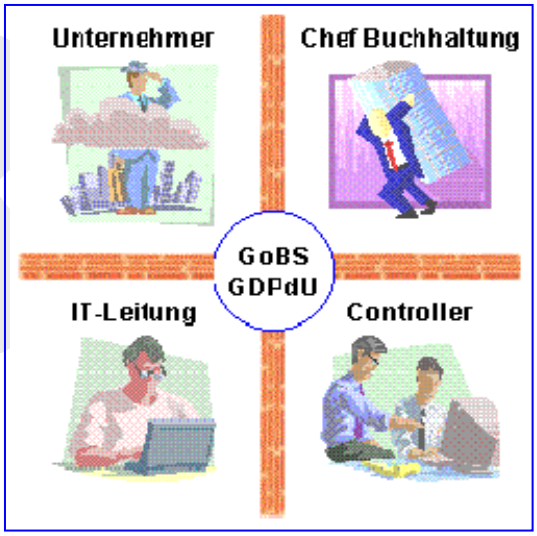
GDPdU und die Archivierung steuerlich relevanter Daten

Das Bundesministerium für Finanzen hat die „Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU) erlassen und am 1. Januar 2002 traten dazu die Änderungen der Abgabenordnung (AO) in Kraft. Es ist seitdem den Finanzbehörden möglich, unmittelbar auf die EDV-Systeme im Unternehmen zuzugreifen und digitale Belege aus dem Buchhaltungssystemen auf Datenträgern zu fordern. Ebenso gelten seit 1995 die Grundsätze ordnungsmäßiger dv-gestützter Buchführungssysteme (GoBS)[1], die darüber hinaus auch die Datensicherheit und authentische Wiedergabe der auf Datenträgern geführten Unterlagen fordern.

Situation

Bei den GoBS und GDPdU handelt es sich um Vorschriften mit Gesetzeskraft. Handels- und Steuerrecht fordern die Einhaltung der GoBS ein. Die GoBS fordern die integre Aufzeichnung der Geschäftsvorfälle der elektronischen Buchführung und deren umfassende Dokumentation.



Ziel der GoBS: Die Außenprüfer sollen sich, um die Prüfung effizient durchführen zu können, in der DV-Buchführung schnell zurechtfinden - möglichst ohne Hilfe.
Ziel der GDPdU: Alle steuerrelevanten, originär digitalen Daten aus Anlagen-, Lohn- und Finanzbuchhaltung sind in maschinell auswertbarer Form vorzuhalten, um diese mit IT-Mitteln zu prüfen.

Im Unternehmen: Für die Unternehmen ergibt sich eine eigenwillige Situation. Der Buchhalter muss sich plötzlich mit Technologie befassen, die IT-Mannschaft mit Gesetzestexten und das Controlling mit bestehenden oder neuen Geschäftsvorfällen. Mit Mühen und Kosten aufwendig integrierte ERP-, Archivierungs- und Dokumentenmanagement-systeme müssen GoBS-dokumentiert und GDPdU-fähig gemacht werden. Die Schwierigkeiten einer abteilungsübergreifende Kooperation in sachfremden Themen auf der Basis schwer verdaulicher Texte führen dazu, dass die Umsetzung der GoBS und GDPdU kaum vorangeht.

Veränderung durch GDPdU: Bis zum Jahre 2002 waren die GoBS die grundlegende gesetzliche Handhabe der Finanzbehörden zur Einforderungen einer umfassenden und prüffähigen Dokumentation der DV-Buchführung.
Mit den GDPdU ändert sich die Situation fundamental: Die Finanzbehörde greift selbst zu IT- Mitteln und steigt mit elektronischen Werkzeugen in das Zahlenmaterial der Steuerpflichtigen ein. Die GoBS erlangen unerwartet neues Gewicht. Denn ein Einstieg in die DV-gestützte Buchführung und maschinelle Auswertung der Daten nach GDPdU bedarf einer detaillierten Dokumentation. Diese wurde zwar bislang für die elektronische Buchführung ohnehin schon verlangt, ging aber bei Datenbanken und Datenstrukturen nie derart in die Tiefe, wie es jetzt erforderlich wird. Die Unternehmen kommen um Kosten nicht herum. Im Falle der Betriebsprüfung ist der Aufwand, die Prüfer über das System zu informieren, nicht geringer, als die systematische Vorbereitung.

[1] GoBS::= Grundsätze ordnungsmäßiger dv-gestützter Buchführungssysteme

Sichtung der Daten - Systeme - Strukturen - Abläufe

Das ist eine sehr komplexe Aufgabenstellung, die unter Umständen mehrere Abteilungen in einem Unternehmen involviert. Verschiedene Zuständigkeitsbereiche sind betroffen und eine pedantische Vorgehensweise ist dabei anzuraten. Praktikabel hierbei hat sich folgende Vorgehensweise bewährt:

1. Erfassung aller IT-Systeme und Sub-Systeme inklusive aller Einzelkomponenten (**Anlagenregister**)

2. Erfassung aller Verfahren und Datenbankstrukturen, mit bzw. auf denen steuerlich relevante Daten verarbeitet werden (**Verfahrensregister**)

3. Erfassung aller steuerlich relevanten Daten inkl. Datenstrukturen (**Datenregister**)

4. Erfassung aller vergebenen "Rechte" (**Rechte-Register**)

5. **Datenstromanalyse** gemäß "IT-Grundschutzhandbuch" des Bundesamt für Sicherheit in der Informationstechnik (BSI).

