

Vorlage für die Erstellung einer im Zusammenhang mit E-Invoicing in der EIDI-V und GeBüV geforderten Verfahrensdokumentation, Version 1.0

Entstanden aus dem swissDIGIN-Forum vom 17. Juni 2009
mit Unterstützung der swissDIGIN-Partner und von Keyon

Dezember 2009

Partner des swissDIGIN-Forums:



Erstellung der Publikation unterstützt durch www.keyon.ch

Zweck und Einordnung der Vorlage

Die Verfahrensdokumentation muss es laut GeBüV¹ einem buchführungskundigen Dritten erlauben, die Funktionsweise eines Datenverarbeitungssystems unter angemessenem Zeitaufwand ausreichend zu begreifen, um die darin enthaltenen Daten hinsichtlich ihrer formellen und sachlichen Richtigkeit innerhalb nützlicher Frist prüfen zu können. Im Zusammenhang mit E-Invoicing dokumentiert sie, wie das Unternehmen die elektronische Rechnungsabwicklung ausgestaltet hat und wie die kritischen Prozesse beherrscht werden. Sie ist deshalb auch organisationsintern von grossem Nutzen, wenn sie als Grundlage für Modifikationen am System und für die Anleitung von Mitarbeitenden verwendet wird.

Der Umfang und die Tiefe der Verfahrensdokumentation richten sich nach der Grösse und Komplexität der Organisation. Grundsätzlich beschreibt sie den effektiven Stand des Systems bzw. das effektive Vorgehen in den Prozessen. Werden Aufgaben an Dritte übertragen, so sollte für diese Aufgaben auf Dokumentationen dieser Partner verwiesen werden können.

Dieses Dokument ist als Orientierungshilfe und Vorlage für die Erstellung der im Rahmen der EIDI-V² verlangten Verfahrensdokumentation zur Beschreibung von Datenverarbeitungssystemen für steuerrelevante Daten konzipiert. Ein gesondertes Beispiel dient speziell KMU als Orientierung, wie sie in der Rolle als Rechnungssteller im E-Invoicing die Verfahrensdokumentation inhaltlich und vom Umfang her gestalten können.

Die Inhaltsstruktur orientiert sich einerseits an den Anforderungen, die in der EIDI-V und GeBüV zum Ausdruck kommen, andererseits an den Vorschlägen zur Erstellung von Sicherheitskonzepten, wie sie in Standards zum Informationssicherheitsmanagement, wie z.B. ISO 27000, festgehalten sind.

Die Eidgenössische Steuerverwaltung (ESTV) schreibt Aufbau und Umfang einer Verfahrensdokumentation nicht vor. Qualitativ ausreichend ist die Verfahrensdokumentation, wenn sie den eingangs beschriebenen Anforderungen genügt. Die ESTV hat von dieser Vorlage Kenntnis genommen.

Haftungsausschluss

Die vorliegende, durch das swissDIGIN-Forum erarbeitete Vorlage für eine Verfahrensdokumentation gilt als Vorschlag aus Sicht der mitwirkenden Personen für die Anwendung in der Schweiz. Sie wurde nach bestem Wissen der Teilnehmenden erstellt. Bei ihrer auch nur auszugswweisen Verwendung können zu keiner Zeit Forderungen gegen Forumsteilnehmende und/oder gegen die durch sie vertretenen Firmen und Organisationen geltend gemacht werden.

¹ Verordnung vom 24. April 2002 über die Führung und Aufbewahrung der Geschäftsbücher (Geschäftsbücherverordnung; GeBüV; SR 221.431)

² Verordnung des EFD über elektronische Daten und Informationen vom 30. Januar 2002 (Stand 1. November 2007) (EIDI-V; SR 641.201.1)

Inhaltsverzeichnis

Zweck und Einordnung der Vorlage	ii
Inhaltsverzeichnis	iii
1 Systemüberblick	1
1.1 Systemgrenzen	1
1.2 Systemkomponenten	1
1.3 Interne/Externe Schnittstellen	1
2 Geschäftsfälle und Prozesse.....	2
2.1 Informationen und Daten	2
2.2 Geschäftsfälle und Verarbeitung.....	2
3 Programmtechnische Verarbeitung.....	3
3.1 Programme/Anwendungen	3
3.2 Programmschnittstellen	3
3.3 Datenspeicherung.....	3
3.4 Signaturerstellung und Signaturprüfung.....	3
4 Organisation und Verantwortlichkeiten.....	4
4.1 Übersicht über die Verantwortlichkeiten	4
4.2 Übersicht über die Kontrollen.....	4
5 Führung und Zugriff auf Archiv.....	5
5.1 Regulärer Archivzugriff	5
5.2 Revisionsbedingter Archivzugriff.....	5
5.3 Periodische Archivüberprüfung	5
5.4 Validierung der elektronischen Signatur	5
5.5 Archivmigration	5
6 Informationssicherheitsmanagement	6
6.1 Abhängigkeiten von Prozessen und Infrastruktur	6
6.2 Schwachstellen und Schutzbedarf (Risiken).....	6
6.3 Massnahmen	6
6.4 Änderungswesen	6
6.4.1 Bestimmen der Anforderungen an eine Änderung	6
6.4.2 Freigabe einer Änderung.....	6
6.4.3 Releasepläne	6
Anhang	7

