Sage

Verfahrensdokumentation

Rechtliches:
Sage ist bei der Erstellung dieses Dokuments mit großer Sorgfalt vorgegangen. Fehlerfreiheit können wir jedoch nicht garantieren. Sage haftet nicht für technische Fehler in diesem Dokument. Die Beschreibungen in diesem Dokument stellen keine zugesicherte Eigenschaft im Rechtssinne dar.

Frankfurt, November 2024

Version 1.1

Sage

Inhaltsverzeichnis

1 Verfahrensdokumentation 3
1.1 Allgemeines 3
1.2 Was ist eine Verfahrensdokumentation 3
1.3 Umfang der Dokumentation 4
1.4 Inhalte der Verfahrensdokumentation 4
1.5 Aufbau einer Verfahrensdokumentation 7
1.6 Handlungsempfehlung zur Erstellung einer Verfahrensdokumentation 7
1.7 Kurzcheck zur Verfahrensdokumentation 8
1.8 Ablauf der Verfahrensdokumentation 8

2 Allgemeine Beschreibung zur Organisation und Aufgabenstellung 9

3 Allgemeine Beschreibung zur Anwendung 10

4 Technische Systemdokumentation 11
4.1 Datensicherheitskonzept 12
4.2 Sicherung gegen Verlust 12
4.3 Sicherung gegen unberechtigte Veränderung 12

5 Betriebsdokumentation 14

6 Mitarbeiterqualifikation 15

7 Prozessbeschreibung 16
7.1 Ersetzendes Scannen 17
7.2 Datenübermittlung 18
7.3 Löschkonzept zur Datenminimierung 18
7.4 Löschkonzept erstellen 18

8 Internes Kontrollsystem (IKS) 19

9 Glossar: Abkürzungen und Bedeutungen 20

1 Verfahrensdokumentation

1.1 Allgemeines

Dieses Dokument beschreibt die Vorgehensweise zur Verfahrensdokumentation, wie sie in der GoBD gefordert wird. Es werden darin die Kriterien Vollständigkeit, Richtigkeit, Unveränderbarkeit, Verfügbarkeit und Nachvollziehbarkeit behandelt.

Achtung: Die konkrete Ausgestaltung dieser Verfahrensdokumentation ist abhängig von der Komplexität und Diversifikation der Geschäftstätigkeit und der Organisationsstruktur sowie des eingesetzten DV-Systems. Dieses Dokument stellt lediglich eine Handlungsempfehlung dar. Für eine detaillierte Ausarbeitung setzen Sie sich bitte mit Ihrem Steuer- und/oder Wirtschaftsberater in Verbindung.

1.2 Was ist eine Verfahrensdokumentation

Die Aufgabe der Aufsichtsbehörden im Datenschutz ist es, die Beachtung der Datenschutzgesetze durch Unternehmen und Behörden (öffentliche und nicht-öffentliche Stellen) zu überwachen.

Die Verfahrensdokumentation beschreibt den organisationsspezifischen und revisionssicheren Zustand des Systems und dient auf diesem Wege einem sachverständigen Dritten (z.B. Wirtschaftsprüfer, Betriebsprüfer, interne Revision) als Basis zur Beurteilung der Implementierung. Die Anforderung zur Erstellung einer Verfahrensdokumentation ergibt sich im Wesentlichen aus den handels- und steuerrechtlichen Anforderungen. Hinzu kommen weitere regulatorische oder spezielle Regelungen.

Sie ist eine umfassende Beschreibung der Prozesse im Unternehmen, die bei der Erstellung z.B. der Buchhaltung stattfinden. Sie ist nicht nur beschränkt auf Abläufe, Vorgänge und Programmbenutzung, sondern soll ebenfalls beschreiben, welche Geräte eingesetzt und wie und von wem genutzt werden.

Die Verfahrensdokumentation für elektronische Archivsysteme (z.B. DMS) hat die Zielsetzung, den organisatorischen und technischen Prozess von der Entstehung der Informationen über die Indizierung und Speicherung, dem eindeutigen Wiederfinden, der Absicherung gegen Verlust und Verfälschung und der Reproduktion am Bildschirm und auf dem Drucker zu dokumentieren“.

Bereits in der GoBS (07.11.1995) wurde gefordert, über die betrieblichen Abläufe im Zusammenhang mit der Datenverarbeitung eine ordnungsgemäße Verfahrensdokumentation

zu erstellen. Mit dem GoBD-Schreiben vom 14. November 2014 (Rz. 151) des Bundesministeriums der Finanzen an die obersten Finanzbehörden der Länder, wurde die Forderung nochmals klar geäußert und präzisiert.

Da sich nach Auffassung der Finanzverwaltung die Ordnungsmäßigkeit einer Datenverarbeitung auch auf die damit in Zusammenhang stehenden Verfahren und Bereiche des DV-Systems erstreckt, muss für jedes System eine übersichtliche und gegliederte Verfahrensdokumentation vorhanden sein. Diese Dokumentation muss die internen Datenverarbeitungsverfahren bezüglich Inhalts, Aufbau und Ergebnisse vollständig, lückenlos und schlüssig beschreiben.

