

# Rechtsgutachten

## windream Archivsystem

Revisionssicherheit  
des windream Archivs  
bei Einsatz veränderbarer  
und unveränderbarer Medien

Deutschland  
Österreich

**Prof. Dr. Wolfgang Hackenberg**  
**Dr. Ivo Geis**

windream GmbH  
Wasserstraße 219  
44799 Bochum  
Deutschland

**Copyright** © 2023

Überreicht von:  
windream GmbH  
Wasserstr. 219  
44799 Bochum

Stand: 06/2023 - V1.05

Alle Rechte vorbehalten. Kein Teil dieser Beschreibung darf in irgendeiner Form (Druck, Fotokopie oder einem anderen Verfahren) ohne Genehmigung der windream GmbH reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden.

### **Wichtige Hinweise**

Alle Informationen und technischen Angaben dieser Beschreibung wurden von den Autoren mit größter Sorgfalt zusammengetragen. Sie können jedoch weder Garantie noch juristische Verantwortung oder irgendeine Haftung für Folgen, die auf fehlerhafte Angaben zurückgehen, übernehmen.

Wir weisen darauf hin, dass die in dieser Beschreibung verwendeten Soft- und Hardwarebezeichnungen und Markennamen der jeweiligen Firmen im Allgemeinen einem Warenzeichen-, Marken- oder Patentrechtsschutz unterliegen.

# Revisionssicherheit des windream Archivs bei Einsatz veränderbarer und unveränderbarer Medien

Von:

Rechtsanwalt Dr. Ivo Geis  
Glockengießerwall 26  
20095 Hamburg

Rechtsanwalt Prof. Dr. Wolfgang Hackenberg  
Robert-Koch-Straße 7  
72800 Eningen unter Achalm



# Inhalt

---

## Rechtsgutachten windream Archivsystem

---

|          |  |           |
|----------|--|-----------|
| <b>1</b> | <b>Auftrag Dr. Ivo Geis, 2011</b>  | <b>1</b>  |
| <b>2</b> | <b>Auftrag Prof. Dr. Wolfgang Hackenberg, 2018, 2020 und 2023</b>  | <b>2</b>  |
| <b>3</b> | <b>Sachverhalt – Allgemeines zu windream und zum windream Archiv</b>   | <b>3</b>  |
| 3.1      | Das windream Archiv  | 8         |
| 3.2      | Die Ablage von Daten bei der Anbindung an windream   | 9         |
| 3.3      | windream Langzeitarchiv  | 10        |
| 3.4      | Pool-Container, BLOB-Container und BLOB  | 11        |
| 3.4.1    | Pool und Pool-Konzept  | 11        |
| 3.4.2    | BLOB-Container   | 13        |
| 3.4.3    | BLOB   | 14        |
| 3.4.4    | Löschen von Dokumenten aus dem Archiv  | 17        |
| 3.5      | Zusätzliche rechtsrelevante Aspekte der windream-Versionen 6.0 und 6.5   | 18        |
| 3.5.1    | Single Instance Storage (SIS) / Dublettenprüfung   | 18        |
| 3.5.2    | Veränderbare Attribute nach der Archivierung assoziierter Dokumente  | 19        |
| 3.5.3    | Kennzeichnung der Attribute als „revisionssicher“  | 19        |
| 3.5.4    | windream Secure Time-Dienst  | 20        |
| <b>4</b> | <b>Rechtliche Bewertung</b>  | <b>22</b> |
| 4.1      | Vertragsabschluss durch E-Mail-Kommunikation   | 22        |
| 4.2      | Aufbewahrung elektronischer Dokumente  | 23        |
| 4.2.1    | Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff | 24        |
| 4.2.2    | Basel II, Sarbanes Oxley Act und Dokumentationspflicht   | 27        |
| 4.2.3    | Zwischenergebnis   | 29        |
| 4.3      | Ordnungsmäßigkeit des windream Archivs   | 29        |
| 4.3.1    | Speichern der Dokumente im Archivsystem  | 29        |
| 4.3.2    | Ordnungsgemäße Indexierung   | 30        |
| 4.3.3    | Integrität der Dokumente durch das Checksummensystem   | 32        |
| 4.3.4    | Ordnungsmäßige Speicherung   | 32        |
| 4.3.5    | Lesbarmachung  | 33        |

|       |   |    |
|-------|---|----|
| 4.3.6 | Ordnungsmäßige Verfahrensdokumentation  | 34 |
| 4.3.7 | Ergebnis für windream   | 34 |
| 4.4   | Die Beweisqualität elektronischer Dokumente   | 34 |
| 4.4.1 | Freie Beweiswürdigung   | 34 |
| 4.4.2 | Beweisqualität der ordnungsmäßigen Archivierung   | 35 |
| 4.4.3 | Die Beweisfunktion des windream Archivsystems   | 35 |
| 4.5   | Die Rechtslage in der Republik Österreich   | 35 |
| 4.5.1 | Republik Österreich   | 35 |
| 4.5.2 | Zwischenergebnis  | 37 |
| 4.6   | Rechtssicherheit des integrierten Enterprise-Content-Management-Systems windream nach den rechtlichen Kriterien der Republik Österreich | 37 |
| 4.6.1 | Das Recht der elektronischen Archivierung der Republik Österreich im Vergleich mit dem Recht der Bundesrepublik Deutschland             | 37 |
| 4.6.2 | Fazit   | 38 |

---

## **5 Ergebnis der rechtlichen Begutachtungen Deutschland, Österreich**

**39**

|     |  |    |
|-----|--|----|
| 5.1 | Ergebnis der Prüfung durch Dr. Ivo Geis                  | 39 |
| 5.2 | Ergebnis der Prüfung durch Prof. Dr. Wolfgang Hackenberg | 40 |

---

## **6 Literaturverzeichnis und Abkürzungen**

**41**

|     |             |    |
|-----|-------------|----|
| 6.1 | Literatur   | 41 |
| 6.2 | Abkürzungen | 41 |

# 1 Auftrag Dr. Ivo Geis, 2011

Die windream GmbH, Wasserstraße 219, Bochum, hat mich beauftragt, das windream ECM-System mit dem integrierten windream Archivsystem rechtlich zu begutachten. Hierfür lag mir die Dokumentation sowie auch die Software von windream und des windream Archivsystems in den u. g. Versionen vor. Die Software wurde geprüft, und die Übereinstimmung der Funktionalitäten mit der Dokumentation wurde festgestellt. Für Informationen standen mir der Geschäftsführer der windream GmbH, Herr R. David, und der Leiter der Dokumentationsabteilung, Herr Dr. M. Duhme, zur Verfügung. Das Gutachten für die windream-Versionen 3.6 und 4.0 sowie für die Archiv-Version 6.0 wurde von Juni bis Oktober 2006 erstellt. Die Prüfung der windream Version 5.0 erfolgte von 16.05.2011 bis zum 20.05.2011.

Folgende Versionen der Software wurden betrachtet:

windream Version 3.6, Version 4, Version 5,

windream Archiv Version 6.

## **2 Auftrag Prof. Dr. Wolfgang Hackenberg, 2018, 2020 und 2023**

Die windream GmbH, Wasserstraße 219, Bochum, hat mich beauftragt, das windream ECM-System mit dem integrierten windream Archivsystem rechtlich zu begutachten. Hierfür lag mir die Dokumentation sowie auch die Software von windream und des windream Archivsystems in den u. g. Versionen vor. Die Software wurde geprüft, und die Übereinstimmung der Funktionalitäten mit der Dokumentation wurde festgestellt. Für Informationen zu den Gutachten der Jahre 2018 und 2020 standen mir der Geschäftsführer der windream GmbH, Herr Roger A. David, und der Leiter der Dokumentationsabteilung, Herr Dr. Michael Duhme, zur Verfügung. Das Gutachten für die windream-Version 6.5 sowie für die Archiv-Version 7.1 wurde in dem Zeitraum Dezember 2017 bis April 2018 erstellt. Die Prüfung der windream Version 7.0 erfolgte im Februar 2020.

