hard- und Software ein SLA abgeschlossen wird.	[…]

5.1.2 Qualifikationsmaßnahmen

- *Schulung der Nutzer, Administratoren und Service-Mitarbeiter*
- *Welche Verfahrensbeteiligten gibt es und wie werden diese auf Ihre Aufgabe vorbereitet?*
- *Sofern Kunden direkt mit dem System kommunizieren, sind die Qualifikationsmaßnahmen ebenfalls zu beschreiben und vertraglich zu vereinbaren.*

5.1.3 Sonstiges Training

- *Welche sonstigen Trainingsmaßnahmen, z.B. generelle Unterweisungen Datenschutz, Umgang mit Passwörtern o.ä. wurden durchgeführt?*

5.2 Availability and Service Continuity

- *Wer überwacht wie den Betrieb generell, z.B. Einhaltung der Betriebsbedingungen, Analyse Fehlerprotokolle etc.?*
- *Welche Maßnahmen werden ergriffen, um sicherzustellen, dass eine Nichtverfügbarkeit der IT-Systeme erkannt wird?*
- *Welche Verfahrensanweisungen gibt es?*

5.2.1 Monitoring und Health Check

- *Welche Monitoring-Infos sind zu Nachweiszwecken wo, für wen verfügbar?*
- *Was passiert mit diesen Protokollen (Prüfung, Archivierung. …)?*

Mustervorlage

5.2.2 Wartungsverträge

- *Welche Wartungsverträge gibt es für die beteiligten Komponenten?*
- *Wer ist für diese Verträge verantwortlich?*

5.2.3 Vorbeugende Wartung

- *Welche Wartung ist für die an diesem Prozess beteiligten Komponenten vorgesehen?*
- *Wer ist verantwortlich?*

5.2.4 Anweisungen zum generellen Verhalten bei Störungen (Notfallhandbuch)

5.3 Incident and Problem Management

5.3.1 Notfall

- *Wie kritisch ist der Prozess für das Unternehmen?*
- *Wer ist verantwortlich (z.B. außerhalb normaler Zeiten)?*
- *Wer ist für K-Fall-Bewertung für diesen Prozess verantwortlich?*
- *Welche K-Fall-Szenarien sind wie und wo beschrieben?*
- *Evtl. Verweis auf generelles Notfallhandbuch*

5.3.2 Recovery bei Störungen der Komponenten dieses Prozesses

- *Was ist bei dem Recovery zu beachten, z.B. bestimmte Reihenfolge des Hochfahrens?*
- *Evtl. Verweis auf eine Arbeitsanweisung*

5.3.3 Probleme der Anwender

Sofern die Prozesse nicht komplett automatisiert erfolgen, ist zu definieren, wo sich Nutzer bei Problemen hin wenden können. Wenn generelle Strukturen (z.B. UHD) verwendet werden, kann auf deren Dokumentationen verwiesen werden.

- *Wer ist für Probleme der Nutzer dieses Prozess verantwortlich (z.B. UHD)?*
- *Wie ist der Ablauf bei Incident und Problem Management bzw. wo sind entsprechende Dokumentationen?*

5.3.4 Fehlerhandling

Fehlerhandling sollte bereits bei der Beschreibung der Prozesse dargestellt werden. Hier ist daher nur das prozessübergreifende Handling zu beschreiben.

Mustervorlage

6 Internes Kontrollsystem (IKS)

Ein Dienstleistungsunternehmen ist ein rechtlich vom auslagernden Unternehmen getrenntes Unternehmen, das eine oder mehrere betriebliche Funktionen des auslagernden Unternehmens in dessen Auftrag selbständig durchführt. Mit der Auslagerung dieser Funktionen erlangt das interne Kontrollsystem des Dienstleistungsunternehmens für die Beurteilung der Frage Bedeutung, ob sich aus der Ausgestaltung der Kontrollen Risiken ergeben, die auf die Rechnungslegung eines die Dienstleistung auslagernden Unternehmens Auswirkungen haben können.