1 Systemüberblick

Es ist zu beschreiben, welche IT-Infrastruktur an welchen Standorten für die relevante Verarbeitung zum Einsatz kommt. Insbesondere sind Schnittstellen nach aussen und gesicherte/ungesicherte Bereiche und Zonen auszuweisen. Dies führt zu einer dokumentierten logischen Darstellung mit Systemen und Schnittstellen.

1.1 Systemgrenzen

Beschreibung der fachlichen, organisatorischen und technischen Systemgrenzen. Festlegen, welche Komponenten in der Verfahrensdokumentation beschrieben werden.

1.2 Systemkomponenten

Beschreibung von Systemkomponenten, auf denen für die Verarbeitung relevante Programme laufen oder auf denen Datenbanken gesteuert werden.

1.3 Interne/Externe Schnittstellen

Beschreibung von Übergängen von einem Verarbeitungssystem ins nächste und den damit verbundenen Umwandlungen von Informationen. Insbesondere ist zu zeigen, wo Daten gesicherte Bereiche verlassen oder in andere Verantwortungsbereiche wechseln.

2 Geschäftsfälle und Prozesse

Definition der Informationen (Stammdaten etc.) und sachlogische Beschreibung der schrittweisen Informationsverarbeitung. Insbesondere ist auszuweisen, welche Verarbeitungsschritte welche Verarbeitungsregeln (Business Rules, Gesetzesartikel) einzuhalten haben und wie diese kontrolliert werden (IKS - Internes Kontrollsystem).

2.1 Informationen und Daten

Beschreibung aller relevanten Informationen, deren Bedeutung und deren Abbildung in Daten (-formate) wie Files, Datensätzen in Datenbanken oder Protokolle.

2.2 Geschäftsfälle und Verarbeitung

Beschreibung der möglichen Situationen (Vorfälle), in denen eine Verarbeitung ausgelöst wird und deren Verarbeitungsschritte. Insbesondere muss gezeigt werden, wie und welche Veränderungen die Schritte an den Daten bewirken (Transformationen) und durch welche Infrastrukturelemente diese Verarbeitungen unterstützt werden (Abhängigkeiten).

Beschreiben der organisatorischen und technischen Prozesse im Falle einer erfolgreichen Verarbeitung der Daten und im Falle einer nichterfolgreichen Verarbeitung der Daten (Aufführen der wichtigsten Fehlerfälle).

3 Programmtechnische Verarbeitung

Programmlogische Beschreibung der Datenverarbeitung, des Datentransports und deren Speicherung. Diese Darstellung lässt klar erkennen, welche Softwarekomponenten für die Verarbeitungsschritte unter 2.2 zuständig sind. Insbesondere ist klar auszuweisen, welche weiteren IT-Infrastrukturelemente für ein sicheres Funktionieren der programmtechnischen Verarbeitung benötigt werden (Abhängigkeiten).

3.1 Programme/Anwendungen

Beschreibung der Anwendungen. Hier sind insbesondere die für die Verarbeitungsschritte gedachten Programmfunktionen zu identifizieren und die Zu- und Abführung von Daten zu definieren.

3.2 Programmschnittstellen

Beschreibung der Kommunikationsschnittstellen zwischen den beteiligten Programmen und zwischen den Nutzern und den Programmen.

3.3 Datenspeicherung

Beschreibung der Datenablagen, die auf dem Weg der Informationsverarbeitung Anwendung finden.

3.4 Signaturerstellung und Signaturprüfung

Beschreibung, mit welchen Mitteln die digitale Signatur erstellt und verifiziert wird. Weiter sind die Verwaltung der digitalen Schlüssel sowie der Zugriff von Systemen auf die digitalen Schlüssel zu beschreiben.

4 Organisation und Verantwortlichkeiten

Beschreibung der für die unter 2 beschriebenen Geschäftsfälle relevanten Aufbauorganisation und Zuordnung von Verantwortlichkeiten für Prozesse, Systeme und Programme. Es muss klar ersichtlich sein, wer für Betrieb, Änderungen und Sicherheit zuständig ist.

4.1 Übersicht über die Verantwortlichkeiten

Auflistung aller Organisationselemente (Prozesse, Infrastruktur etc.) zusammen mit der verantwortlichen Einheit (sog. Prozess- und Systemeigner).