Für Informationen zum Rechtsgutachten des Jahres 2023 stand mir Herr Stephan Serger, seit Januar 2023 Geschäftsführer der windream GmbH, zur Verfügung. Dieses Gutachten bezieht sich auf die windream-Version 8, die zum Ende des Jahres 2022 freigegeben wurde. Die Prüfung der Version 8 erfolgte im Februar 2023.<sup>1</sup>

Folgende Versionen der Software wurden betrachtet:

windream Version 6.5, Version 7.0,

windream Archiv Version 7.1 sowie

windream Version 8 und windream Archiv 8  
im Februar 2023.

---

<sup>1</sup> Gegenstand des Rechtsgutachtens ist das Archivsystem der windream Version 8. die zum Betrieb erforderliche IT-Infrastruktur, einschließlich Datenbanken, Laufwerkstechnologien oder Schnittstellen zu anderen Systemen sind nicht Gegenstand dessen.



### 3 Sachverhalt – Allgemeines zu windream und zum windream Archiv

Prinzipiell repräsentiert windream eine Enterprise-Content-Management-Software (ECM-Software), die sowohl ein Dokumenten-Management- (DMS) als auch ein Archivsystem in *einem* integrierten System vereint. windream arbeitet auf der Basis der patentierten VFS-Technologie (VFS = Virtual File System), durch die das ECM-System (DMS und Archivsystem) vollständig als erweitertes Dateisystem in das Betriebssystem integriert ist. Dies bedeutet, dass alle Windows-Standardanwendungen direkt und ohne weitere Anpassung auf Dokumente im DMS/Archiv zugreifen oder sie im DMS/Archiv ablegen können. Die folgende Abbildung (*Abbildung 1: DMS/Archiv-Integration in das Betriebssystem*) veranschaulicht die Integration der Software in das Betriebssystem und zeigt die Gliederung in die Bereiche ECM-Client und ECM-Server mit Datenbank (auf der Serverseite).

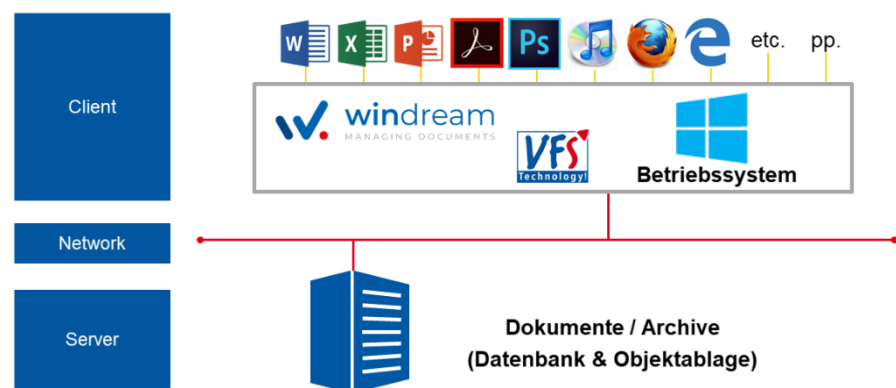


Abbildung 1: DMS/Archiv-Integration in das Betriebssystem

Auf der Clientseite wird windream durch ein virtuelles Laufwerk im Windows Explorer dargestellt. Die Ordnerstruktur dieses Laufwerks ist frei definierbar und kann sowohl bearbeitbare als auch archivierte Dokumente anzeigen. Die Sicht des Anwenders auf die im DMS oder im Archiv enthaltenen Dokumente ist somit immer gleich.

Die folgende Abbildung zeigt die Systemarchitektur von windream in einer etwas technischeren Form.

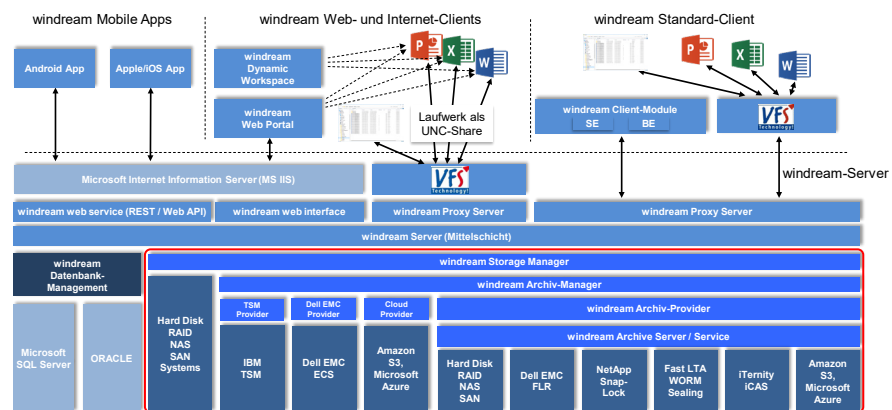


Abbildung 2: Schematische Darstellung der windream-Architektur und des windream Archivs

Hauptbestandteil der rechtlichen Bewertung ist die Art und Weise der Ablage und Verwaltung der Dokumente in windream, in der Darstellung rot markiert. Bestandteil dieses Bereichs ist das windream Archiv, der so genannte windream Objektspeicher<sup>2</sup>.

Die logische Verbindung zwischen dem Dokumenten-Management-System und dem windream Archiv besteht in der windream-Lebenszyklusverwaltung. Sie ermöglicht eine automatisierte Verwaltung der Lebenszyklen aller in windream gespeicherten Dokumente anhand bestimmter Regeln, vom Erstellungsdatum bis zum endgültigen Löschen aus dem Archiv. Die Regeln werden von den Administratoren des Kunden konfiguriert und legen fest,

- wie lange ein Dokument bearbeitet werden kann,
- wo es während der Bearbeitungszeit gespeichert wird,
- wann es archiviert wird,
- wo es während der Archivierungsdauer gespeichert wird,
- wie lange das Dokument im Archiv gespeichert bleibt und
- wann es aus dem Archiv entfernt werden kann oder soll.

Die folgende Abbildung zeigt die Registerkarte *Lebenszyklus* mit der Untergliederung in die Bereiche „Bearbeitbare Dokumente“ und

<sup>2</sup> Die Begriffe *windream Archiv* und *windream Objektspeicher* werden synonym verwendet.

„Archivierte Dokumente“ sowie mit den entsprechend einstellbaren Archivierungsoptionen:

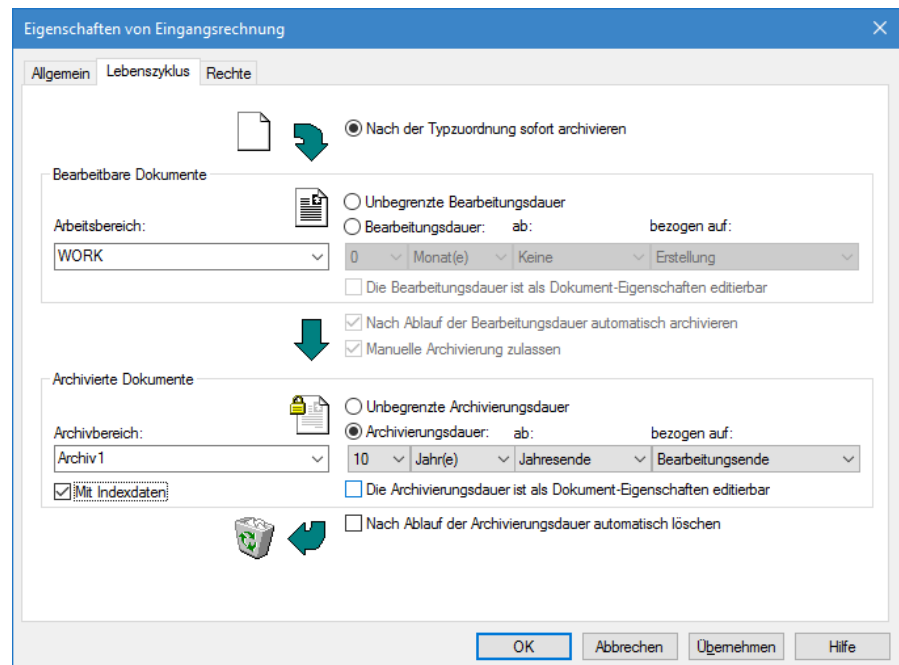


Abbildung 3: Registerkarte *Lebenszyklus* zur Einstellung der Lebenszyklus-Daten (am Beispiel eines Dokumenttyps *Rechnung*)

Nachdem der Bearbeitungszeitraum (falls definiert) eines Dokuments abgelaufen ist, wird es automatisch in das Archiv bzw. in einen definierbaren *Archivbereich* verschoben. Ab diesem Zeitpunkt kann das Dokument – da es archiviert ist – nicht mehr weiterbearbeitet werden; über eine neue Version können Änderungen vorgenommen werden, ohne den alten Stand zu verlieren. Versionen von Dokumenten bilden eine Versionskette, die über eine eindeutige Kennung miteinander verbunden sind.