Führen Dienstleistungsunternehmen im Auftrag von auslagernden Unternehmen in Bereichen der Rechnungslegung Vorgänge eigenständig durch, entbindet dies die auslagernden Unternehmen nicht von ihrer Verantwortung für die ausgelagerten Vorgänge und deren ordnungsgemäße Abbildung in der Rechnungslegung. Aus diesem Grund ist das von den Dienstleistungsunternehmen eingerichtete dienstleistungsbezogene interne Kontrollsystem insbesondere für die Jahresabschlussprüfungen der auslagernden Unternehmen von Bedeutung.

Die Beurteilung des internen Kontrollsystems der auslagernden Unternehmen muss daher auch das dienstleistungsbezogene interne Kontrollsystem der Dienstleistungsunternehmen umfassen. Die Beurteilung des dienstleistungsbezogenen internen Kontrollsystems kann dabei auch durch einen anderen Wirtschaftsprüfer als den des auslagernden Unternehmens erfolgen. Der einer solchen Prüfung zugrunde liegende internationale Prüfungsstandard ist der des American Institute of Certified Public Accountants (AICPA) „Statement on Auditing Standards No. 70, Service Organizations (SAS 70)“, der in Deutschland mit dem Prüfungsstandard 951 des Instituts der Wirtschaftsprüfer (IDW) umgesetzt wurde.

Der Gegenstand dieser Prüfung ist das in einer Beschreibung dargestellte dienstleistungsbezogene interne Kontrollsystem. Verantwortlich für den Inhalt der Beschreibung sind die gesetzlichen Vertreter des Dienstleistungsunternehmens. Zusammen mit der Beschreibung des internen Kontrollsystems können diese Prüfungsberichte im Bedarfsfall an die Wirtschaftsprüfer der auslagernden Unternehmen herausgegeben werden.

Da diese Art von Prüfung an Relevanz gewinnen wird, sei an dieser Stelle empfohlen, die Erstellung einer Verfahrensdokumentation anhand dieses Musters mit der Beschreibung des dienstleistungsbezogenen internen Kontrollsystems zu kombinieren.

Allgemeine Definition „Internes Kontrollsystem“

Das interne Kontrollsystem (IKS) umfasst gem. IDW PS 260 die von einer Unternehmensleitung eingeführten und implementierten Grundsätze, Verfahren und Maßnahmen, die auf die organisatorische Umsetzung der Entscheidungen der Unternehmensleitung hinsichtlich der folgenden Ziele gerichtet sind:

- *Sicherung der Wirksamkeit und Wirtschaftlichkeit der Geschäftstätigkeit einschließlich des Schutzes des Vermögens und der Verhinderung (und ggf. Aufdeckung) von Vermögensschädigungen.*
- *Verlässlichkeit und Ordnungsmäßigkeit der internen und externen Rechnungslegung.*
- *Einhaltung der für das Unternehmen einschlägigen Gesetze und sonstigen Vorschriften und Verordnungen.*

Konzeption, Implementierung, Beaufsichtigung und laufende Anpassung sowie Fortentwicklung eines der jeweiligen Größe und Komplexität sowie Rechts- und Organisationsform des Unternehmens angemessenen IKS obliegt der Geschäftsleitung.

Im Rahmen der Rechnungslegung und des Controlling schließt das IKS das Rechnungslegungssystem und das Buchführungssystem ein. Das IKS besteht aus Regelungen zur

- *Steuerung der Unternehmensaktivitäten (sog. internes Steuerungssystem), und*
- *Überwachung der Einhaltung dieser Regelungen (sog. internes Überwachungssystem). Dazu gehören*
  - *prozessintegrierte Überwachungsmaßnahmen (organisatorische Überwachungsmaßnahmen und die verschiedenen Formen von Kontrollen) und*
  - *prozessunabhängige Überwachungsmaßnahmen (die vor allem durch die Interne Revision oder das Internal Audit abgedeckt werden).*

Mustervorlage

Beschreibung des dienstleistungsbezogenen internen Kontrollsystems

*Die Beschreibung des dienstleistungsbezogenen internen Kontrollsystems hat eine Darstellung der Kontrollziele und der zur Erreichung der **Kontrollziele** eingerichteten **Kontrollen** in den jeweiligen Komponenten des dienstleistungsbezogenen internen Kontrollsystems zu beinhalten, die sich auf das interne Kontrollsystem eines auslagernden Unternehmens direkt auswirken können.*

Es ist empfehlenswert, sich bei der Darstellung der Kontrollziele und deren Kontrollen an einem bestehenden Framework, wie z. B. COSO oder CoBIT zu orientieren.