1.3 Umfang der Dokumentation

Der Umfang einer Verfahrensdokumentation wird dadurch bestimmt, was zum Verständnis der Datenverarbeitungsprozesse notwendig ist. Als Maßstab wird wiederum auf einen sachverständigen Dritten verwiesen, der in angemessener Zeit, die Prozessabläufe anhand der Dokumentation verstehen, nachvollziehen und prüfen können. Folgendes ist dabei zu beachten:

- Die Aufzeichnungen sollten verständlich formuliert sein
- Die Prozesse sollten transparent und lückenlos beschrieben sein, wobei nicht nur manuelle Verfahren wie etwa das Scannen gemeint sind, sondern auch digitale Prozesse. Hierzu gehört beispielsweise die Art und Weise wie selbst erstellte elektronische Belege aufbewahrt werden
- Änderungen an den Abläufen sind zu dokumentieren, wobei ältere Verfahrensdokumentationen ebenfalls aufzubewahren sind.

Achtung: Der Umfang der Verfahrensdokumentation hängt von vielen Faktoren ab. Hierzu gehören beispielsweise die eingesetzten Systeme oder die Komplexität der Abläufe. Eine für alle Betriebe gleichermaßen passende Blaupause kann es daher nicht geben.

1.4 Inhalte der Verfahrensdokumentation

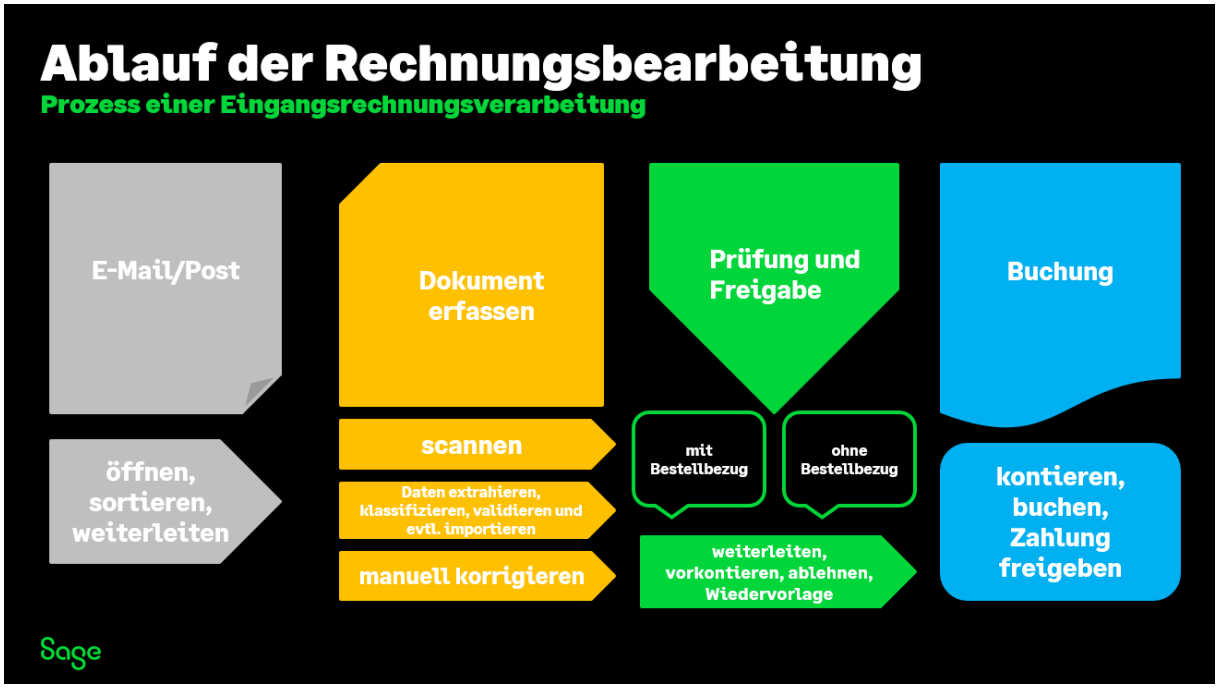
Im Folgenden finden Sie eine Gliederungsstruktur, die die Tiefe der Dokumentation beschreibt:

Hinweis: Beschreiben Sie nur Punkte, die für die Nachvollziehbarkeit von organisatorischen oder technischen Prozessen erforderlich sind. Umfang und Aufbau einer Verfahrensdokumentation sind in der GoBD nicht vorgeschrieben.