Wird die Option „Mit Indexdaten“ angekreuzt, so werden nicht nur die Binärobjekte selbst (z. B. ein Microsoft-Word-Dokument), sondern auch alle in windream bekannten Metadaten (Dokumenttyp, Attribute, Rechte, Historie, Versionsinformationen etc.) im XML-Format an das Archiv übergeben und dort in einem Objekt (BLOB) gespeichert. Da somit die Datenbankinformationen eines Dokuments mit dem Dokument archiviert werden, wird diese Option auch „self contained objects“ genannt, da das archivierte Objekt alle beschreibenden Informationen ebenfalls als eigenständigen Objektteil enthält.

Bestandteil der Metadaten in windream ist auch der reine ASCII-Text eines Dokuments, den windream nach der Speicherung eines Dokuments automatisch extrahiert und für die Volltext-Recherche in der Datenbank ablegt.

Speziell für die Archivierung von Dokumenten, die auf jeden Fall nach der Übergabe an windream nicht mehr bearbeitet werden dürfen, bietet windream mehrere Schutzmöglichkeiten:

- Die Option „Nach Typzuordnung sofort archivieren“ führt zu einer direkten Übertragung des Dokuments in den angegebenen Archivspeicher. windream erlaubt aber in diesem Fall noch eine rechtskonforme Nachindizierung der Dokumente (vgl. 3.5.2 *Veränderbare Attribute nach der Archivierung assoziierter Dokumente* und 3.5.3 *Kennzeichnung der Attribute als „revisionssicher“*).
- Auch bei der Definition einer Bearbeitungsdauer kann der Zugriff vor der eigentlichen Archivierung sicher eingeschränkt werden:
  - Durch die Option des Dokumenttyps „Datei nicht bearbeitbar“ wird die Bearbeitung des Dokuments auch bei anderslautenden Rechten auf jeden Fall verhindert.
  - Auf diese Art ist aber eine Nachindizierung des Dokuments für einen Prozessablauf noch gestattet.
  - Durch das Einschränken der Rechte auf das Dokument kann ebenfalls die Bearbeitung des Dokuments auf Administratoren oder den windream-Hauptbenutzer eingeschränkt werden.
  - Auch hier ist eine Nachindizierung des Dokuments dann noch gestattet.

Vor der Übertragung an das windream Archiv wird eine SHA 512 Checksumme (Default nach der Installation; ebenfalls unterstützt: SHA256, MDC2, RIPEMD160) generiert, die dann zur Absicherung

der Übertragung der Daten an das windream Archiv genutzt wird. Dies verhindert eine mögliche Veränderung der Daten während der Übertragung, da das windream Archiv diese Checksumme bei jedem Zugriff prüft. Zusätzlich zur Prüfung über Checksummen kann optional eine Verifizierung der Datenintegrität auch über den Einsatz von Zeitmarken erfolgen. Bei einer Zeitmarke handelt es sich um die aktuelle Zeit aus Datum und Uhrzeit des windream Servers, die zu einem Objekt, wie z.B. einem windream-BLOB oder zu einer Aktion, gespeichert wird (z.B. Logausgaben). Im Kontext dieser Verifizierungsmethode werden mögliche Datenmanipulationen, die durch veränderte Datums- und Uhrzeit-Einstellungen hervorgerufen werden könnten, erfolgreich verhindert. Die vom windream-System vergebene Zeitmarke wird dabei zusätzlich durch eine weitere neutrale Zeitmarke verifiziert, die der windream-Server von einem anderen Server, z.B. außerhalb der eigenen Organisation, bezieht.

In allen o. g. Fällen kann der Verlauf des Dokuments über die windream-Historie nachvollzogen werden. In der Historie werden durch das windream-System in Summe ca. 50 Aktionen automatisch protokolliert. Hierauf hat der Benutzer keinen Einfluss, kann also diese Einträge weder verhindern, noch in irgendeiner Form verändern oder löschen. Der Anwender kann ausschließlich eigene Einträge, z.B. Kommentare, zu der Historie hinzufügen, die dann vom System mit dem Benutzernamen, Datum/Uhrzeit und als Benutzereintrag gekennzeichnet aufgenommen werden. Auch diese Einträge können dann aber nicht mehr verändert oder gelöscht werden.

## 3.1 Das windream Archiv

Das windream Archiv ist integrativer Bestandteil des windream ECM-Systems und wird zur Dokumentenverwaltung und Archivierung eingesetzt. Die Dokumente werden in ihren jeweiligen Originalformaten gespeichert. Optional kann das System von den Dokumenten auch Renditions im PDF/A-Format erzeugen. Das windream Archivsystem unterstützt zwei Arten der Ablage von Objekten:

- Ablage in konfigurierbaren hierarchischen Strukturen und
- Ablage in Form von Containern konfigurierbarer Größe.

Neben der Ablageform können im windream Archiv auch die Zielspeicher frei definiert werden. Das Archiv unterstützt die Speicherung auf folgenden Speichersystemen:

- Festplatten, RAID-Systeme,
- NAS, SAN-Systeme,
- Spezialexsysteme wie Dell EMC Celerra mit FLR, Dell EMC Data Domain mit FLR, Dell EMC VNX mit FLR, NetApp mit SnapLock und FAST LTA Silent Cubes,
- Systeme, die auf der Basis optischer Medien arbeiten.

Anmerkung: Archivsubsysteme (wie z.B. Dell EMC Centera etc.) werden von dem windream ECM-Speichermanagement (vgl. *Abbildung 2: Schematische Darstellung der windream-Architektur und des windream Archivs*) direkt angesprochen, da sie selbst über eine objektorientierte Ablage ähnlich dem windream Archiv verfügen, die somit nicht über das windream Archiv aufgesetzt werden muss.

## 3.2 Die Ablage von Daten bei der Anbindung an windream

windream verwaltet die Dokumente in windream-Speichern. Dies sind

- die „normalen“ windream-Dateiablagen für die Verwaltung der bearbeitbaren Dokumente und
- die windream Archivbereiche für die Verwaltung der archivierten Dokumente.

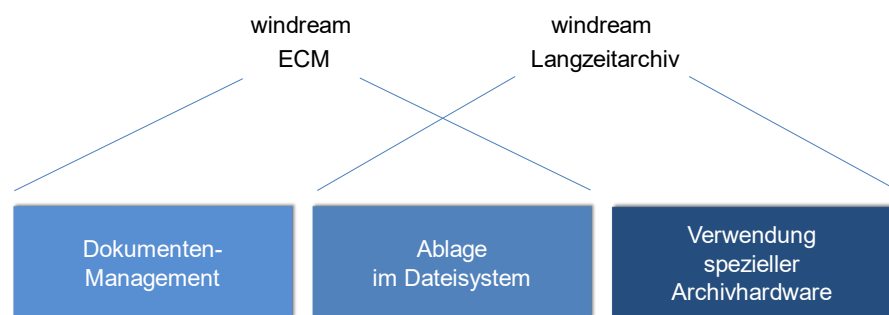


Abbildung 4: windream ECM-System bzw. DMS und Objektspeicher (Langzeitarchiv)

Bei der Konfiguration der Dokumenttypen werden Arbeitsbereiche und Archivbereiche für die zu verwaltenden Dokumente festgelegt (vgl. *Abbildung 3: Registerkarte Lebenszyklus zur Einstellung der Lebenszyklus-Daten (am Beispiel eines Dokumenttyps Rechnung)*). Bearbeitungsbereiche verweisen auf Dateiablagen, in denen die Dokumente innerhalb ihres Bearbeitungszeitraums abgelegt und verwaltet werden. Archivierungsbereiche sind Speicherbereiche, in denen die Dokumente innerhalb des Archivierungszeitraums abgelegt und verwaltet werden.