Extraktion und Archivierung steuerrelevanter Daten

Im Rahmen der steuerlichen Außenprüfung darf die Finanzbehörde ausschließlich auf Daten, die für die Besteuerung von Bedeutung sind, zugreifen.
Dies umfasst die Daten der

- Finanzbuchhaltung (FIBU),
- Anlagenbuchhaltung und
- Lohnbuchhaltung
- sonstige steuerlich relevante Daten (email, Excel-sheets)

Für die Prüfung müssen die originär digitalen Unterlagen in (irgend-)einem Datenverarbeitungssystem (DV-System) bis zum Abschluss der Außenprüfung, mindestens jedoch 10 Jahre vorgehalten werden. Mit originär digitalen Unterlagen sind die in einem DV-System in elektronischer Form eingehenden oder in einem DV-System erzeugten Daten gemeint. Daten, die über die genannten drei Buchhaltungsbereiche hinausgehend sich in anderen Bereichen des Datenverarbeitungssystems befinden und steuerlich relevant sind, sind ebenfalls nach Maßgabe der steuerlichen Aufzeichnungs- und Aufbewahrungspflicht zu qualifizieren und für den Datenzugriff in geeigneter Weise vorzuhalten.

Alle papiernen Dokumente, die zur Belegung von Buchungen mit steuerlich relevanten Daten fungieren, müssen gem. §147 der Abgabenordnung über mindestens zehn Jahre in den bestehenden Archiven wie bisher vorgehalten werden.

Zunächst sind die Daten zu identifizieren, die für die Besteuerung von Bedeutung sind. Laut BMF gibt es keine allgemeingültige Definition des Begriffs „steuerlich relevant“. Je nach Einzelfall können Daten bei einem Steuerpflichtigen von steuerlicher Bedeutung sein, bei einem anderen jedoch nicht. Der Begriff wird wie folgt umschrieben: Steuerlich relevant sind Daten immer dann, wenn sie für die Besteuerung des Steuerpflichtigen von Bedeutung sind.

Datenextraktion

Die GDPdU-Daten stammen aus den Buchhaltungssystemen oder -Anwendungen und können durch einen Extraktionsmechanismus bereit gestellt werden. Diese Funktionalität fällt in den Zuständigkeitsbereich des Herstellers oder Lieferanten.

Dieser kennt die interne Applikationslogik und Strukturen, die für den Extrakt der GDPdU-Daten vonnöten sind. Auf Knopfdruck oder durch sonstige Funktionselemente, die nun als Anwendungsstandard zu erwarten sind, werden die steuerlich relevanten Daten extrahiert. Dies kann täglich z.B. per Batch-Job oder ggf. in anderen Periodizitäten geschehen.

Die entstandenen Dateien mit allen verknüpften Struktur- und Formatinformationen können anschließend der Archivierung zugeführt werden. Die steuerrechtlich relevanten Daten werden in Form von Dateien, die gemäß dem Beschreibungsstandard des BMF und audicon strukturiert sind, an einen Archivierungsmechanismus weitergereicht bzw. für die Zugriffsmöglichkeit Z3 verarbeitet.

Beschreibungsstandard

In Zusammenarbeit mit Herstellern von Entgeldabrechnungs-, Finanzbuchhaltungs- und Archivierungssystemen sowie dem deutschen Vertrieb der Prüfsoftware „IDEA“ hat die Finanzverwaltung eine einheitliche technische Bereitstellungshilfe zur Format- und Inhaltsbeschreibung der steuerlich relevanten Daten entwickelt. Die festgelegten Strukturen basieren auf den CSV- und XML-Formaten. Durch diesen Beschreibungsstandard des BMF und audicon (vgl.a. http://www.bundesfinanzministerium und http://www.audicon.net) können die steuerlich relevanten Daten als Extrakt aus den ERP-Systemen im einheitlichen und offen gelegten Format erwartet und weiterverarbeitet werden.

Archivierung von Formatbeschreibungen
Originäre digitale Unterlagen werden durch Übertragung ihrer Inhalte und den jeweiligen gültigen Formatbeschreibungen auf einen digitalen Datenträger archiviert.

Zwischenspeicherung von Arbeitsergebnissen
Nicht aufbewahrungspflichtig sind die während der maschinellen Verarbeitung durch das Buchführungssystem erzeugten Dateien, sofern diese ausschließlich einer temporären Zwischenspeicherung von Verarbeitungsergebnissen dienen und deren Inhalte im Laufe des weiteren Verarbeitungsprozesses vollständig Eingang in die Buchführungsdaten finden. Voraussetzung ist jedoch, dass bei der weiteren Verarbeitung keinerlei Verdichtung steuerlich relevanter Daten vorgenommen wird (Fragen und Antworten zum Datenzugriffsrecht der Finanzbehörde, BMF Schreiben, Stand 06.03.03).

GDPdU-konforme Archive:

Die in den DV Systemen erzeugten originären digitalen Daten müssen für einen Zeitraum von elf Jahren (das aktuelle und die letzten zehn abgeschlossenen Jahre) auswertbar vorgehalten werden. Das Vorhalten der steuerlich relevanten Daten sollte in einem Archivsystem erfolgen. Das Archivsystem muss die Anforderungen, die sich aus den Vorgaben der „Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen“ (GDPdU) und den „Grundsätzen ordnungsgemäßer DV-gestützter Buchführungssysteme“ (GoBS, Abschnitt V und VIII) über Datensicherheit und Wiedergabe der auf Datenträgern geführten Unterlagen ergeben, erfüllen.