Beispiel einer Beschreibung des dienstleistungsbezogenen internen Kontrollsystems

Kontrollziel	Kontrolle
Change Management: Es muss hinreichend gewährleistet sein, dass Entwicklungen/Änderungen im System genehmigt, getestet, freigegeben, korrekt implementiert und dokumentiert werden.	Programmänderungen werden mittels eines Formulars beantragt und durch Unterschrift des Vorgesetzten genehmigt. Es existiert eine Entwicklungs-, Test- und Produktivlandschaft. Tests werden anhand von Checklisten durchgeführt. Freigabe und Dokumentation mittels Projektmanagement-Software. Vier-Augen-Prinzip.
Systemzugriff: Es muss hinreichend gewährleistet sein, dass der Zugang zu Programmen und Daten ausschließlich autorisierten Personen vorbehalten ist.	Formular zur Anlage, Änderung, Sperrung von Usern. Direkte Zusammenarbeit mit der Personalabteilung. Genehmigungsverfahren. Berechtigungskonzept auf Gruppenbasis. Monatliche Kontrollen der Berechtigungskonzepte.
Physischer Zugang: Es muss hinreichend gewährleistet sein, dass der Zugang zum Rechenzentrum, zu relevanten Servern, zu Speichermedien und Systemdokumentationen ausschließlich autorisierten Personen vorbehalten ist.	Zugangskontrollen durch Chipkarten, vergeben an ausgewählte IT-Mitarbeiter. Protokollierung, Kameraüberwachung.
Prozess E-Billing: Es muss hinreichend gewährleistet sein, dass alle Rechnungen nur einmal den E-Billing-Prozess durchlaufen. Lücken dürfen ebenfalls keine entstehen.	Eingehende Dokumente werden in einer Datenbank eingetragen. Nachdem der Prozess durchlaufen ist, wird in der Datenbank ein Ausgangsflag gesetzt. Für Prozessdurchlauf bleiben 2 Stunden, danach werden nicht bearbeitete Einträge automatisch identifiziert im Rahmen eines Monitoring gemeldet.
Signaturkarten: Es muss hinreichend gewährleistet sein, dass die Signaturkarten stets unter der alleinigen Kontrolle des Signaturkarteninhabers bleiben.	Jeder Signaturkarteninhaber hat eine eigene Geldkassette, in der derzeit nicht verwendete Karten aufbewahrt werden. Kassetten werden darüber hinaus im Tresor aufbewahrt. Schlüssel trägt jeder Mitarbeiter am Körper. Aktive Karten, die sich im Kartenleser befinden, sind in einzelnen Serverracks abgeschlossen. Schlüssel trägt jeder Mitarbeiter am Körper.
Kundenverwaltung: Es muss hinreichend gewährleistet sein, dass Kundenstammdaten nur von autorisierten Mitarbeitern angelegt, eingesehen und geändert wer-	Beschränkung über Berechtigungskonzept. Änderungen sind vorab mit Unterschrift genehmigen zu lassen. Vier-

Angaben sind nur beispielhaft zur Verdeutlichung der Intention.

Mustervorlage

den können. Solche Vorgänge müssen genehmigt werden.	Augen-Prinzip.
usw.	usw.