Auf alle in windream definierten Speicherbereiche wird von dem windream-Kern ausschließlich unter der Benutzerkennung des windream-Hauptbenutzers (windream Mainuser) zugegriffen. Damit kann der Zugriff auf die definierten Speicherbereiche nicht nur auf die Administratoren, sondern sogar ausschließlich auf den windream-Hauptbenutzer eingeschränkt werden. Der windream Hauptbenutzer repräsentiert einen Systemadministrator, der generell mit ausnahmslos allen Rechten ausgestattet ist, die in einem windream-System nach dem Rechtekonzept zur Verfügung

stehen. Er administriert das windream-System ohne jegliche Rechteeinschränkung. Damit ist sichergestellt, dass innerhalb einer windream-Umgebung mindestens ein Benutzer existiert, der das System in vollem Umfang administrieren darf.

### 3.3 windream Langzeitarchiv

Im Falle des windream-Archivs verweisen die windream-Speicher auf Pools des windream-Archivs (vgl. *Abbildung 5: Struktur des windream-Archivs*). In diesen Speicherbereichen werden die Dateien und – optional - die Dokument-Eigenschaften (Meta-Daten) im XML-Format archiviert. Zu den Metadaten, die im XML-Format abgelegt werden, zählen auch die Checksummen und die windream-Zeitmarke zur Verifizierung der Integrität (s.o.).

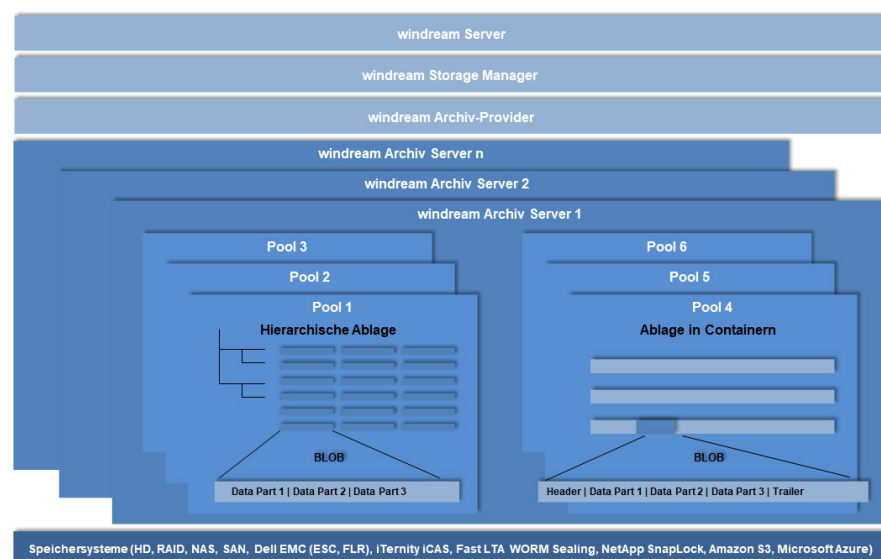


Abbildung 5: Struktur des windream-Archivs

Möglich ist die Ablage der Dokumente in Pools auf Speichersystemen, die einen Share-Zugriff erlauben<sup>3</sup>. Die erforderlichen Pools werden bei der Konfiguration des windream-Archivsystems mit Hilfe der Administrationsanwendung, der windream ObjectStore Management Console, eingerichtet.

<sup>3</sup> Eine Speicherung kann auch auf optischen Medien erfolgen. Dies ist heutzutage jedoch nur noch selten der Fall.



## 3.4 Pool-Container, BLOB-Container und BLOB

Das windream Archivsystem speichert die Daten als BLOBs in den Pools – entweder als einzelne Dateien oder in BLOB-Containern der Pools (vgl. *Abbildung 5: Struktur des windream-Archivs*).

### 3.4.1 Pool und Pool-Konzept

Das windream Archivsystem sichert die Daten (BLOBs) in definierten Speicherbereichen (Pools). Die BLOBs werden in den Pools mit einer eindeutigen BLOB-ID abgelegt. Hierdurch ermöglicht das Poolsystem eine eindeutige Referenzierung archivierter Objekte anhand von BLOB-IDs.

Möglich ist die Ablage der BLOBs sowohl

- in einzelnen Dateien in einem Dateisystem als auch
- gesammelt in BLOB-Containern, die als Datendatei in einem Dateisystem verwaltet werden <sup>4</sup>

Für die verschiedenen Speichermedien existieren entsprechende Pooltypen. Die Speicherorte der BLOBs werden in dem BLOB-Register eines Pools verwaltet.

#### 3.4.1.1 Pools und Pooltypen

Ein Pool ist eine Speichereinheit zur Ablage von logisch ähnlichen BLOBs, z. B. Rechnungen. Ein Pool enthält somit BLOBs, die gleichbehandelt werden sollen. Damit kann einem windream-Dokumenttyp ein bestimmter Pool zugewiesen werden. Pools können auch als Backup- oder Caching-Pools konfiguriert werden, in die Daten für spätere Datensicherungen oder zur temporären Ablage zwischengespeichert werden.

Ein Pool repräsentiert einen Speicherbereich für Dateien in einem Dateisystem (z. B. einer Festplatte). Für die verschiedenen Speichersysteme, die das windream Archivsystem unterstützt,

---

<sup>4</sup> Hinweis: Die Ablage der BLOBs bzw. Container ist auch auf optischen Laufwerken möglich, jedoch kommt diese Technik heute nur noch selten zum Einsatz und gilt als veraltet, da sie weitgehend von moderneren Systemen wie NAS, SAN und sonstigen Festplatten-Arrays abgelöst worden ist.

werden Pools unterschiedlicher Pooltypen verwendet. Als Pooltypen kommen entweder Directory Pools für einzelne Dateien oder FileStream-Pools für BLOB-Container zum Einsatz. Ein Pool kann dann auch mehrere BLOB-Container enthalten.

### 3.4.1.2 Ablauf der Archivierung von BLOBs auf Speichersystemen

Die folgende Grafik zeigt die Prozesse, die ein Dokument als sogenanntes Binary Large Object (BLOB) von seiner Erfassung in windream bis hin zur Archivierung auf Festplatten bzw. Speichersubsystemen durchläuft.

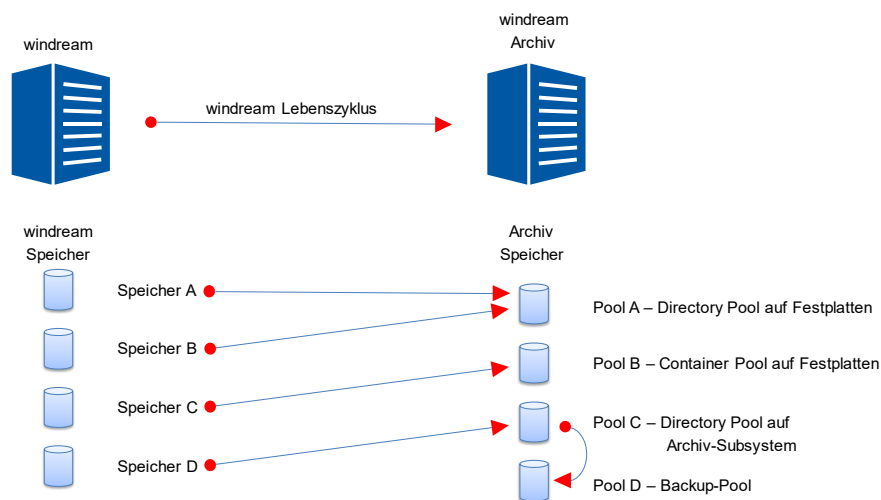


Abbildung 6: Prozess der Archivierung

Die Dokumente werden im windream ECM-System bzw. DMS erfasst bzw. erstellt, indexiert, d. h. mit Objekttypen und weiteren Metadaten versehen, und dann zunächst in windream-Speichern abgelegt. Über den Lebenszyklus wird festgelegt, wie lange ein Dokument zur weiteren Bearbeitung in den windream-Speichern zur Verfügung steht und wann es an das (Langzeit-)Archiv übergeben werden soll. Bei der Archivierung werden die Daten dann als BLOBs bzw. Container in die dafür vorgesehenen Hardware-Archivierungssysteme bzw. Speichersubsysteme mit ihren definierten Archivpools verschoben. Durch den Lebenszyklus wird auch festgelegt, wie lange die Daten im Archiv verbleiben und wann sie gelöscht werden sollen.