- Allgemeine Beschreibung der Einsatzgebiete im Unternehmen
  Die allgemeine Beschreibung beinhaltet Informationen zu den Rahmenbedingungen, Zielsetzungen und den Anwendungsbereich der Verfahrensdokumentation. Dies umfasst insbesondere eine kurze Beschreibung des Unternehmens, der betroffenen Organisationsbereiche, des Gegenstands der Digitalisierung und Archivierung und der verwendeten Softwarelösungen. Darüber hinaus sollten in diesem Abschnitt die Verantwortlichkeiten geregelt werden.
- Anwenderdokumentation aus fachlicher Sicht
  Die Anwenderdokumentation erklärt die Verfahren und Maßnahmen, die bei der Verarbeitung von Belegen zu beachten sind. Sie beschreibt insbesondere, wie Daten erfasst, erstellt, geprüft, vorbereitet, digitalisiert, abgelegt, archiviert und vernichtet werden. Darüber hinaus regelt die Anwenderdokumentation auch die Verfahren zur Kontrolle und die entsprechenden Verantwortlichkeiten.
- Technische Systemdokumentation
  Die technische Systemdokumentation enthält alle erforderlichen Informationen zur im Verfahren eingesetzten Hard- und Software. Soweit keine intern entwickelten Lösungen zum Einsatz kommen, sollte bezüglich der Spezifikationen der einzelnen Komponenten auf Handbücher und technische Beschreibungen der Hersteller verwiesen werden. (z.B. Programmversion)
- IT-Sicherheit
  beschreibt die Datensicherheit und –integrität sowie den Datenschutz im Unternehmen
- Betriebsdokumentation
  In der Betriebsdokumentation sind typischerweise Anweisungen und Dokumentationen zum IT-Betrieb enthalten, z.B. betriebliches Umfeld, Kennzahlen aus organisatorischer und technischer Sicht, Anzahl der Mitarbeiter. In diesem Teil sollten die relevanten, firmenspezifischen Architekturen, Vorgehensweisen, Abhängigkeiten und Einstellungen von IT-Systemen. Dazu gehören auch Informationen zur IT-Sicherheit wie Zugriffsrechte und Datensicherung.

> **Hinweis:** Aufgrund von Überschneidungen sind die einzelnen Bereiche nicht immer klar abgrenzbar. Da jedoch keine formellen Vorgaben zur Verfahrensdokumentation bestehen, sind Unternehmen in der Strukturierung nicht gebunden.
>
> Ebenso können relevante Teile der Verfahrensdokumentation bereits im Unternehmen vorliegen. Die Verfahrensdokumentation kann aus mehreren Dokumenten bestehen oder auf andere Dokumente verweisen, beispielsweise auf Handbücher, Arbeitsanweisungen, Anwenderdokumentation, auf Testdokumentationen oder IT-Sicherheitsrichtlinie usw.

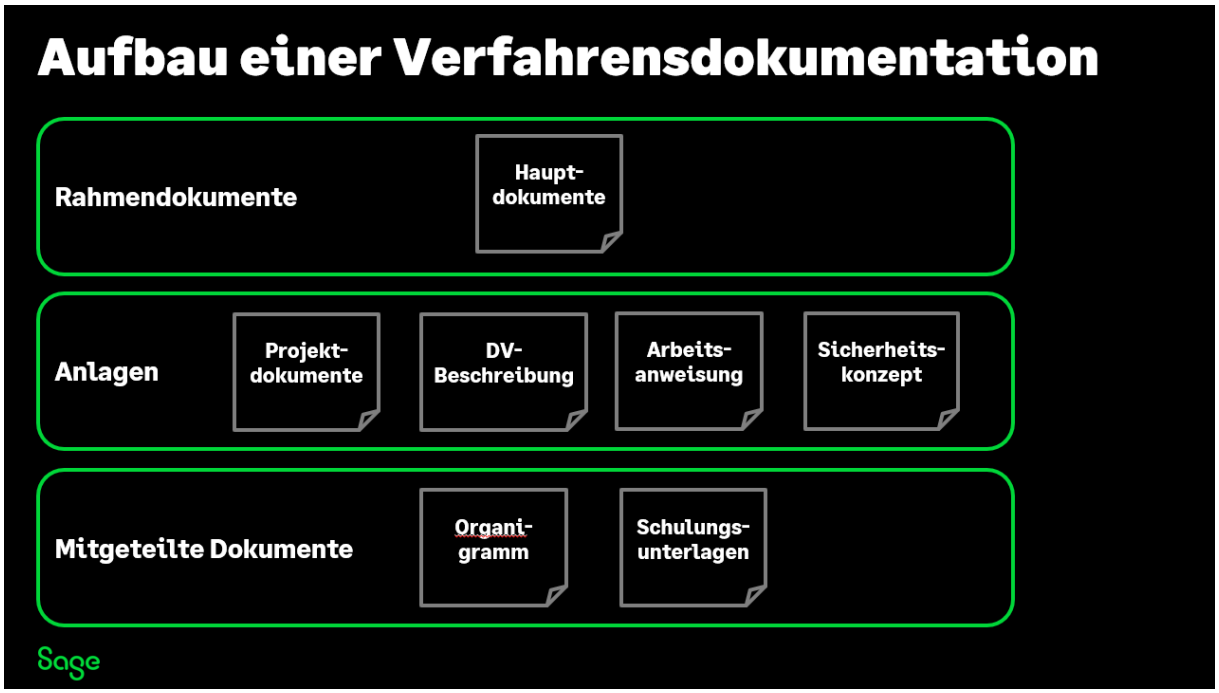
- Prozessbeschreibung
  die z.B. bei der Erstellung der elektronischen Buchführung oder Bearbeitung des Posteingangs anfallen. Hier bietet sich an, den Prozess in einem graphischen Ablaufdiagramm darstellen. Kurze Kommentierungen runden das Schaubild ab.