Datenzugriffsrecht und Datenträgerüberlassung
Die GDPdU konkretisiert §147 (6) der AO der Finanzbehörde. Danach müssen die drei folgenden Zugriffsmöglichkeiten auf digitale Unterlagen zur Verfügung stehen:

- unmittelbares Zugriffsrecht (Z1),
- mittelbares Zugriffsrecht (Z2)

- und die Datenträgerüberlassung (Z3).

Die Entscheidung, von welchen Zugriffsmöglichkeiten die Finanzbehörde Gebrauch macht, steht in ihrem Ermessen. Daher müssen durch die Systemlösung alle drei Zugriffsmöglichkeiten realisiert

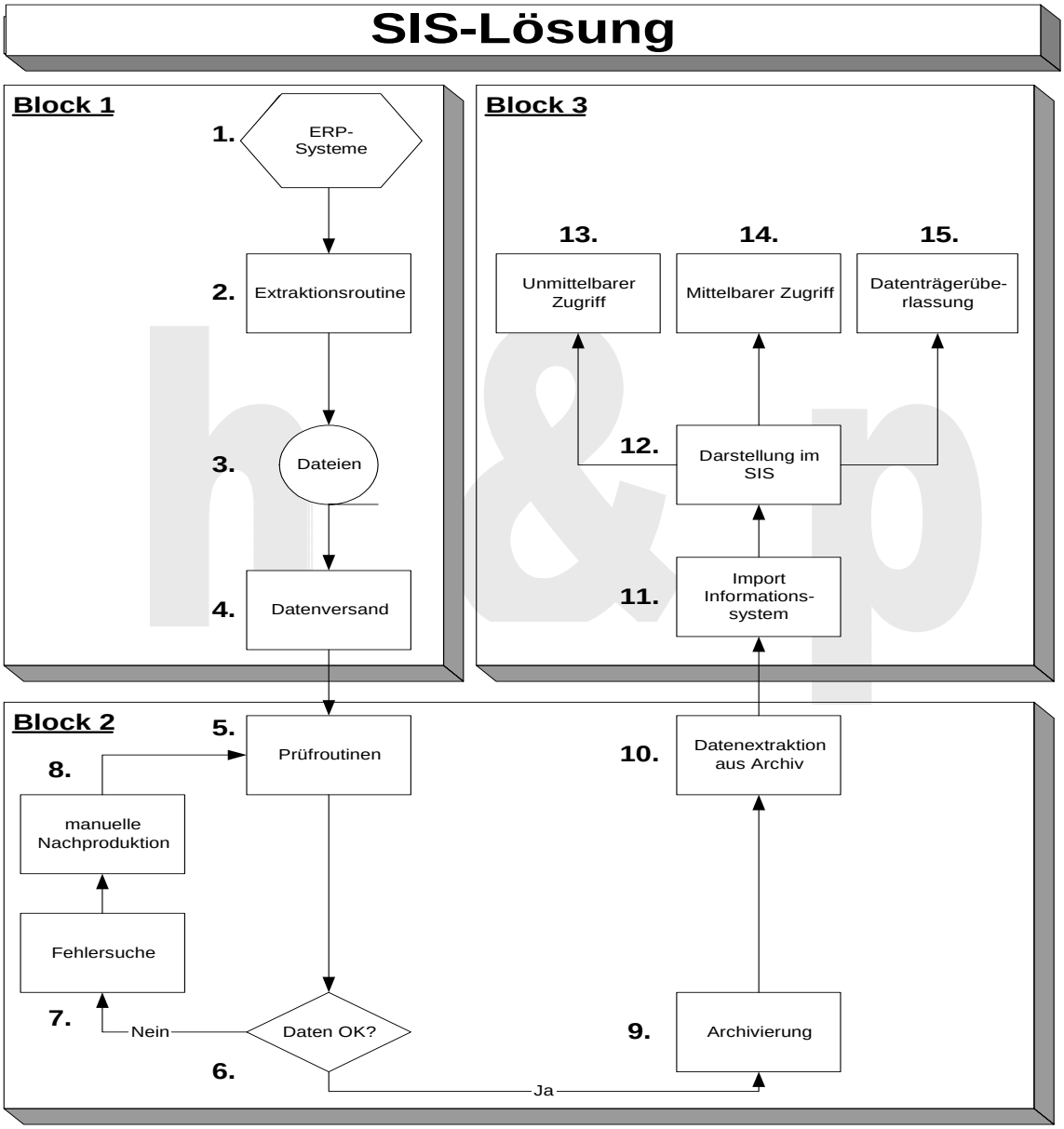
werden. Insbesondere ist darauf zu achten, dass der Finanzbehörde der Zugriff nur auf steuerlich relevante Daten (gemäß aktueller Gesetzeslage) ermöglicht wird. Alle kundenbezogenen Daten sind entweder nicht anzuzeigen oder so zu anonymisieren, dass ein Rückschluss auf den Kunden nicht möglich ist.

Um die gesetzlichen Anforderungen zu erfüllen, ist es möglich die in den Legacy-Systemen erzeugten steuerlich relevanten Daten in einem optischem Archiv für 11 Jahre vorzuhalten (ggf. unter Berufung auf §148 AO). Steht eine steuerliche Außenprüfung bevor, so werden die Daten der angeforderten Jahre aus dem Archiv in ein Informationssystem importiert und dort dem Prüfer zu Verfügung gestellt. Die geforderte „maschinelle Auswertbarkeit“ von Daten ist durch ein Archivsystem gegeben, wenn das Archivsystem in quantitativer und qualitativer Hinsicht die gleichen Auswertungen ermöglicht als wären die Daten noch im Produktivsystem.