Aufgrund der Sicherheitsmechanismen wie z.B. durch den Einsatz von Zeitmarken können die archivierten Daten effizient vor unberechtigter Manipulation geschützt werden (s.o.). Dies bedeutet, dass Dokumente selbstverständlich auch dann geschützt sind, wenn sie auf veränderbaren Hardware-Systemen wie einzelnen Festplatten oder auf modernen Speichersubsystemen von z.B. Dell EMC, NetApp, Fast LTA, HP, IBM und anderen Speichersystemen dauerhaft abgelegt werden. Eine Verbindung zwischen dem windream ECM-System und den Speichersubsystemen der Provider erfolgt über die Einstellungen der Lebenszyklen, die in windream für Dokumente definiert werden können.

#### **3.4.1.3 BLOBs und BLOB-IDs generieren**

Anhand der zugewiesenen Dokumenttypen werden die Dokumente in den entsprechenden Pools des Archivs abgelegt. Dabei werden die BLOBs und für jeden BLOB die zugehörige BLOB-ID generiert.

#### **3.4.2 BLOB-Container**

Ein BLOB-Container oder Volume ist eine Datendatei, in der BLOBs in Filestream-Pools gespeichert werden (vgl. *4.3.4 Ordnungsmäßige Speicherung*). BLOB-Container können sich in Dateien – sogenannten Volume-Files – einer bestimmten Größe oder auf einzelnen Medien befinden. Jeder BLOB-Container besitzt einen Namen (Volume-ID), über den er vom System identifiziert wird. BLOB-Container werden bei der Konfiguration von Filestream-Pools angelegt.

Ein BLOB-Container besteht aus einem Header, der neben Verwaltungsinformationen insbesondere den BLOB-Container identifiziert, und einem Speicherbereich für BLOBs, der mit BLOBs gefüllt wird.

**BLOB-Container / -Volume**

Struktur zur Speicherung der BLOBs

Ein BLOB-Container / -Volume:

- wird durch eine Datei abgebildet, z.B. mit der Bezeichnung  
WMO123\_PERM1\_20040103141021.volume
- oder
- wird durch ein Medium abgebildet, z.B. WORM, MO/WORM

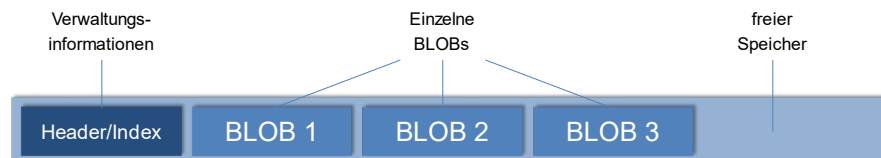


Abbildung 7: BLOB-Container

### 3.4.3 BLOB

BLOB steht für „Binary Large Object“.

Dieses „Binary Large Object“ bezeichnet ein strukturiertes, nicht weiter durch das führende System zu bearbeitendes Binärobjekt, das ein archivierte Dokument in windream repräsentiert und dessen Verwaltung der windream Archivdienst übernimmt.

Ein BLOB besteht aus mehreren Komponenten: einem Header, sogenannten Data Parts (Datenteile) und einem Trailer. Header und Trailer beinhalten interne Verwaltungsinformationen. Die Anzahl und die Inhalte der Data Parts sind abhängig von der führenden Anwendung (hier das windream ECM-System bzw. DMS), mit der das windream Archivsystem eingesetzt wird.

Beim Einsatz des Archivs mit windream enthält der erste Data Part das Dokument, der zweite Data Part die Dokument-Eigenschaften im XML-Format (falls diese Option [„Mit Indexdatei“] ausgewählt wurde – vgl. *Abbildung 3: Registerkarte Lebenszyklus zur Einstellung der Lebenszyklus-Daten (am Beispiel eines Dokumenttyps Rechnung)*) und der dritte Data Part eine Inhaltsübersicht. Ein einzelner Data Part wird über eine vom System vergebene, eindeutige Referenznummer identifiziert. Die einzelnen Data Parts eines BLOBs können von der führenden Anwendung (hier: windream ECM-System bzw. DMS) separat angefordert werden.

**BLOB – Binary Large Object**

Struktur zur objektorientierten Speicherung von Dokumenten im Archiv

Die Struktur besteht aus:

- *Header* mit internen Verwaltungsinformationen
- 1 – n separate *Data Parts* mit den Informationen des Dokuments
- *Trailer* mit internen Verwaltungsinformationen

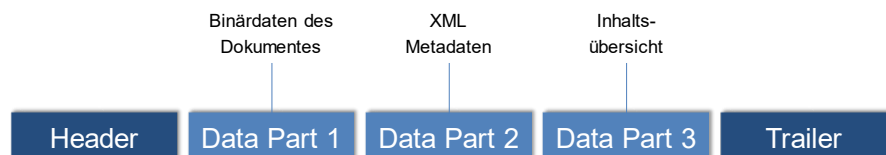


Abbildung 8: Aufbau eines BLOBs – Binary Large Object

**3.4.3.1 Checksummen und windream-Zeitmarke**

Für jeden Data Part wird von dem windream Archiv eine Checksumme generiert, mit der die Authentizität der archivierten Dokumente nachgewiesen wird. Die Generierung der Checksummen erfolgt per Default auf Basis des SHA 512-Standards vor der Übergabe der Daten an das windream Archiv. Bei erfolgreicher Speicherung wird dieser Hash dann in die windream Datenbank übernommen. Bei der Anforderung von Objekten bzw. Dokumenten durch einen Anwender bzw. durch das windream ECM-System respektive windream DMS prüft das windream Archiv die Checksummen der assoziierten Objekte. Falls das System bei der Prüfung Fehler, also eine Dokument-Manipulation feststellt, wird dem Anwender der Zugriff verweigert. Zusätzlich werden autorisierte Administratoren per E-Mail benachrichtigt. Durch die Verwendung von Checksummen, die auch neben dem Archiv in der windream Datenbank gespeichert werden (also an zwei getrennten Orten), können windream-Anwender unabhängig von der Art der aktuell eingerichteten Ablageform und den eingesetzten Speichermedien (vgl. *Abbildung 5: Struktur des windream-Archivs*) nachweisen, dass die gespeicherten Dokumente unverändert bzw. nicht manipuliert sind. Eine zusätzliche Verifizierung der Datenintegrität kann optional auch durch den Einsatz von Zeitmarken erfolgen, die sich wiederum durch den windream Secure Time-Dienst validieren lassen. Somit ist es möglich, Zeitmarken sowohl systemintern als auch von externer Seite als Schutzmechanismus vor Datenmanipulationen in Bezug auf eine

mögliche unautorisierte Manipulation einzusetzen. Die Zeitmarken werden in den Metadaten der Dokumente und somit auch in der windream Datenbank abgelegt.

### 3.4.3.2 BLOB-ID

Den „Binary Large Objects“ (BLOBs) wird jeweils eine BLOB-ID zugewiesen. Die Objekte werden dann entweder als einzelne Dateien in einer hierarchischen Struktur abgelegt oder als Objektsammlung in einem BLOB-Container.

Die BLOB-ID ist ein weltweit eindeutiger Kennzeichner eines BLOBs in einem Objektspeicher. Sie wird vom windream Archiv bei der Archivierung eines BLOBs in einem Pool vergeben. Eine BLOB-ID setzt sich zusammen aus der World-ID, der Pool-ID und einer laufenden Nummer nach dem Muster `<World ID>.<Pool ID>.<lfid.Nr>`. Die World-ID ist ein weltweit eindeutiger Schlüssel für das Archiv und damit auch für die darin enthaltenen Daten (BLOBs). Die World-ID wird von der windream GmbH vergeben und über den Lizenzschlüssel den Endkunden zugeteilt.