*In dieser Musterverfahrensdokumentation wird an mehreren Stellen mit dem Zeichen „**IKS!**“ darauf hingewiesen, wenn die Darstellung eines Kontrollziels und einer Kontrolle sinnvoll erscheint. Diese Hinweise sind jedoch keineswegs erschöpfend, sondern sollen nur als Beispiele dienen.*

Mustervorlage

7 Test

Für die Tests der eInvoice-Lösung ist verantwortlich: [V_Test]

Die Einzelheiten des Testlaufs, die Testkriterien und die Testergebnisse sind festgehalten im Dokument: [Dok_Test]

7.1 Testkonzept und Abnahme

- *Wie wird die Konformität zu den konzeptionellen Vorgaben bzw. zum Pflichtenheft sichergestellt?*
- *Wie ist die Testumgebung und wie ist das Berechtigungskonzept im Testsystem?*
- *Wie erfolgt die Abnahme durch Kunden?*

7.2 Standardtests

7.2.1 Testbereich Dokumenteingang

- *Welche Tests stellen die korrekte Eingangsbearbeitung der Rechnungen sicher?*

7.2.2 Testbereich Importieren & Archivieren

- *Welche Tests stellen die korrekte Archivierung der Dokumente sicher?*

7.2.3 Testbereich Retrieval, Anzeige und Reproduktion

- *Welche Tests stellen die korrekte Reproduktion der Dokumente sicher?*

7.2.4 Testbereich Configuration Management

- *Welche Tests stellen die korrekte Umsetzung von Konfigurationsänderungen sicher?*
- *Welche Protokolle werden erstellt?*

7.3 Individuelle Tests

- *Welche Sonderfälle (Abweichungen vom „normalen“ Betrieb, z.B. Recovery) sollen getestet werden?*
- *Welche Tests sind nach der Implementierung neuer Releases vorgesehen?*

7.4 Testprotokolle

- *Welche Protokolle gibt es und wo sind sie zu finden (Archivierung wo, von wem)?*

Mustervorlage

7.5 Change and Release Management

Der gesamte Prozess von der Anforderung einer Änderung, über die Durchführung und die Tests der Änderung muss nachvollziehbar sein, dass ein hohes Qualitätsniveau sichergestellt ist und vorsätzliche oder versehentliche Änderungen Einzelner, die die Sicherheit unterminieren ausgeschlossen sind (z.B. 4-Augen-Prinzip, verteilte Rollen u. ä.)

7.5.1 Änderungsprozess

- *Wie ist der Prozess und wie sind die Verantwortlichkeiten bei Änderungsanforderungen?*

7.5.2 Freigabeprozess

- *Wie ist der Prozess und wie sind die Verantwortlichkeiten bei Freigabe von Änderungen oder Releasewechsel der Komponenten, z.B. Dokumentation?*

  Beispiel mit IKS-Bezug:

IKS!

Kontrollziel	Kontrolle
Es muss sichergestellt sein, dass beim Test-/Freigabeprozess das Vier-Augenprinzip eingehalten wird	In dem entsprechenden Formular XY muss die freigebende Person unterzeichnen, ...).

- *Wie erfolgt die Protokollierung?*

Mustervorlage

8 Tabellarischer Anhang

8.1 Geltungsbereich und Kundenverträge

Die abgeschlossenen Nutzungsvereinbarungen und Vollmachten befinden sich im Original in der Ablage: [Dok_Contract_Org]

Soweit sie auch in elektronischer Form vorliegen, finden sie sich in der folgenden Ablage: [Dok_Contract]

In diesen Verzeichnissen finden sich auch die VeR-Vereinbarungen (Code of Ethics und Interoperabilitätsvereinbarung).

Mit den folgenden Kunden wurden die genannten Vereinbarungen getroffen, die in den aufgeführten Ablagen zu finden sind und für die somit diese Verfahrensbeschreibung gilt:

Kundenname	**Verträge & Vereinbarungen**				**Bemerkung**
	NV RST	**Vollmacht RST**	**NV RE**	**Vollmacht RE**	
Mustermann-Rechnungssteller	✓	✓	×	×	
Mustermann- Rechnungsempfänger	×	×	✓	✓	

Legende: NV RST = Nutzungsvereinbarung Rechnungssteller, NV RE = Nutzungsvereinbarung Rechnungsempfänger

Mustervorlage

8.2 Relevante Dokumentationen, Handbücher, etc.

Die folgende Tabelle dient der Pflege der internen Ablagen relevanter Dokumente, die im vorliegenden Text nur über die Kurzbezeichnung referenziert werden.