Die Systemlösung zur Erfüllung der gesetzlichen Anforderungen laut **GDPdU** kann dabei in drei Blöcke unterteilt werden (vgl. unten). Im ersten Block werden die steuerlich relevanten und zusätzlichen Daten aus dem Legacy-Systemen extrahiert und in Schnittstellendateien abgelegt. Diese Dateien werden anschließend mittels eines Dateitransfermechanismus an einen zentralen Archivserver übertragen. Die zu archivierenden Daten müssen die von den **GDPdU** gestellten Anforderungen erfüllen (vgl.a. oben).

Nach der Übertragung auf einen Archivserver, werden die übertragenen Daten auf syntaktische Korrektheit geprüft und für die Dauer von 11 Jahren auf optischen Medien archiviert. Dieser Prozess umfasst den Block 2 der Systemlösung.

Block 3 der Systemlösung beinhaltet die Bereitstellung der steuerlich relevanten Daten zur steuerlichen Außenprüfung. Dies umfasst den Import der archivierten Daten in ein Informationssystem und die anschließende Präsentation der steuerlich relevanten Daten. Die Darstellung beinhaltet die von den Finanzbehörden geforderten Datenzugriffe (mittelbarer Zugriff, unmittelbarer Zugriff und Datenträgerüberlassung). Durch den Import zusätzlicher Daten, neben den steuerlich relevanten, können hier auch erweiterte Reports für den Fachbereich realisiert werden. Das folgende Diagramm zeigt die Komponenten bzw. Blöcke und die einzelnen Bearbeitungsschritte der Lösung einer Infrastruktur für GDPdU-konforme Archive. Besonders erwähnenswert neben Block 1 (Extraktions-System) und neben Block 2 (Archivierungs-System) ist der dritte Block das Audit- and Balancing-System (ABS - im Sinne eines Recherche- oder Datawarehouse-Systems):



In den einzelnen Blöcken werden die folgenden Schritte durchgeführt:

Block 1

1. Alle relevanten (Buchhaltungs-)Systeme mit steuerlich relevanten Daten stellen Programme zu Extraktion dieser Daten bereit.

2. Periodische Extraktionen steuerlich relevanten Daten aus dem beteiligten Systemen und Bereitstellung in Schnittstellendateien.

3. Die Schnittstellendateien haben bestimmte Formate. (vgl.a. Beschreibungsstandard des BMF und audicon)

4. Die Dateien werden von dem jeweiligen System mittels Dateitransfer an einen Archivserver übertragen.

Block 2

5. Auf dem Archivserver findet eine Prüfung statt, ob alle erwarteten Dateien übertragen worden sind (Vollständigkeitsprüfung). Anschließend werden eine syntaktische Format- und Integritätsprüfung dieser Dateien durchgeführt.
   Dieser Vorgang wird protokolliert.

6. Sind die Prüfungen erfolgreich durchgeführt, dann weiter mit Punkt 9, sonst mit Punkt 7.

7. Stellt eine der Prüfroutinen einen Fehler fest, dann wird automatische eine Protokoll E-Mail an den Administrator des Systems verschickt. Dieser muss den Fehler analysieren und unter Umständen Daten in den Basissystemen nachproduzieren lassen.

8. Manuelle Bereitstellung der Daten.

9. Archivierung der geprüften Daten auf optischen Medien.

10. Steht eine Steuerprüfung an, dann müssen die Daten für einen definierten Zeitraum (Prüfungsanordnung) aus dem Archiv extrahiert werden.

Block 3

11. Import der Daten in ein Audit and Balancing-System.

12. Nach dem Import der Daten in das Audit and Balancing -System stehen die Daten für eine Steuerprüfung zu Auswertung bereit.

13. Über Filter-, Sortier- und Aggregationsfunktionen des Audit and Balancing -Systems wird dem Prüfer der Zugriff auf die steuerlich relevanten Daten ermöglicht. Hiermit wird der mittelbare Datenzugriff (Z2) und die Anforderung realisiert.

14. Der Prüfer kann über vordefinierte Abfragen auf Daten zugreifen und damit den unmittelbaren Datenzugriff (Z1) durchführen.

15. Über eine Exportfunktion können Daten aus dem Audit and Balancing -System auf einem externen Speichermedium abgelegt werden. Hiermit wird die Zugriffsart Datenträgerüberlassung (Z3) realisiert. Sowohl die steuerlich relevanten Daten als auch die Beschreibungsdaten werden auf einem gemeinsamen Datenträger zur Verfügung gestellt. Diese Daten können dann in die Analyse-Software des Betriebsprüfer importiert und ausgewertet werden.

Einbau in die bestehenden Netze

Die GDPdU-Dateien sollen von den verschiedenen Systemen an den Server des Archivsystems gesendet werden können. In der vorhandenen Netzwerkstruktur sollen Standardprotokolle und Systemkomponenten genutzt werden können, so dass mittels eines gesicherten Dateitransfers die GDPdU-Dateien auf dem Server empfangen und archiviert werden können. Ein produktives System soll in der Lage sein, die Archivobjekte zu recherchieren und wieder aus dem Archiv wiederherzustellen. Dazu muss es möglich sein, mit einem typischen PC-Client auf das Serversystem zugreifen zu können.