- Mitarbeiterqualifikation
  Darstellung der Schulungsmaßnahmen, Kompetenzen und Verantwortlichkeiten
- Internes Kontrollsystem (IKS)
  Nach innen gerichtete, betriebsinterne Kontrollüberprüfung und Überwachung der Abläufe, welche in der Verfahrensdokumentation beschrieben werden, in regelmäßiger und permanenter Weise

Achtung: Beachten Sie, dass eine fehlende Dokumentation zum Verwerfen der Buchführung führen kann, wenn insbesondere bei Betriebsprüfungen die handelsrechtlichen Grundsätze der GOB nicht eingehalten werden (Vollständigkeit, Richtigkeit, Unveränderbarkeit, Verfügbarkeit und Nachvollziehbarkeit). Wird eine der vorgenannten Forderungen nicht erfüllt, kann ein schwerer Mangel vorliegen, der in extremen Fällen zum Verwerfen der Buchführung führen kann. Der Prüfer wäre dann berechtigt, entsprechende Schätzungen oder bei extremen Fällen eine Vollschätzung vorzunehmen.

1.5 Aufbau einer Verfahrensdokumentation



1.6 Handlungsempfehlung zur Erstellung einer Verfahrensdokumentation

- ☐ Überblick über die vorhandenen Geräte und Programme
  - Erstellung einer Liste
- ☐ Abbildung der Prozesse und Abläufe im Unternehmen ggfs. in graphischer Darstellung (Ablaufplan)
  - Benennung verantwortlicher Mitarbeiter für entsprechende Bereiche
  - Sind bereits Verfahrensvorgaben, Arbeitsanweisung vorhanden
  - Nutzen Sie die Benutzerhandbücher für Hard- und Software
- ☐ Erstellung eines Zeitplans zur Umsetzung und Abstimmung mit verantwortlichen Mitarbeitern

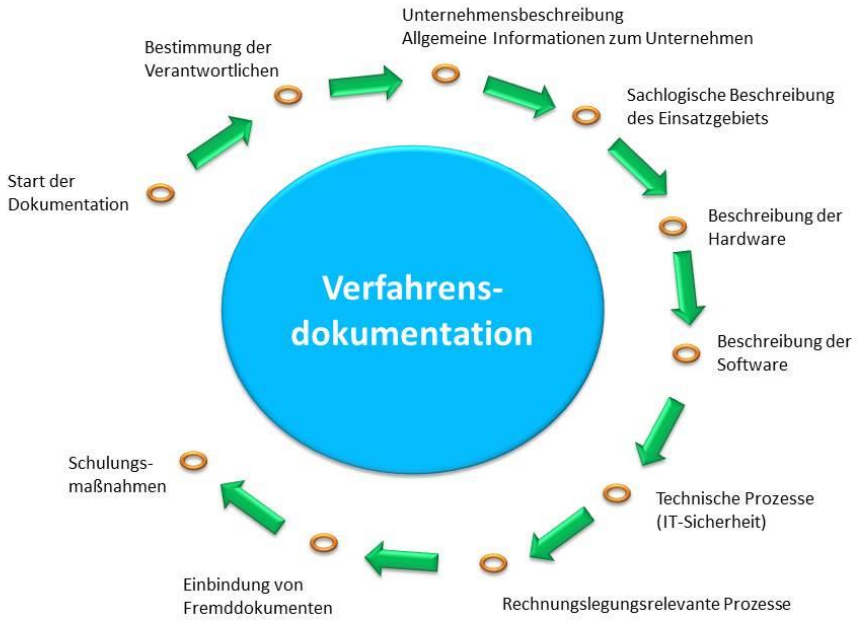
Hinweis:
Eine Musterverfahrensdokumentation wurde von der Bundessteuerberaterkammer und dem Deutschen Steuerberaterverband e. V. gemeinsam entwickelt. Diese kann Ihnen als Vorlage dienen!
Weitere Informationen zum “Ersetzenden Scannen” liefert das Bundesamt für Sicherheit in der Informationstechnik (BSI) in der “Technischen Richtlinie 03138”. Sie ist im Internet unter **https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03138/TR-03138.pdf** zu finden.