Kurzbez.	Dokumentation	Archiv, Ablage, Verzeichnis	Bemerkung
[Dok_AA]	Arbeitsanweisungen		
[Dok_Contract]	Verträge und Vereinbarungen		
[Dok_Contract_Org]	Originale der Verträge und Vereinbarungen		
[Dok_Reference]	Technische Dokumente und Handbücher, generell		
[Dok_Test]	Durchgeführte Tests, inkl. Ergebnisse		

8.3 Interne Verantwortlichkeiten

Die folgende Tabelle dient der Pflege der internen Verantwortlichkeiten, die im vorliegenden Text nur über die Kurzbezeichnung referenziert werden.

Kurzbez.	Verantwortlichkeit	Zugeordnete Nutzer	Bemerkung
[L_Name]	Name des Standorts (Location)		
[V_BDSG]	Einhaltung BDSG, Datenschutzbeauftragter		
[V_Location]	Standortsicherheit		
[V_IT_Operating]	IT-Betrieb		
[V_IT_Security]	IT-Sicherheit		
[V_Test]	Test der eInvoice-Lösung		
[V_VFD]	Pflege dieser Verfahrensdokumentation		

Mustervorlage

8.4 Benutzer und Nutzergruppen

Die folgende Tabelle dient der Pflege der Nutzer- und Nutzergruppen für die eInvoice-Lösung.

Gruppen-bezeichnung	Rolle/Aufgabe	Zugeordnete Nutzer /Gruppen	Bemerkung
SysAdm	*System-Administratoren*	*Adm_SigSrv* *Adm_SigVer* *Adm_Windows* *Adm_Linux*	*Übergeordnete Gruppe*
Adm_SigSrv	*Sys-Admin Signatur-server*	*Mustermann1*	
Adm_SigVer	*Sys-Admin Verifikati-onsserver*	*Mustermann2*	
Adm_Windows			
Adm_Linux			

Kursive Angaben sind nur beispielhaft zur Verdeutlichung der Intention.

Mustervorlage

8.5 Zugriffsberechtigungen

Die folgende Tabelle dient der Pflege der Zugriffsberechtigungen für die eInvoice-Lösung.

Ressource (Kurzbez.)	**Zugeordnete Gruppen**			**Bemerkung**
(z.B. Applikation, Server-bereich, Dok.-/ Datenbe-stand)	**Lese-recht**	**Schreib-recht**	**Admin-recht**	
[AP_SigSrv] *Austauschverzeichnis*	*ALL*	*Adm_SigSrv*	*Adm_SigSrv*	
[AP_SigSrv] *Sonstige Verzeichnisse*	*Adm_SigSrv*	*Adm_SigSrv*	*Adm_S*	Hier eingegebene Texte dienen nur der Verdeutlichung
[HW_SigSrv]	*ALL*	*Adm_SigSrv*	*Adm_Linux*	

Mustervorlage

8.6 Configuration Management

In diesem Anhang sind die Angaben zu den beteiligten Hard- und Softwarekomponenten, inklusive der eingestellten Parameter aufgeführt. Die Datenblätter sind gruppiert in die Kategorien:

- Applikationen
- Infrastruktur-Software (die durch die Applikationen benötigt wird)
- Hardware (die für Applikationen und Infrastruktur-Software benötigt wird)

Soweit die Komponenten in anderen Dokumenten oder über ein Inventarisierungssystem gepflegt werden, sind entsprechende Verweise enthalten.

- *Die folgenden Beispiele enthalten nur die wichtigsten Daten. Sofern ausführlichere Informationen an anderer Stelle vorgehalten reicht ein eindeutiger Verweis.*
- *Wenn ein Inventarisierungssystem vorhanden ist, kann hier auch eine Liste der genutzten Komponenten mit einem entsprechenden Verweis auf die genaue Bezeichnung in der Inventarisierung ausreichend sein.*

Mustervorlage

8.6.1 Datenblätter Applikationen

Applikationen sind eigenständige führende Software-Systeme, die ihrerseits auf Infrastruktur-System im Hintergrund zugreifen.