Archivierungsmechanismus

Die GDPdU-Dateien sollen auf den Server gelangen und dort als Archivobjekte automatisch archiviert werden. Das Archivierungskonzept soll mehrere logisch oder physikalisch getrennte Archive ermöglichen. Die Daten verschiedener Mandanten müssen verteilt und getrennt voneinander einer Langzeitarchivierung überführt werden können. Das Archivsystem soll hierzu eine Art Pool-Bildung erlauben. Bei der Konzeption des Systems und für die Umsetzung ist diese Mandantenfähigkeit vorgesehen worden, so dass systemtechnisch keine Umbaumaßnahmen vorzunehmen sind.

Datentransfer
Die GDPdU-Dateien sollen von den verschiedenen Systemen an den Server des Archivsystems gesendet werden können. Entsprechende Jobs sollen zu bestimmten Zeitpunkten den gesicherten Dateitransfers der GDPdU-Dateien zu dem Server anstoßen. Nach dem automatisierten Empfang soll die weitere Verarbeitung der GDPdU-Dateien erfolgen.

Dateinamensschema und Struktur:

Die steuerlich relevanten Daten liegen in Dateiform vor. Als Format wird ASCII mit fixer Feldlänge verwendet. Die Trennzeichen der einzelnen Datensätze (=Belegzeilen) sind mit Zeilenumbruch festgelegt. Folgende Konventionen werden bei der Verwendung der ASCII-Dateien eingehalten:

- Die Datei besteht ausschließlich aus Datensätzen ohne Überschriften.
- Die Datumsangaben müssen dem Format YYYYMMDD und Zeitangaben dem Format hhmmss entsprechen. Trennzeichen sind nicht darin enthalten.
- Die Dezimaltrennzeichen werden mittels Kommata „,“ dargestellt, z.B. ist die Schreibweise für 1 Euro und 50 Cent dann „1,50“. Es sind hierbei sämtliche Nachkommastellen zu übertragen.
- Negative Zahlen werden mit einem führenden Minuszeichen „-„ dargestellt (z.B. „–100,50“) und positive Zahlenwerte erhalten ein Plus „+“ als Vorzeichen. Die Zahlen werden innerhalb ihres Datenfeldes rechtsbündig dargestellt. Zu beachten ist auch, dass das Vorzeichen dem Betragsfeld vorangestellt ist und dort sowohl das "-" als auch das "+" abgelegt sein muss.
- Erreichen die Füllung der Daten in den Datenfeldern aufgrund ihrer Formatvorgaben nicht die Maximalgrenze, so sind diese restlichen Feldern mit Leerzeichen aufzufüllen. In den ASCII-Dateien sind die einzelnen Datenfeldern direkt hintereinander abgelegt.
- Der in den ASCII-Dateien zu verwendende Zeichensatz soll sich auf die darstellbaren Zeichen beschränken, d.h. nur sichtbare Zeichen aus der ASCII-Codepage und keine Steuerzeichen oder dergleichen.

- Die Inhalte der einzelnen Datenfelder werden ohne Trennzeichen sequentiell dargestellt. Die Ausnahme von dieser Regel bildet das jeweils letzte Datenfeld der Zeile. Hiernach folgt kein weiteres Datenfeld, sondern ein Zeilenumbruch. Im Text durch „<***Zeilenumbruch***>“ kenntlich gemacht. Für den Aufbau bedeutet das nun, dass die jeweils gleichartigen Zeilen in sich durch den „<***Zeilenumbruch***>“ voneinander getrennt sind und jede Sequenz der Datenfelder als Zeile in der Datei erscheint.

- Die Extraktions-Routine geht bei der Erzeugung der Dateien von einer festen Struktur aus (feste Anzahl von Datenfeldern fixer Länge). Sind in einem Datenfeld keine Daten gespeichert, so sind sogenannte Leerzeichen einzufüllen. Die Anzahl der Datenfelder und die der Zeichen muss in jeder Datei konstant sein.

Allgemeine Anforderungen an Schnittstellendateien
Im Archiv sollen die steuerlich relevanten Daten im ASCII Format mit fester Feldlänge vorliegen. Die Werte sind nach CSV (Comma Separated Values) strukturiert. Dies hat den Vorteil, dass dieses Format sowohl bei der Archivierung, wie auch bei dem Import ins Informationssystem Zukunftssicher ist. D.h., es ist nicht von einem spezifischen Archiv- oder Informationssystemformat abhängig, so dass eine Migration auf andere Technologien einfacher zu gestallten ist. Auf der Seite der Zuliefersysteme erreicht man ebenfalls eine Unabhängigkeit von einem speziellen System- oder Betriebssystemformat. Eine Migration der Systeme ist hier ebenfalls einfacher zu gestallten. Hierdurch wird die Anforderung der GDPdU auf Zugriff der Daten auch nach einem Systemwechsel erfüllt.

Kontroll- und Archivierungsprogramm
Für die automatisierte Archivierung der GDPdU-Dateien ist ein bestimmter Algorithmus gefordert. Zu einem bestimmten Zeitpunkt (z.B. jeden Morgen eines Banktags zwischen 6 und 8 Uhr) soll überprüft werden, ob alle geforderten Dateien erfolgreich übersendet worden sind. Hiernach sollte für jede empfangene Datei eine Verarbeitungsliste durchlaufen werden, die die notwendigen Funktionen aufruft. Nach dem Empfang ist z.B. eine dekomprimierte Datei zu entpacken. Danach soll das Format der Datei und der Belegzeilen überprüfen werden. Der letzte Schritt in der Liste ist die Übergabe der GDPdU-Datei an das Archivsystem. Das Archivierungsprogramm selbst soll die GDPdU-Datei nehmen und dem optischen Archiv übergeben. Eine Überprüfung auf Fehlen oder das doppelte Vorkommen einer Datei ist im Weiteren gefordert.