1.7 Kurzcheck zur Verfahrensdokumentation

Nachfolgend finden Sie einen Kurzcheck für Ihre Verfahrensdokumentation:

- ☐ Sind alle relevanten Prozesse und Tätigkeiten durch Verfahrens- und Arbeitsanweisungen dokumentiert?
- ☐ Sind alle relevanten Bearbeitungsschritte bekannt und dokumentiert?
- ☐ Liegen aktuelle interne Verfahrensübersichten bzw. ein Verfahrensverzeichnis vor?
- ☐ Liegen Anwenderdokumentationen und technische Systemdokumentationen für sämtliche IT-Systeme im Unternehmen vor?
- ☐ Sind alle involvierten Mitarbeiter bezüglich der Abläufe geschult?
- ☐ Sind IT-Richtlinien im Unternehmen vorhanden?
- ☐ Können Veränderungen zeitnah eingepflegt werden?
- ☐ Liegen Dokumentationen der Hersteller zu den verwendeten Softwarelösungen (Benutzerhandbuch, Administrationshandbuch usw.) vor?
- ☐ Wurden die vom Hersteller gelieferten Dokumentationen durch die Darstellung der individuellen Anpassungen ergänzt?

1.8 Ablauf der Verfahrensdokumentation



Es muss eine umfassende Beschreibung der Prozesse im Unternehmen vorgenommen werden, die sich nicht nur auf Abläufe, Vorgänge und Programmbenutzung beschränkt, sondern beschreibt, welche Geräte eingesetzt werden und wie und von wem diese genutzt werden.

2 Allgemeine Beschreibung zur Organisation und Aufgabenstellung

Nachfolgend nehmen sie eine allgemeine Beschreibung zur Organisation und Aufgabenstellung des Unternehmens vor. Geben Sie einen Überblick über die relevanten Geschäftsprozesse und eine Zuordnung zur Aufbau- und Ablauforganisation vor und setzten Sie einen Verweis auf die relevanten rechtlichen Grundlagen.

Allgemeine Beschreibung des Einsatzgebietes	
Darstellung der Organisation *Art des Unternehmens, Rechtsform, geltende rechtliche Grundlagen und relevante Compliance-Anforderungen*	
Standort *Adressangaben*	
Aufbauorganisation *Beschreibung der allgemeinen und steuerbezogenen Aufbauorganisation (evtl. grafisches Ablaufdiagramm)*	
Ablauforganisation *Beschreibung des fachlichen und technischen Ablaufs im Betrieb (evtl. grafisches Ablaufdiagramm)*	
Ansprechpartner *Aufstellung der relevanten Ansprechpartner in der Organisation*	

3 Allgemeine Beschreibung zur Anwendung

Die nachfolgende Checkliste gibt Ihnen eine Übersicht der fachlichen Beschreibungen zu den unterschiedlichen Aufgabenbereichen. Es sollte eine leicht verständliche Gebrauchsanweisung für den Anwender darstellen, damit auch Dritten (z.B. einem Betriebsprüfer) die dargestellten Prozesse schnell verständlich sind.

Allgemeine Beschreibung des Einsatzgebietes	
Beschreibung zur sachgerechten Bedienung der IT-Anwendung	
Beschreibung der abgedeckten Aufgabenbereiche	
Beziehungen zwischen verschiedenen Modulen	
Beschreibung der Eingabeerfordernisse und Ausgaberegeln	
Beschreibung der Verarbeitungsregeln	
Beschreibung der eingerichteten Kontrollen und Fehlerbehandlung	
Beschreibung der Rahmen, Aufgabenstellung und Richtlinien	
Organisationsbeschreibung	
Auflistung der Dokumentenbestände	
Beschreibung der Verarbeitungsregeln	
Vorgehensweise bei Vernichtung von Papier- und sonstigen Originaldokumenten	
Beschreibung der Übernahme für elektronisch eingehender Dokumente	
Behandlung von E-Mails	
Vorgehensweise bei elektronischen Signaturen	

4 Technische Systemdokumentation

Die Übersicht enthält eine allgemeine Beschreibung der eingesetzten Hardware, der Vernetzung und der Software. Hier muss die technische Infrastruktur dokumentiert werden. Listen Sie auf, welches Betriebssystem im Einsatz ist und wie viele Clients und Server eingesetzt werden. Auch die Auflistung der einzelnen Softwareanwendungen ist darzustellen. Insbesondere bei der Softwaredokumentation ist darauf zu achten, welche Programmversionen aktuell eingesetzt werden.

Technische Soft- und Hardwaresysteme	
Speichersysteme	
Erfassungssysteme	
Ausgabesysteme	
Server-Hardware / -Software	
Client-Hardware / -Software	
Grafische Systemdarstellung	
Individualsoftware	
Schnittstellen	
Netzwerk-Systembeschreibung	
Elektronische Signatur	
Langzeitverfügbarkeit / Migrationsfähigkeit *Die steuerrelevanten Daten müssen über den Zeitraum der Aufbewahrungsfrist verfügbar sein.* *- Online-Verfügbarkeit der Daten* *- Offline-Verfügbarkeit der Daten (Datenarchivierung, Sicherungsbänder)* *- Beschreibung der Vorgehensweise bei der Löschung oder Archivierung von prüfungsrelevanten Informationen aus den führenden Anwendungen* *- Sicherstellung der Auswertungsmöglichkeiten nach der Löschung aus dem führenden System*	

4.1Datensicherheitskonzept

Über ein Datensicherungskonzept sind insbesondere die Verfahren und Prozeduren der Datensicherung zu dokumentieren.