Die Pool-ID ist ein eindeutiger Kennzeichner für jeden Objektspeicher-Pool. Die Pool-IDs werden von den Systemadministratoren bei der Einrichtung der Pools festgelegt.

Die Nummerierung der BLOBs in einem Pool bzw. in einem BLOB-Container beginnt mit der Ziffer „1“ und wird für jeden weiteren BLOB immer um eins hochgezählt. So hat beispielsweise der erste BLOB eines Archiv-Pools „PERM1“ mit der World-ID „WMO123“ immer die BLOB-ID „WMO123.PERM1.1“.

## BLOB-ID

Identifikator eines BLOBs im Archiv

Das Kennzeichen:

- identifiziert einen BLOB eindeutig
- wird vom Archiv-Dienst automatisch vergeben

Das Kennzeichen setzt sich zusammen aus:

- World-ID : Identifiziert den Archiv-Dienst
- Pool-ID : Identifiziert den Pool in dem Archiv
- Laufende Nummer : Identifiziert den BLOB in einem Pool

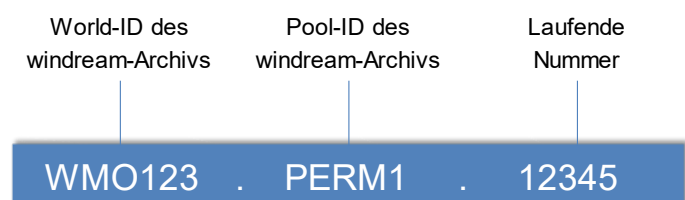


Abbildung 9: BLOB-ID

### 3.4.4 Löschen von Dokumenten aus dem Archiv

Archivierte Dokumente sind generell vor einem (auch unbeabsichtigten) Löschvorgang geschützt. Auf Basis der Einstellungen im windream-Lebenszyklus (vgl. *Abbildung 3: Registerkarte Lebenszyklus zur Einstellung der Lebenszyklus-Daten (am Beispiel eines Dokumenttyps Rechnung)*) sind alle Dokumente während ihres gesamten Archivierungszeitraums unveränderbar abgelegt. Dadurch ist ein Löschen der Dokumente im Archivzeitraum ausgeschlossen. Auch nach Ablauf der Archivierungsperiode lassen sich Objekte nur dann aus dem Archiv entfernen, wenn sie in einem Pool mit hierarchischer Ablage gespeichert sind. Löschvorgänge in BLOB-Containern sind auch auf änderbaren Medien nach Ablauf des Lebenszyklus ausgeschlossen. Falls Daten aus Containern gelöscht werden sollen, erfordert dies eine explizite Reorganisation und Migration des betreffenden Datenbestands. In diesem Fall werden die noch aufbewahrungspflichtigen Blobs in einen neuen Container migriert, und anschließend wird der Container mit den zu löschenden Blobs entfernt. Eine Reorganisation der Daten wird mit den so genannten „windream Enhanced Archive Functions“ („windream EAF“)

vorgenommen. Dabei handelt es sich um eine Software der windream GmbH, mit der sich erweiterte Archivierungsfunktionen ausführen lassen.

### **3.5 Zusätzliche rechtsrelevante Aspekte der windream-Versionen 6.0 und 6.5**

Bei den zusätzlich zu betrachtenden Funktionen, die rechtsrelevant sind, handelt es sich um die Aspekte des Single Instance Storage (SIS), um die Option der veränderbaren Dokument-Attribute nach Archivierung der assoziierten Dokumente und um eine Kennzeichnung als „Revisionssicher“.

#### **3.5.1 Single Instance Storage (SIS) / Dublettenprüfung**

windream unterstützt eine Dublettenprüfung bzw. das so genannte Single Instance Storage (SIS). Dies bedeutet, dass das System bei der Archivierung von Dokumenten optional eine Überprüfung auf doppelt oder mehrfach vorhandene Dokumente durchführt. Diese Prüfung bezieht sich ausschließlich auf den Dokumentinhalt und nicht auf die Metadaten (Attribute, Historie, Rechte, Volltexte, Versionen etc.) der Dokumente. Im Fall eines Duplikats werden die Dokumentinhalte selbst nur einmal statt mehrfach (redundant) im Archiv abgelegt. Dies führt zu einem deutlich reduzierten Speicherplatzbedarf. Das Single Instancing kann für alle Archivbereiche des windream ECM-Systems bzw. der Archiv-Komponente individuell aktiviert werden. Die Dublettenprüfung gilt auch für die Archivierung von E-Mails mit der Mailarchivierungslösung windream Exchange. Technisch wird hier für ein Dokument zuerst ein Hash-Wert gebildet. Ist ein identischer Hash-Wert bereits vorhanden, werden die Dokumente binär verglichen, um mögliche Fehler einer Hash-Prüfung auszuschließen. Der archivierte Dokumentinhalt wird nach festgestellter Gleichheit dann von zwei (oder mehr) Metadatensätzen referenziert. Hierdurch ist sichergestellt, dass jedes Dokument seine individuellen Angaben (Attribute, Rechte,



etc.) behält und auch die Richtlinien des Datenschutzes eingehalten werden.

### **3.5.2 Veränderbare Attribute nach der Archivierung assoziierter Dokumente**

Ab windream 5.0 ist es dem windream-Hauptbenutzer (windream Mainuser), nicht aber den Administratoren gestattet, Attribute (Indizes) eines Dokuments für eine Veränderung nach der Archivierung (Attributeigenschaft „Immer veränderbar“) zuzulassen (durch Änderung der Konfiguration des entsprechenden Dokumenttyps). Diese Option hat jedoch keine Auswirkung auf die betreffenden Dokumente als solche, sondern lediglich auf die Veränderung der eigens dafür gekennzeichneten Attribute (z. B. das Attribut „Bemerkung“), die die Eigenschaften des jeweiligen Dokuments beschreiben. Die Änderung eines für die Veränderung gekennzeichneten Attributs ist dann - in Abhängigkeit von den vergebenen Rechten - Anwendern oder Administrationen gestattet und wird in der Historie des betroffenen Dokuments gespeichert.

Der Sinn dieses Leistungsmerkmals besteht darin, auch nach der Archivierung beispielsweise einer Rechnung noch z. B. das Attribut „Status“ von „offen“ auf „bezahlt“ ändern zu können.

### **3.5.3 Kennzeichnung der Attribute als „revisionssicher“**

Dokument-Attribute (Indizes), die die Eigenschaften (Metadaten) des jeweils assoziierten Dokuments beschreiben, lassen sich durch einen autorisierten Administrator in der windream Administration (windream System Center) bei den Attribut-Eigenschaften der Attribute eines Dokumenttyps auch mit der Option „revisionssicher“ kennzeichnen. Auch diese Eigenschaft kann ausschließlich von dem windream-Hauptbenutzer eingetragen werden. Die Besonderheit hierbei ist, dass dieses Verhalten für ein Attribut nur einmal gesetzt, danach aber nicht mehr zurückgesetzt werden kann. Setzt man also z. B. das Attribut „Rechnungsnummer“ auf „Revisionssicher“, so ist gewährleistet, dass die unter „3.5.2 Veränderbare Attribute nach der Archivierung assoziierter

Dokumente“ sowie „3.5.3 Kennzeichnung der Attribute als „revisionssicher““ beschriebene Funktionalität für dieses Attribut auch durch den windream-Hauptbenutzer nicht mehr verändert werden kann. Das Attribut ist also nach der Archivierung auf jeden Fall nicht mehr veränderbar.

Das Leistungsmerkmal der revisionssicheren Attribute ist für den Erhalt der Integrität nicht notwendig, schafft aber zusätzliche Sicherheit.

### 3.5.4 windream Secure Time-Dienst

Wie unter 3.4.1.1 *Pools und Pooltypen* beschrieben, werden die einzelnen BLOBs durch eine Zeitmarke abgesichert. Diese windream-Zeitmarken werden generell verwendet

- für das Archivierungsdatum (Zeitpunkt der Archivierung) eines Dokuments, das im letzten Data Part des BLOBS eines archivierten Dokuments gespeichert wird,
- bei der Prüfung des Löschedatums am Ende des Archivierungszeitraums (Ablauf der Aufbewahrungsfrist) und
- für die Suche nach zu archivierenden und zu löschenden Dokumenten mittels des automatisierten Prozesses „windream Objekte archivieren und löschen“.