Prüfprogramm
Wenn morgens die Archivierung angestoßen wurde, so kann am Mittag die Archivierung geprüft werden. Dieses Programm überprüft, ob alle empfangenen und zur Archivierung übergebenen Dateien ins Archiv gelangt sind. Die Liste der archivierten Dateien soll mit der Liste der zu erwartenden GDPdU-Dateien abgeglichen werden. Alle relevanten Daten sollen dem Administrator zugesandt werden. Das Prüfprogramm nach einer gewissen Zeit nach den Archivierungsläufen gestartet werden.

Dateien und deren Funktionalität
Die Liste der zu erwartenden GDPdU-Dateien ist in Dateiform mit einem gut pflegbaren Standard zu implementieren. Diese Datei soll von dem Archivierungsmechanismus als eine Art „Abhakliste“ für die von den verschiedenen Systemen gesendeten Dateien benutzt werden. Für jede GDPdU-Datei soll eine Aufgabenliste – ebenfalls in Dateiform – referenziert werden. In dieser weiteren Liste stehen alle Arbeitsschritte für die jeweilige Datei. Eine Status-Datei soll über den aktuellen Bearbeitungstand jeder GDPdU-Datei Buch führen und abschließend als Information dem Administrator zukommen. Diese Informationen sollen sich alle aus der jeweiligen „index.xml“-Datei ableiten, die als Beschreibungsdatei nach dem Standard des BMF und audicon strukturiert zu den GDPdU-Dateien im CSV-Format abgelegt worden ist. Ein Log-Mechanismus schreibt fortwährend eine Datei, die bei Bedarf jeden Funktionsaufruf und jede Rückmeldung protokolliert.

Suchprogramm
Die Verwaltungsdaten der Archivobjekte werden auf dem Archivserver gespeichert. Die Suche bzw. das Extrahieren der Dateien ist daher mittels der Funktionen des ABS (Audit and Balancing-System) durchzuführen. Das Resultat einer Recherche soll in Form einer Ergebnisliste präsentiert werden, in der man einzelne oder alle Treffer markieren kann. In dieser Liste soll man einzelne oder alle Treffer markieren können. Eine weitere Funktion soll den Export der markierten GDPdU-Dateien auslösen. Die so aus dem Archiv exportierten GDPdU-Dateien stehen auf dem Dateisystem des Archivservers zur Verfügung.

Manuelles Archivieren
Der tägliche Lauf des Kontroll- und Archivierungsprogramm soll automatisch jeden Morgen angestoßen werden. Aufgrund verschiedener Umstände kann aber der Bedarf einer nachträglichen Bearbeitung oder Archivierung bestehen, so dass es möglich sein muss, die Archivierungsfunktion manuell aufzurufen. Ein Shell-Kommando mit den geeigneten Optionen und Parametern soll einem Administrator ermöglichen, den Archivierungsmechanismus per Hand zu starten.

Zugriffsschutz
Aus Datenschutz- und revisionstechnischen Gründen ist ein Zugriffsschutz der Daten der jeweiligen Mandanten notwendig.

Zugriffsschutz Server

Der Archivserver muss gegen unbefugten Zugriff und Manipulationen geschützt sein. Das komplette Archivsystem und seine Daten sind gemäss Anforderungen der Datensicherheit und des Datenschutz auszulegen. Das Zugriffsberechtigungskonzept der technischen User soll auf dem UNIX-Server des Archivsystems analog implementiert werden.

Zugriffsschutz Daten

Die GDPdU-Dateien müssen nach den Qualifiern und nach der Mandantentrennung getrennt empfangen werden. Die Dateien sollen unabhängig voneinander zwischengespeichert und archiviert werden. Ferner müssen die Zugriffsprofile dergestalt sein, dass ein Administrator nur auf den von ihm zu verwaltenden Datenbestand Zugriff haben darf. Entsprechend sind die Benutzerprofile und Zugriffsberechtigungen umzusetzen.

Fehlerbehandlung
Für jede Datei, die jeden Morgen eines Banktages erwartet wird, gibt es einen Eintrag in einer Liste, die von dem Kontroll- und Archivierungsprogramm abgearbeitet wird. Der Bearbeitungsstatus der jeweiligen Datei soll sich in einer Status-Datei nachsehen lassen. In einer Log-Datei sollen die einzelnen Arbeitsschritte protokolliert werden, so dass im Fehlerfall der letzte Funktionsaufruf und die mögliche Fehlerursache besser nachvollzogen werden kann. Nach jedem Lauf des Prüfprogramms, das die Archiveinträge abfragt, soll eine Notifikation in Form einer E-Mail an den Administrator bzw. E-Mail-Account gesendet werden. Inkorrekte Abläufe oder Fehlerfälle sollen dabei gesondert gekennzeichnet sein.

Folgende Fehlerfälle sollen programmtechnisch „abgefangen“ und einem Administrator gemeldet werden:

- Ausbleiben einer Datei: Es wird eine GDPdU-Datei erwartet, die bis zu dem letzten Lauf des Kontroll- und Archivierungsmechanismus nicht eingetroffen ist. Diese Datei kann nicht verarbeitet und nicht archiviert werden.
- Fehler beim Zugriff auf diese Datei: Auf die GDPdU-Datei kann nicht zugriffen werden. Es fehlen die Zugriffsberechtigungen oder sie kann z.B. defekt sein.