- ☐ Was ist zu sichern?
  - Software (Betriebssystem und Anwendungssoftware)
  - Tabellen- und Stammdaten
  - Bewegungsdaten
  - Sonstige Aufzeichnungen
- ☐ Wogegen ist zu sichern?
  - Datenverlust
  - Unberechtigte Veränderung
  - Unberechtigte Kenntnisnahme

4.2 Sicherung gegen Verlust

- ☐ Übersicht der Übersicht der Datensicherungsprozeduren
  - Vorkehrungen gegen Verlust der Sicherungen vornehmen:
  - Unauffindbarkeit (systematische Verzeichnisse über die gesicherten Programme und Datenbestände mit Standort, Inhalt, Datum der Sicherung und frühestes Datum der Löschung)
  - Vernichtung (physische Sicherung gegen Feuer, Temperatur, Feuchtigkeit, Magnetfelder z.B. durch örtliche Trennung etc.)
  - Diebstahl (verschlossene Räume, Tresore, externe Lagerung)
- ☐ Test der Lesbarkeit bei Langzeitlagerung

4.3 Sicherung gegen unberechtigte Veränderung

Ergreifen Sie Maßnahmen, die zum Schutz der Daten oder Datenkategorien führen:

- ☐ **Zutrittskontrolle**
  Unbefugten ist der Zutritt zu den Datenverarbeitungsanlagen, auf denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Diese Kontrolle bezieht sich auf den physischen Zutritt. Er kann z. B. durch verschlossene Türen zum Serverraum oder durch den Einsatz eines Pförtners bewerkstelligt werden.
- ☐ **Zugangskontrollen**
  Es ist zu verhindern, dass Datenverarbeitungsanlagen von Unbefugten genutzt werden

können. Die Zugangskontrolle wird am Computer üblicherweise durch die Eingabe von Login- Namen und Passwort realisiert. Sie kann aber auch mit Magnet- oder Chipkarten sichergestellt werden.

☐ **Zugriffskontrolle**
Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können. Außerdem muss gewährleistet sein, dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Diese Befugnis zum Zugriff kann sich zum Beispiel bei Mitarbeitern aus der innerbetrieblichen Organisation ergeben. Umgesetzt werden kann sie im EDV-Bereich z. B. durch differenzierte Berechtigungen bei der Nutzung von Software. Beispiel: Daten der Buchhaltung dürfen nur von dieser selbst, aber nicht von der Vertriebsabteilung eingesehen werden. Die Zugriffskontrolle ist getrennt zu betrachten von Zutrittskontrolle und Zugangskontrolle.

☐ **Weitergabekontrolle**
Hiermit soll verhindert werden, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transportes oder ihrer Speicherung auf Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können. Zudem soll überprüft und festgestellt werden können, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen der Datenübertragung vorgesehen ist. Die Weitergabekontrolle betrifft deswegen in der Praxis insbesondere Daten, die über Netzwerke fließen. E-Mails, die personenbezogene Daten enthalten, sind im Rahmen der Weitergabekontrolle zu schützen (in der Praxis oftmals mittels Verschlüsselung).

☐ **Eingabekontrolle**
Unter Eingabekontrolle versteht man, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungsanlagen eingegeben, verändert oder entfernt worden sind. Dies geschieht in der Regel durch eine automatische Protokollierung der Eingaben in Logfiles. Elemente einer Protokollierung sind der betroffene Datensatz, die Art der Aktivität (Anlage, Veränderung, Löschung des Datensatzes), der Zeitpunkt der Aktivität bzw. des Ereignisses sowie ausführende Person (Benutzerkennzeichen). Die Eingabekontrolle setzt eine funktionierende Zugangskontrolle voraus.

☐ **Auftragskontrolle**
Die Kontrolle ist nur anwendbar, wenn eine Auftragsdatenverarbeitung nach § 11 BDSG vorliegt. Ein Auftrag liegt dann vor, wenn die Daten durch eine andere juristische Person nach genauen Vorgaben verarbeitet werden (Beispiel: externe Buchhaltung). In diesem Fall ist vertraglich und ggfs. durch Kontrollen sicherzustellen, dass die personenbezogenen Daten nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

☐ **Verfügbarkeitskontrolle**
Unter Verfügbarkeitskontrolle versteht man, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust zu schützen sind. In der Regel geschieht dies durch fachgerechte regelmäßige Datensicherungen, aber auch durch einen Notfallplan, Virenschutz und andere Maßnahmen.

☐ **Trennungsgebot**
Das Trennungsgebot ist ein Grundsatz, nach dem zu unterschiedlichen Zwecken erhobene Daten auch nur getrennt verarbeitet werden dürfen. Deshalb ist z. B. der Test-Datenbestand strikt zu trennen vom Produktiv-Datenbestand

5 Betriebsdokumentation

Nach § 9 BDSG muss sich im Unternehmen eine Abteilung verantwortlich um die technischen und organisatorischen Sicherheitsmaßnahmen kümmern, um eine datenschutzgerechte Verarbeitung personenbezogener Daten sicherzustellen.