Kurzbezeichnung	**Archiv-Services**
Genauere Bezeichnung oder Kurzbeschreibung der Komponente?	
Wie ist die genaue Version des Herstellers?	
Wer ist der Hersteller?	
Wesentliche, benötigte Funktion der Software?	
Link zur internen Dokumentation	<hier ggf. Link einfügen>
Link zur Konfigurationsbeschreibung	<hier ggf. Link einfügen>
Wer im Haus ist verantwortlich für Pflege und Dokumentation dieser Applikation?	??? ???
Datenblatt ist gültig ab	????
Datenblatt war gültig bis	31.12.2100
Sonstige Bemerkung	

Mustervorlage

Kurzbezeichnung	**Individual-SW für ??**
Genauere Bezeichnung oder Kurzbeschreibung der Komponente?	
Wie ist die genaue Version des Herstellers?	
Wer ist der Hersteller?	
Wesentliche, benötigte Funktion der Software?	
Link zur internen Dokumentation	<hier ggf. Link einfügen>
Link zur Konfigurationsbeschreibung	<hier ggf. Link einfügen>
Wer im Haus ist verantwortlich für Pflege und Dokumentation dieser Applikation?	??? ???
Datenblatt ist gültig ab	????
Datenblatt war gültig bis	31.12.2100
Sonstige Bemerkung	

Mustervorlage

Kurzbezeichnung	**??**
Genauere Bezeichnung oder Kurzbeschreibung der Komponente?	
Wie ist die genaue Version des Herstellers?	
Wer ist der Hersteller?	
Wesentliche, benötigte Funktion der Software?	
Link zur internen Dokumentation	<hier ggf. Link einfügen>
Link zur Konfigurationsbeschreibung	<hier ggf. Link einfügen>
Wer im Haus ist verantwortlich für Pflege und Dokumentation dieser Applikation?	??? ???
Datenblatt ist gültig ab	????
Datenblatt war gültig bis	31.12.2100
Sonstige Bemerkung	

Mustervorlage

8.6.2 Datenblätter Infrastruktur-Software

Als Infrastruktur-Software wird Software bezeichnet, die von verschiedenen Applikationen genutzt wird, z.B. ein LDAP-System zur Nutzer-Authentifizierung.

Kurzbezeichnung	**LDAP**
Wie ist die genaue Bezeichnung der Komponente?	
Wie ist die genaue Version des Herstellers?	
Wer ist der Hersteller?	
Wesentliche, benötigte Funktion der Software?	
Link zur internen Dokumentation	<hier ggf. Link einfügen>
Link zur Konfigurationsbeschreibung	<hier ggf. Link einfügen>
Wer im Haus ist verantwortlich für Pflege und Dokumentation dieser Infrastruktur-Software?	??? ???
Datenblatt ist gültig ab	????
Datenblatt war gültig bis	31.12.2100
Sonstige Bemerkung	

Mustervorlage

Kurzbezeichnung	**Archiv-Basissystem**
Wie ist die genaue Bezeichnung der Komponente?	
Wie ist die genaue Version des Herstellers?	
Wer ist der Hersteller?	
Wesentliche, benötigte Funktion der Software?	
Link zur internen Dokumentation	<hier ggf. Link einfügen>
Link zur Konfigurationsbeschreibung	<hier ggf. Link einfügen>
Wer im Haus ist verantwortlich für Pflege und Dokumentation dieser Infrastruktur-Software?	??? ???
Datenblatt ist gültig ab	????
Datenblatt war gültig bis	31.12.2100
Sonstige Bemerkung	

Mustervorlage

Kurzbezeichnung	**Optional: Signatur-Services**
Genauere Bezeichnung oder Kurzbeschreibung der Komponente?	
Wie ist die genaue Version des Herstellers?	
Wer ist der Hersteller?	
Wesentliche, benötigte Funktion der Software?	
Link zur internen Dokumentation	<hier ggf. Link einfügen>
Link zur Konfigurationsbeschreibung	<hier ggf. Link einfügen>
Wer im Haus ist verantwortlich für Pflege und Dokumentation dieser Applikation?	??? ???
Datenblatt ist gültig ab	????
Datenblatt war gültig bis	31.12.2100
Sonstige Bemerkung	