- Fehler bei der Dekompression: Bei der Dekomprimierung einer zuvor gepackten Datei tritt ein Fehler auf. Die Ursache kann ein Lese- oder Schreibfehler oder ein falsches Format sein.

- Fehler beim Überprüfen des Dateiformats: Es ist ein Fehler im Format der GDPdU-Datei gefunden worden. Die Datenfelder sind nicht bzgl. ihrer Länge laut Vorgaben der Beschreibung in der Meta-Datei gefüllt. Ferner können fälschlicherweise Zeichen in vorkommen, die außerhalb des Bereichs der darstellbaren ASCII-Zeichen liegt.
- Fehler bei der Archivierung: Bei der Archivierung ist ein Fehler aufgetaucht. Der Archivierungsvorgang konnte z.B. nicht ordnungsgemäß angestoßen worden oder der Aufruf Dienstes kommt direkt mit einer Fehlermeldung zurück.
- Fehler durch das nochmalige Vorkommen einer Datei: Eine GDPdU-Datei wird nochmalig in das Empfangsverzeichnis des Servers abgelegt. Die doppelte Existenz ist in dieser Situation aufgrund des Kontextes nicht vorgesehen und würde eine Kollision in dem Datenbestand des Archivs bedeuten. Die Datei darf nicht archiviert werden und erzeugt eine Fehlermeldung, die auch in der E-Mail-Notifikation an den Administrator vorkommen soll.
- Fehler durch zu viele Dateien: In dem Empfangsverzeichnis des Servers sind Dateien angelegt worden, die nicht in der Dateiliste der zu archivierenden GDPdU-Dateien verzeichnet sind. Für diese Dateien gibt es keine TODO-Liste und können somit auch nicht verarbeitet werden. In diesem Fall muss diese Fehlersituation geklärt werden und ggf. manuell nacharchiviert werden.

Folgendes Diagramm verdeutlicht den Ablauf des Archivierungsmechanismus. Im Weiteren werden die einzelnen Punkte im Detail erläutert.

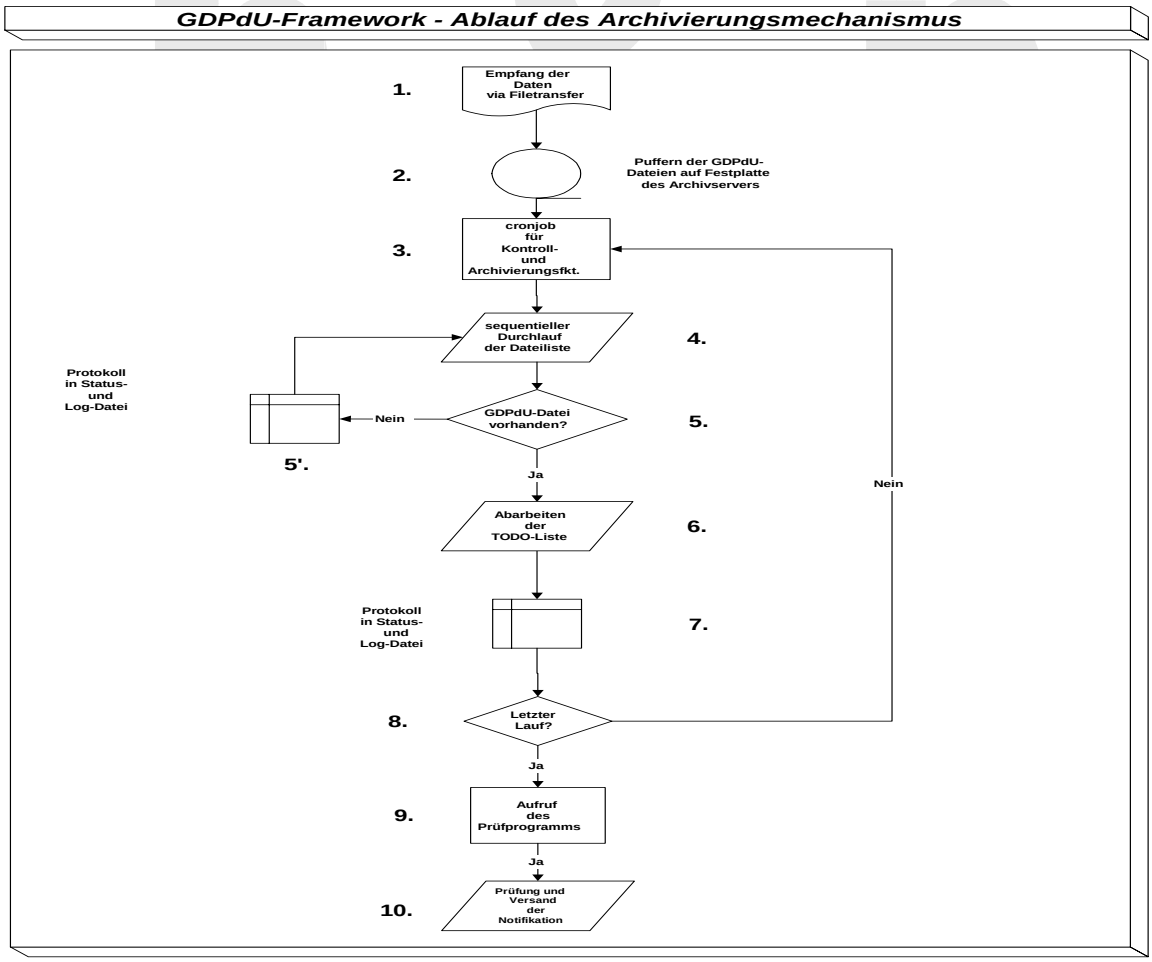
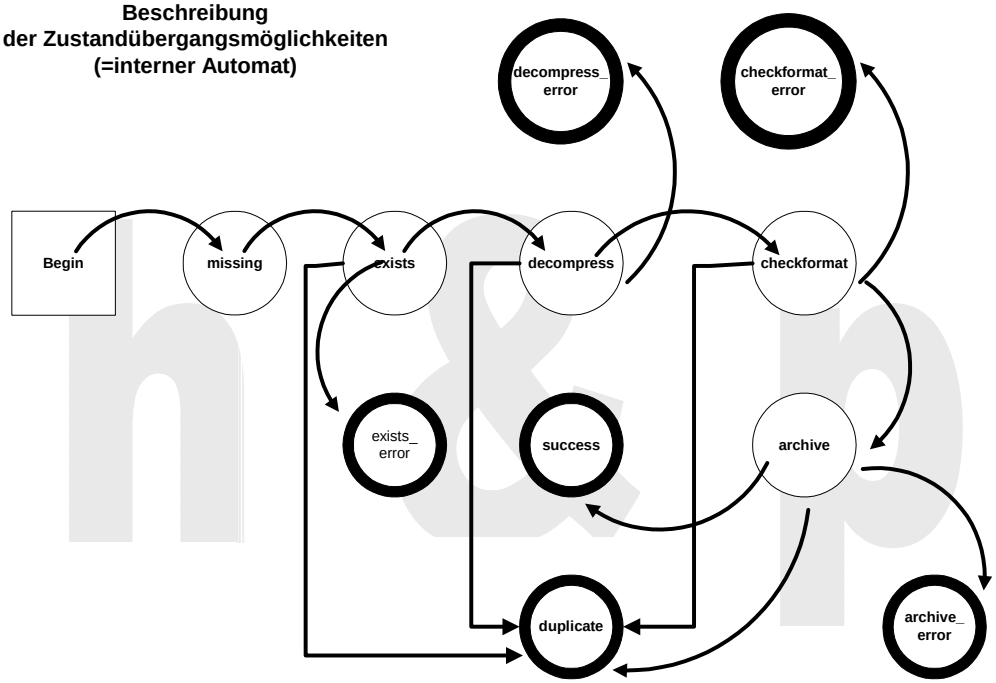