Die von dem windream-Server generierten Zeitmarken können durch den optionalen windream Secure Time-Dienst ergänzt und validiert werden. Der Dienst sichert die Systemzeit des windream-Servers über eine zweite Zeitquelle ab, die nicht von dem windream-Server selber stammt und über einen Webservice eingebunden wird. Auf einem zweiten Server innerhalb oder außerhalb der eigenen Organisation wird eine windream-Komponente betrieben, die eine unabhängige Zeit zur Prüfung der Systemzeit des windream-Servers liefert.

Solange die Differenz der beiden Zeiten kleiner als eine Stunde ist, wird die Zeitmarke des windream-Servers als gültig akzeptiert und

der DMS-Dienst gestartet. Andernfalls wird eine entsprechende Fehlermeldung ausgegeben, und der DMS-Dienst startet nicht. Während des Betriebs wird dieser Zeitabgleich stündlich ausgeführt. Für die Berechnung des Intervalls berechnet der DMS-Server laufend die Differenz zwischen dem aktuellen Tickcount und dem Tickcount beim Start des windream-Servers (beim Tickcount handelt es sich um die verstrichene Zeit in Millisekunden seit dem Systemstart). Sobald diese Differenz größer als eine Stunde ist, wird erneut die Zeit des Referenz-Servers über den Web-Service angefordert (d.h., die Überprüfung der Referenzzeit erfolgt im Stunden-Rhythmus). Kann der windream DMS-Service im Betrieb innerhalb einer Stunde keinen gültigen Zeitvergleich durchführen (wenn z.B. der Web-Service des zweiten Servers nicht erreichbar ist), so werden entsprechende Meldungen ausgegeben und die betreffenden Aktionen (Dokumente archivieren oder aus der Datenbank löschen) werden nicht ausgeführt.

Der Zugriff auf den Web-Service, der die Referenzzeit liefert, erfolgt über SSL mit https-Zertifikat, das über einen der gängigen externen Zertifikatslieferanten (z.B. Symantec) erworben werden kann. Außerdem kann zusätzlich ein Thumbprint des Server-Zertifikats des zweiten Servers auf dem windream-Server geprüft werden (erhöhte Sicherheitsstufe). Dieser Thumbprint des zweiten Servers wird verschlüsselt in der Windows Registry des windream DMS-Servers gespeichert. Nur wenn der Thumbprint bei der Prüfung stimmt, wird die Referenzzeitquelle verwendet. Falls der Thumbprint des zweiten Servers von dem in der Registry gespeicherten Thumbprint abweicht, startet der windream DMS-Service nicht mehr. Der verschlüsselte Thumbprint des zweiten Servers (Referenz-Server) wird von der windream GmbH generiert und bereitgestellt. Die Funktionalität mit der Prüfung einer zweiten Zeitquelle wird über einen entsprechenden Lizenzschlüssel (Security Level) aktiviert.

## 4 Rechtliche Bewertung

Die Verpflichtung zur Aufbewahrung elektronischer Dokumente ergibt sich in erster Linie aus den handelsrechtlichen und steuerrechtlichen Aufbewahrungspflichten für Unternehmen. Das sind insbesondere die Regelungen in den §§ 238 ff HGB und §§ 90 Abs. 3, 141 – 147a AO sowie § 8 GwG. Aber auch aus anderen Steuergesetzen ergeben sich Aufbewahrungspflichten (z.B. aus § 22 UStG, § 4 Abs. 3 Satz 5, § 4 Absatz 4a Satz 6, § 4 Absatz 7 und § 41 EStG). Für einzelne Rechtsformen folgt die Aufbewahrungspflicht aus gesondert statuierten Aufzeichnungspflichten (z.B. §§ 91 ff AktG, §§ 41 ff GmbHG, § 33 GenossenschaftsG). Darüber hinaus erfordern zahlreiche branchenspezifische Aufzeichnungspflichten (z.B. §§ 25a ff KWG, § 23 VAG) eine elektronische Aufbewahrung. Unbeschadet der gesetzlichen Aufbewahrungs- und Aufzeichnungspflichten ist es zur Sicherung der Beweisqualität sinnvoll, auch solche Dokumente analog den gesetzlichen Anforderungen aufzubewahren, die das Unternehmen an sich nicht aufbewahren müsste.

Es ist daher zu prüfen, ob die zu begutachtende Software den gesetzlichen Ansprüchen genügt.

### 4.1 Vertragsabschluss durch E-Mail-Kommunikation

Die Rechtswirksamkeit der elektronischen Kommunikation ergibt sich aus dem traditionellen Grundsatz der Formfreiheit. Ist ausnahmsweise für eine rechtswirksame Erklärung Schriftform erforderlich, so kann diese durch die Sicherheitstechnik der elektronischen Signaturen ersetzt werden: Die vereinbarte Schriftform durch die einfache elektronische Signatur oder die fortgeschrittene elektronische Signatur oder die gesetzliche Schriftform durch die qualifizierte elektronische Signatur.<sup>5</sup>

---

<sup>5</sup> Zur zivilrechtlichen Wirksamkeit elektronischer Erklärungen siehe die aktuelle Zusammenfassung von *Kitz*, in *Hoeren/Sieber* (Hrsg.), Handbuch MultiMediarecht Teil 13.1 – Stand: Februar 2020.

Durch die „VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt“ und das daraufhin erlassene Vertrauensdienstegesetz (VDG) wurde das Signaturgesetz und die Signaturverordnung abgelöst.<sup>6</sup> Ziel war und ist es, digitale Transaktionen innerhalb des EU-Binnenmarktes effektiver durchführen zu können. Zwar wird nach wie vor die im BGB verankerte Differenzierung hinsichtlich der Formvorschriften übernommen, wonach nur die qualifizierte elektronische Signatur die handschriftliche Unterschrift ersetzen soll. Und so findet sich auch in § 3 Nr. 12 der EU-Verordnung eine Definition der qualifizierten elektronischen Signatur (qeS). Die Vorgaben sehen aber auch wesentliche Vereinfachungen und Verbesserungen vor, zu denen unter anderem die Einführung sogenannter elektronischer Siegel (Organisationszertifikate), mit denen nun auch Unternehmen und Behörden sowie andere Organisationen ihre elektronischen Korrespondenz mit einer qeS versehen können gehört, wie auch die Möglichkeit sogenannte Fernsignaturen zu verwenden, bei denen die Nutzung einer qeS auch ohne spezielle SmartCards und Lesegeräte möglich ist und so die Nutzung per Tablet oder Smartphone ermöglicht werden.

## 4.2 Aufbewahrung elektronischer Dokumente

Aufbewahrungspflichtig sind nach § 257 Abs. 1 Nr. 1-4 HGB und § 147 Abs. 1 Nr. 1-5 AO neben den außersteuerlichen und steuerlichen Büchern, Aufzeichnungen und Unterlagen zu Geschäftsvorfällen auch alle anderen Unterlagen, die zum Verständnis und zur Überprüfung der für die Besteuerung gesetzlich vorgeschriebenen Aufzeichnungen im Einzelfall von Bedeutung sind.<sup>7</sup> Dazu zählen neben Unterlagen in Papierform auch alle Unterlagen in Form von Daten, Datensätzen und elektronischen

---

<sup>6</sup> Zum Zeitpunkt der Begutachtung ist die überarbeitete Fassung der Verordnung, auch bekannt als eIDAS 2.0, noch nicht in Kraft. Die neue Fassung integriert neben elektronischen Signaturen, Zeitstempeln und Siegel auch weitere Arten von Vertrauensdiensten, wie z.B. elektronische Einschreiben und elektronische Zertifikate zur Authentifizierung.

<sup>7</sup> vgl. BFH-Urteil vom 24. Juni 2009, BStBl II 2010 S. 452

Dokumenten, die dokumentieren, dass die Ordnungsvorschriften umgesetzt und deren Einhaltung überwacht wurde.<sup>8</sup>

Die GoBD konkretisieren die bis 31.12.2014 gültigen „Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)“ und „Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS)“ und ersetzen diese<sup>9</sup>. Die ordnungsmäßige Archivierung hat schon lange durch Basel II und den US - Sarbanes Oxley Act eine internationale Dimension erreicht.