4.2 Übersicht über die Kontrollen

Auflistung aller einzuhaltenden Regeln, der Verantwortlichkeit für deren Umsetzung, dem Ort und dem Gegenstand der Kontrolle.

5 Führung und Zugriff auf Archiv

Beschreibung der Sicherstellung des dauerhaften Zugriffs auf relevante Informationen für eigene Zwecke und für Einsichtsberechtigte während der geforderten Aufbewahrungsfrist.

Im E-Invoicing sind drei grundsätzliche Formen der Archivierung der elektronischen Rechnungen samt den dazugehörigen Dateien möglich:

- 1) Archivierung auf CD oder DVD des E-Invoicing Service Providers,
- 2) Archivierung durch einen Dienstleister,
- 3) Archivierung in einem eigenen elektronischen Archiv.

5.1 Regulärer Archivzugriff

Beschreibung, wie die verschiedenen Geschäftsfälle aus dem Archiv heraus rekonstruiert (nachvollzogen) werden können.

5.2 Revisionsbedingter Archivzugriff

Beschreibung, wie die ordentliche Buchführung (Prüfpfade) mithilfe der Möglichkeiten des Archivs nachgewiesen werden kann (progressiver und retrograder Prüfpfad).

5.3 Periodische Archivüberprüfung

Beschreibung, wie die Beweiskraft (Integrität und Authentizität) der archivierten Daten periodisch überprüft wird.

5.4 Validierung der elektronischen Signatur

Beschreibung, wie die digitale Signatur verifiziert werden kann und wie das Ergebnis der Verifikation in einem Prüfprotokoll festgehalten wird.

5.5 Archivmigration

Beschreibung, welche Vorkehrungen bei Änderungen im Archivbereich (neue Systemreleases etc.) zu treffen sind, um die Verfügbarkeit und Integrität der Information zu gewährleisten.

6 Informationssicherheitsmanagement

Es ist zu beschreiben, wie die Integrität, Vertraulichkeit und Verfügbarkeit der Daten und Informationen sichergestellt wird. Im Fall von kleineren Organisationen können die relevanten Aspekte durchaus schon in den voran stehenden Kapiteln integriert dokumentiert sein.

6.1 Abhängigkeiten von Prozessen und Infrastruktur

Beschreibung, wie Verarbeitungsschritte (Prozessschritte) von unterstützenden Infrastrukturelementen wie Servern, Programmen, Datenbanken, Räumen etc. abhängig sind. Insbesondere ist auch zu klären, welche Verarbeitungsschritte beim Ausfall bestimmter IT-Infrastruktur betroffen wären.

6.2 Schwachstellen und Schutzbedarf (Risiken)

Anhand der geklärten Abhängigkeiten zwischen Verarbeitungsschritten und Infrastruktur sind die möglichen Schwachstellen zu identifizieren und systematisch zu bewerten (Risikomanagement) und ist der Schutzbedarf explizit auszuweisen.

6.3 Massnahmen

Um Schwachstellen zu eliminieren oder abzusichern sind vorgeschlagene Standardmassnahmen (z.B. nach ISO27000 oder nach BSI Grundschutz) auf Zweckmässigkeit hin zu überprüfen und gezielt und planmässig umzusetzen. Für Restrisiken sind Notfallmassnahmen zu definieren.

6.4 Änderungswesen

Es ist zu beschreiben, wie die Konfigurationsverwaltung von Stammdaten, Prozessen, Systemen, Konfigurationen (Steuertabellen etc.) und Programmen und deren Dokumentationen samt der zugehörigen Ausbildungsunterlagen durchgeführt wird.

6.4.1 Bestimmen der Anforderungen an eine Änderung

Es ist zu beschreiben, wie Anforderungen gesammelt und bewertet werden. Weiter ist aufzuzeigen, wie mögliche Lösungen bewertet (Zeit, Budget, Wirksamkeit) und priorisiert werden.

6.4.2 Freigabe einer Änderung

Es ist zu beschreiben, wie Änderungen an Anforderungen, Lösungen und deren Umsetzung systematisch freigegeben und dokumentiert werden.

6.4.3 Releasepläne

Es ist zu definieren, wann welche Konfiguration von Komponenten (=Release) zum Einsatz kommt. Insbesondere sind Testdaten und Freigabeerklärungen zu den Releases nachzuweisen.

Anhang

- Beispiele von Datensätzen entlang der Verarbeitung (Files, PDFs, Datenbank-Records, Screenshots, etc.)
- Arbeitsanweisungen
- Prüfchecklisten
- Protokolle
- Unterlagen der involvierten Service Provider wie
 - Leistungsbeschreibung samt Delegation der übertragenen Aufgaben
 - Verweis auf Verfahrensdokumentation der involvierten Service Provider
- Programmtechnische Dokumentationen der eingesetzten Software-Produkte