Tragen Sie in der Übersicht die entsprechend zuständigen Mitarbeiter ein. Tragen Sie in der Übersicht die entsprechend zuständigen Mitarbeiter ein.

Betriebsdokumentation	
Dokumentation der ordnungsgemäßen Anwendung des Verfahrens	
Datensicherungsverfahren	
Verarbeitungsnachweise	
Freigabeverfahren für neue/geänderte Software	
Auflistung der eingesetzten Programme mit Versionsnachweis	

6 Mitarbeiterqualifikation

Alle Mitarbeiter erhalten eine Unterweisung in die jeweiligen Prozesse sowie eine Schulung zur ordnungsgemäßen Bedienung der eingesetzten IT-Systeme bzw. erhalten entsprechende Qualifizierungsmaßnahmen. Die unterwiesenen Mitarbeiter verpflichten sich (durch Unterzeichnung eines Protokolls) zur Einhaltung dieser Verfahrensdokumentation.

Mitarbeiterqualifikation	
Rollen	
Erforderliche Kenntnisse	
Verantwortlichkeiten	
Qualifizierungsmaßnahmen	
Dokumentation der Qualifikationen und Maßnahmen	

7 Prozessbeschreibung

In den einzelnen Prozessschritten dokumentieren Sie die Arbeitsschritte sowie die Art und Weise der Ausführung. Alle Änderungen sind zu protokollieren, z.B. wenn sich Zuständigkeiten ändern.

Prozesse	
Übernahme von Papierdokumenten	
Vernichtung von Papieroriginalen	
Übernahme originär digitaler Dokumente	
E-Mail-Dokumente	
Massendatenverarbeitung	
Elek. signierte Dokumente	
Indexierung/Verschlagwortung	
Archivieren	
Recherche & Zugriff	
Check-in/Check-out	
Bearbeitung und Versionierung	
Löschen	
Verfahrensdokumentation	
Fortschreibung des IKS	
Kontrolle & Auswertung des IKS	

7.1 Ersetzendes Scannen

Der Prozess zum Ersetzenden Scannen muss die einzelnen Bearbeitungsschritte genau dokumentieren, damit klar ist, wer Dokumente wann, wo und auf welche Weise bearbeitet hat. Alle Änderungen sind zu protokollieren, z. B. wenn ein neuer Scanner oder eine neue Programmversion installiert wird.

Die Mitarbeiter, die mit dem Scanprozess befasst sind, müssen entsprechend geschult werden. Das bezieht sich auf die Arbeitsschritte Vorbereitung, Digitalisierung, Archivierung, Kontrolle, Freigabe und Vernichtung.

Falls nicht der gesamte Prozess im Unternehmen stattfindet, sondern ein Teil davon von anderen Stellen übernommen wird (Steuerberater, Scan-Dienstleister usw.), muss genau dokumentiert werden, wer für welche Prozessschritte zuständig ist.

Der Steuerpflichtige sollte daher eine Organisationsanweisung erstellen. Im Allgemeinen empfiehlt sich, die einzelnen Prozessschritte des Verfahrens zum Ersetzenden Scannens in grafischer Form darzustellen:

- ☐ Zu welchem Zeitpunkt wird gescannt (z. B. beim Posteingang, während oder nach Abschluss der Vorgangsbearbeitung)
    - Bei Posteingang: Vorsortierung der Dokumente inklusive Echtheitsprüfung
    - Wer darf scannen
- ☐ Identifikation der zu scannenden Belege
    - Welches Schriftgut wird gescannt
    - Ist eine bildliche oder inhaltliche Übereinstimmung mit dem Original erforderlich
- ☐ Vorbereitung und Digitalisierung der Belege
- ☐ Kontrolle auf Vollständigkeit, Lesbarkeit, Plausibilität
    - Protokollierung von Fehlern
- ☐ Nachverarbeitung und Archivierung mit Integritätssicherung
- ☐ Freigabe zur Vernichtung der Papierbelege
- ☐ Dokumentation, wer die Papierbelege vernichtet
- ☐ Freigabe zur Löschung der digitalen Archivbestände nach Ende der Aufbewahrungsfrist
- ☐ Löschung der digitalen Archivbestände

Hinweis: Besonders schutzwürdige Dokumente sollten nur einem besonders bezeichneten Personenkreis zugänglich sein (z.B. Lohnbuchhaltungsdaten).

7.2 Datenübermittlung

Hier sind die Übermittlungen, auch soweit bislang nur geplant, in Drittstaaten (Nicht-EU-Länder bzw. Nicht-EWR-Länder) anzugeben und zu begründen.

Dabei sind Name der Drittstaaten und die übermittelten Daten zu benennen.

7.3 Löschkonzept zur Datenminimierung

Im Datenschutzrecht besteht eine gesetzliche Verpflichtung für Unternehmen personenbezogene Daten zu löschen, wenn diese für die Zwecke, für die sie ursprünglich erhoben oder verarbeitet wurden, nicht mehr erforderlich sind und zudem auch keine gesetzliche Aufbewahrungspflicht der Löschung entgegensteht.