Mustervorlage

Kurzbezeichnung	**Optional: Signaturprüf-Services**
Genauere Bezeichnung oder Kurzbeschreibung der Komponente?	
Wie ist die genaue Version des Herstellers?	
Wer ist der Hersteller?	
Wesentliche, benötigte Funktion der Software?	
Link zur internen Dokumentation	<hier ggf. Link einfügen>
Link zur Konfigurationsbeschreibung	<hier ggf. Link einfügen>
Wer im Haus ist verantwortlich für Pflege und Dokumentation dieser Applikation?	??? ???
Datenblatt ist gültig ab	????
Datenblatt war gültig bis	31.12.2100
Sonstige Bemerkung	

Mustervorlage

Kurzbezeichnung	**??**
Wie ist die genaue Bezeichnung der Komponente?	
Wie ist die genaue Version des Herstellers?	
Wer ist der Hersteller?	
Wesentliche, benötigte Funktion der Software?	
Link zur internen Dokumentation	<hier ggf. Link einfügen>
Link zur Konfigurationsbeschreibung	<hier ggf. Link einfügen>
Wer im Haus ist verantwortlich für Pflege und Dokumentation dieser Infrastruktur-Software?	??? ???
Datenblatt ist gültig ab	????
Datenblatt war gültig bis	31.12.2100
Sonstige Bemerkung	

Mustervorlage

8.6.3 Datenblätter Hardware

Als IT-Hardware werden hier vor allem Server und ggf. Arbeitsplatzsysteme bezeichnet, die als Hardware für die Applikationen und Infrastruktur-Software-Module genutzt werden.

Kurzbezeichnung	**Archiv-Server**
Was ist die Funktion der Komponente?	
Hersteller	
Betriebssystem	
IP-Adresse	
Gateway	
Standort der Hardware	
Domäne	
Anzahl der CPU's	
Taktfrequenz in GHz	
Hauptspeicher	
Link zur internen Dokumentation	<hier ggf. Link einfügen>
Link zur Konfigurationsbeschreibung	<hier ggf. Link einfügen>
Verantwortlichkeit im Haus	
Datenblatt ist gültig ab	????
Datenblatt war gültig bis	31.12.2100
Sonstige Bemerkung / Beschreibung	

Mustervorlage

Kurzbezeichnung	**Optional: Signatur-Server**
Was ist die Funktion der Komponente?	
Hersteller	
Betriebssystem	
IP-Adresse	
Gateway	
Standort der Hardware	
Domäne	
Anzahl der CPU's	
Taktfrequenz in GHz	
Hauptspeicher	
Link zur internen Dokumentation	<hier ggf. Link einfügen>
Link zur Konfigurationsbeschreibung	<hier ggf. Link einfügen>
Verantwortlichkeit im Haus	
Datenblatt ist gültig ab	????
Datenblatt war gültig bis	31.12.2100
Sonstige Bemerkung / Beschreibung	

Mustervorlage

Kurzbezeichnung	**Optional: Verifikations-Server**
Was ist die Funktion der Komponente?	
Hersteller	
Betriebssystem	
IP-Adresse	
Gateway	
Standort der Hardware	
Domäne	
Anzahl der CPU's	
Taktfrequenz in GHz	
Hauptspeicher	
Link zur internen Dokumentation	<hier ggf. Link einfügen>
Link zur Konfigurationsbeschreibung	<hier ggf. Link einfügen>
Verantwortlichkeit im Haus	
Datenblatt ist gültig ab	????
Datenblatt war gültig bis	31.12.2100
Sonstige Bemerkung / Beschreibung	

Mustervorlage

Kurzbezeichnung	**??-Server**
Was ist die Funktion der Komponente?	
Hersteller	
Betriebssystem	
IP-Adresse	
Gateway	
Standort der Hardware	
Domäne	
Anzahl der CPU's	
Taktfrequenz in GHz	
Hauptspeicher	
Link zur internen Dokumentation	<hier ggf. Link einfügen>
Link zur Konfigurationsbeschreibung	<hier ggf. Link einfügen>
Verantwortlichkeit im Haus	
Datenblatt ist gültig ab	????
Datenblatt war gültig bis	31.12.2100
Sonstige Bemerkung / Beschreibung	

Mustervorlage