Abbildung 1: Schema des Archivierungsmechanismus

Zur automatischen Archivierung der gesendeten und zu speichernden GDPdU-Dateien startet jeden Morgen eines Tages z.B. zwischen 6 und 8 Uhr - alle halbe Stunde – ein z.B. per cronjob gestartetes Kontroll- und Archivierungsprogramm.
Dieses Programm überprüft, ob alle geforderten Dateien erfolgreich übersandt worden sind. Die Informationen, welche Dateien zu überprüfen sind, befinden sich in einer Dateiliste auf dem Archivserver und als Aufrufparameter für das o.g. Programm mitgegeben wird.

Folgendes Schema stellt den Automaten dar. Für jede GDPdU-Datei wird ein Eintrag in der Datei „status.properties“ erzeugt. Der konkrete Name der Datei wird aus dem ggf. generischen Angaben aus „filelist.xml“ berechnet und abgeleitet. Aus dem abgeleiteten Dateinamen – die Datei befindet sich in Bearbeitung bzw. wird für die Abarbeitung herangezogen – entsteht ein Eintrag in der „status.properties“.

Beschreibung der Zustandübergangsmöglichkeiten (=interner Automat)



Log-Datei

Der Name der Log-Datei lautet „Logfile.log“. Für jedes Element in der Liste der Dateinamen, das in der Datei „filelist.xml“ aufgeführt ist, gibt es einen Eintrag in der Datei „status.properties“. Für jede Funktion der Verarbeitungskette, die für die GDPdU-Datei aufgerufen wird, kann es einen Eintrag in der Log-Datei geben. Wie eloquent die Meldungen und Einträge sind, wird über den sogenannten Log-Level geregelt. Die möglichen Level sind:

- Level 0, nicht eloquent, nur Fehler oder Abbrüche werden geloggt.
- Level 1, wichtige Funktionsaufrufe, Warnings und Fehler werden geloggt.
- Level 2, alle Funktionsaufrufe und Fehler werden geloggt.

In der Betriebsbeschreibung für diesen Archivierungsmechanismus werden weitere Details und Beispiele enthalten sein. All die oben beschriebenen Dateien, die den Kontrollfluss des Archivierungsmechanismus steuern, sind unter dem Verzeichnis **/exchange/steuerarchiv/** abgespeichert und nur mit besonderen Administrationsberechtigungen änderbar.

Rollenkonzepte
Neben den erwähnten Benutzer ist noch der Administrator des Archivsystems zu nennen. Dieser hat uneingeschränkte Zugriff auf sämtlich Ressourcen, inklusiver aller Dateien und somit auch auf allen GDPdU-Daten. Für diesen Benutzer ist es nur im Ausnahmefall vorgesehen, in das produktive System einzugreifen. Im Normalfall werden mit getrennten Benutzern die GDPdU-Dateien produziert und mit dieser Trennung auf Server-Seite die Dateien empfangen und abgelegt. Das Dienstprogramm zur Archivierung läuft unter eigener Kennung und hat einen wohldefinierten Funktionsumfang. Es können unbefugtes Lesen und die Manipulation von Daten ausgeschlossen werden.