Durch die neue Datenschutzgrundverordnung (DSGVO) wurden diese Löschpflichten nochmals erheblich erweitert. Bei Nichtbeachtung drohen jetzt hohe Bußgelder.

Daher ist die Implementierung eines DSGVO konformen Löschkonzepts eng mit der Umsetzung handels- und steuerrechtlicher sowie weiterer Aufbewahrungspflichten verbunden (GoBD), die ebenfalls eine genaue Kenntnis der Datenflüsse im Unternehmen und ggfs. eine Bestandsaufnahme erfordern. So lässt sich z.B. ein Widerspruch gegen den Erhalt von E-Mail-Werbung nur durch Löschung bestimmter Daten umsetzen.

7.4 Löschkonzept erstellen

Für jede Abteilung des Unternehmens sollte erfasst werden, welche personenbezogenen Daten dort verarbeitet werden. Welche Daten werden auf welchen Systemen gespeichert? Gibt es ein zentrales System für Stammdaten?

Die erhobenen Daten sollten verschiedenen Kategorien zugeordnet werden, für die jeweils die gleiche Aufbewahrungsdauer gilt. Dabei sollte danach unterschieden werden, ob es sich um besondere personenbezogene Daten handelt, da hier weitere Einschränkungen gelten können.

Personenbezogene Daten sollten nur so lange gespeichert werden, wie dies unbedingt notwendig ist. Daher sollte für jede Kategorie anhand von Erhebungsdatum, voraussichtlicher (durchschnittlicher) Bearbeitungszeit und dem Beginn der jeweiligen Aufbewahrungsfrist eine Löschregel bestimmt werden. Es ist sinnvoll, die Anzahl der Löschregeln möglichst gering zu halten.

8 Internes Kontrollsystem (IKS)

Laut GoBD hat der Steuerpflichtige ein internes Kontrollsystem einzurichten, auszuüben und zu protokollieren. Die Beschreibung des Kontrollsystems gehört zur erforderlichen Verfahrensdokumentation.

Die Ausgestaltung des Kontrollsystems ist abhängig von der Komplexität und Diversifikation der Geschäftstätigkeit und der Organisationsstruktur sowie des eingesetzten Datenverarbeitungssystems.

Zum Kontrollverfahren gehören u. a. Zugangs- und Zugriffsberechtigungskontrollen, Erfassungs- und Plausibilitätsprüfungen, Verarbeitungskontrollen sowie Schutzmaßnahmen gegen die beabsichtigte und unbeabsichtigte Verfälschung von Programmen, Daten und Dokumenten.

Internes Kontrollsystem	
Organisatorische Sicherheitsmaßnahmen	
Technische Schutzmaßnahmen	
Dokumentation aktueller Änderungen	
Revision des IKS	
Zuordnung von Verantwortlichkeiten	

9 Glossar: Abkürzungen und Bedeutungen

AO:
Abgabenordnung – schreibt vor, welche Aufbewahrungsfristen beachtet werden müssen.

Basel II:
Der Begriff bezeichnet die Eigenkapitalvorschriften des Basler Ausschuss für Bankenaufsicht. Nach Basel II müssen die Kreditnehmer in Systeme und Prozesse investieren, welche die Verfügbarkeit aller ratingrelevanten Informationen sicherstellt.

BDSG:
Bundesdatenschutzgesetz – regelt unter anderem die Löschfristen personenbezogener Daten.

GDPdU:
Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen – legen fest, dass das Datenverarbeitungssystem die Unveränderbarkeit der Daten gewährleisten muss.

GoB:
Die Gesamtheit aller GoB wird häufig als „Grundsätze ordnungsmäßiger Buchführung und Bilanzierung“ bezeichnet- Die Anerkennung einer Buchführung und deren Aufzeichnungen setzt die Beachtung der GoB voraus.

GoBD:
Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie Datenzugriff - Definiert die Anforderungen an DV-Systeme aus steuerlicher Sicht

GobS:
Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme

HGB:
Handelsgesetzbuch – legt fest, welche handelsrechtlich relevanten Dokumente überhaupt archiviert werden müssen und dürfen.

Indexierung
Eineindeutige Verknüpfung zwischen einem digitalen Dokument und einem Kriterium für das Wiederauffinden dieses Dokuments.

Inhouse-Format
Unternehmensinternes Format zur Datenspeicherung.

SOX:
Sarbanes-Oxley Act – regelt die Haftung der verantwortlichen Manager für die Jahresabschlüsse US-börsennotierter Unternehmen.

Sage GmbH
Franklinstraße 61 – 63
60486 Frankfurt am Main

+49 69 50007-0
info@sage.de

www.sage.com

© Sage GmbH. Alle Rechte vorbehalten. Sage, dass Sage Logo sowie hier genannte Sage Produktnamen sind eingetragene Markennamen der Sage Global Services Limited bzw. ihrer Lizenzgeber. Alle anderen Markennamen sind Eigentum der jeweiligen Rechteinhaber. Technische, formale und druckgrafische Änderungen vorbehalten.