#### **4.2.1 Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff**

Für die im Sinne der GoBD<sup>10</sup> „ordnungsmäßige Aufbewahrung“ kommt es im Rahmen der elektronischen Verarbeitung, und nur diese wird hier betrachtet, auf diejenigen Elemente der Software an, die sich mit der Erfassung, Indexierung, Speicherung, Verwaltung, Lesbarmachung und langfristigen und unveränderlichen Aufbewahrung von elektronisch zu speichernden Daten und Dokumenten beschäftigen. Zu betrachten sind daher das Speichersystem, welches die Speichermedien verwaltet, sowie die Funktionsweise der Programmelemente, die sich mit der Indexierung und Archivierung selbst beschäftigen.

##### **- Ordnungsmäßige Speichersysteme**

Die Aufbewahrung von Unterlagen ist materiell ordnungsmäßig, wenn die Geschäftsvorfälle einzeln, nachvollziehbar, vollständig, richtig, zeitgerecht und geordnet in ihren Auswirkungen erfasst, gebucht und verarbeitet sind. Die Ordnungsmäßigkeit ist nicht von

---

<sup>8</sup> Schreiben des Bundesministeriums der Finanzen vom 14.11.2014, Tz 5, besser bekannt als „Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)“

<sup>9</sup> siehe hierzu GoBD. Tz. 183

<sup>10</sup> BMF v. 28.11.2019 - IV A 4 - D 0316/19/10003 :001, abgerufen zuletzt am 15.05.2020 unter

[https://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF\\_Schreiben/Weitere\\_Steuerthemen/Abgabenordnung/2019-11-28-GoBD.html](https://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Weitere_Steuerthemen/Abgabenordnung/2019-11-28-GoBD.html)

einem bestimmten Speichermedium abhängig. Es spielt auch keine Rolle, ob die Systeme vom Aufbewahrungspflichtigen als eigene Hardware bzw. Software erworben und genutzt oder in einer Cloud oder einer Kombination dieser Systeme betrieben werden. Zulässig und damit ordnungsmäßig im Sinne der handelsrechtlichen und steuerrechtlichen Aufbewahrungsvorschriften sind vielmehr grundsätzlich alle Systeme und Speichermedien. Entscheidend für die Ordnungsmäßigkeit sind die hardwaremäßigen, softwaremäßigen und organisatorischen Sicherheitsfunktionen, die für das jeweilige Speichermedium gesondert ausgeprägt sein können. Die Aufbewahrungsfrist beträgt für empfangene und die Kopien abgesandter Handelsbriefe 6 Jahre und für Handelsbelege 10 Jahre (§ 257 Abs. 4 HGB). Die Aufbewahrungsfrist für Dokumente, deren Inhalt deliktsrechtlichen Verjährung unterliegen, müssen unter Umständen über einen Zeitraum von mindestens 30 Jahren archiviert werden. Zu beachten ist, dass sich die Aufbewahrungsfristen auch nach dem Verschieben der Daten und Dokumente verändern können, etwa durch Fristhemmung oder -unterbrechung (z.B. § 147 Absatz 3 Satz 5 AO). Während dieses Zeitraums muss der Zugriff auf das Dokument jederzeit möglich sein.

#### - **Ordnungsmäßige Wiedergabe durch Indizierung**

Die Wiedergabe von aufbewahrungspflichtigen Informationen ist gemäß § 257 Abs. 3 HGB ordnungsmäßig, wenn der Zugriff innerhalb einer angemessenen Frist möglich ist und nach § 147 Abs. 2 AO, wenn der Zugriff „unverzüglich“ möglich ist. In der zivilrechtlichen Definition heißt „unverzüglich“ ohne schuldhaftes Zögern (§ 121 Abs. 1 Satz 1 BGB). Die Frist zur Lesbarmachung ist im Einzelfall nach Verhältnismäßigkeitsgesichtspunkten zu entscheiden. Dabei spielt es unter anderem eine Rolle, welche Datenmengen lesbar gemacht werden sollen, welches Speichermedium genutzt wurde und welche Streuung die relevanten Daten im Archivsystem haben.

Elektronische Dokumente sind jeweils mit einem nachvollziehbaren und eindeutigen Index zu versehen. Der Erhalt der Verknüpfung

zwischen Index und elektronischem Dokument muss während der gesamten Aufbewahrungsfrist gewährleistet sein. Es ist sicherzustellen, dass das elektronische Dokument unter dem zugeteilten Index verwaltet werden kann. Dabei darf das Anbringen der Indexierung keinen Einfluss auf die Lesbarmachung des Originalzustands haben. Die elektronischen Bearbeitungsvorgänge sind zu protokollieren und mit dem elektronischen Dokument zu speichern, damit die Nachvollziehbarkeit und Prüfbarkeit des Originalzustands und seine Ergänzungen gewährleistet sind.<sup>11</sup>

#### - **Ordnungsmäßige Verfahrensdokumentation**

Die Anforderungen an die Verfahrensdokumentation sind vom Bundesfinanzministerium in den GoBD definiert worden. Nach Textziffer 151 müssen der Inhalt, Aufbau, Ablauf und Ergebnisse des DV-Verfahrens vollständig und schlüssig ersichtlich sein.

#### - **Datenzugriff**

Das Bundesfinanzministerium hat mit den GoBD das Recht zum Zugriff auf originär digitale Unterlagen im Rahmen der Außenprüfung in Form des unmittelbaren Datenzugriffs, des mittelbaren Datenzugriffs und der Datenträgerüberlassung konkretisiert. Nach Textziffer 131 müssen eingehende elektronische Handels- oder Geschäftsbriefe und Buchungsbelege in dem Format aufbewahrt werden, in dem sie empfangen wurden. Für den unmittelbaren Datenzugriff der Finanzbehörde muss der Steuerpflichtige nach Abschnitt 11.2 GoBD dem Prüfer die erforderlichen Hilfsmittel zur Verfügung stellen, damit er selbstständig auf die Daten zugreifen kann. Für den mittelbaren Datenzugriff hat der Steuerpflichtige entsprechend den Angaben des Prüfers den Zugriff auf die Daten zu organisieren. Statt des unmittelbaren und mittelbaren Datenzugriffs kann die Finanzbehörde einen Datenträger verlangen, auf dessen Daten sie zugreifen kann.

---

<sup>11</sup> GoBD Textziffer 122, 123



### - **Maschinelle Auswertbarkeit**

Um den Datenzugriff zu ermöglichen, muss nach § 147 Abs. 2 Nr. 2 AO sichergestellt sein, dass die Daten während der Dauer der Aufbewahrungsfrist jederzeit verfügbar sind, unverzüglich lesbar gemacht und maschinell ausgewertet werden können. Damit sind originär digitale Unterlagen auf maschinell verwertbaren Datenträgern während der gesamten Aufbewahrungsfrist zu archivieren. Nach Abschnitt 9.1 GoBD ist die maschinelle Auswertbarkeit u.a. dann gegeben, wenn mathematisch-technische Auswertungen, eine Volltextsuche oder sonst eine Prüfung im weitesten Sinne möglich ist (z.B. Bildschirmabfragen, die Nachverfolgung von Verknüpfungen, oder die Textsuche nach bestimmten Eingabekriterien). Die Reduzierung einer bereits bestehenden maschinellen Auswertbarkeit der vorhandenen Aufzeichnungen und Belege ist nach Textziffer 129 ausdrücklich nicht zugelassen.

### **4.2.2 Basel II, Sarbanes Oxley Act und Dokumentationspflicht**

Basel II und Sarbanes Oxley Act (SOA) wirken sich indirekt auf die Dokumentationspflicht aus: Die Anforderungen von Basel II und SOA können nur durch möglichst lückenlose Dokumentation rechtlich bedeutsamer elektronischer Dokumente erfüllt werden.

### - **Basel II**

Zweck der „Internationalen Konvergenz der Kapitalmessung und Kapitalanforderung (Basel II)“ ist die wirtschaftliche Sicherheit von Kreditinstituten. Der kritische Punkt sind die „operationellen Risiken“: die Gefahr von Verlusten, die durch das Versagen interner Systeme oder durch externe Ereignisse eintreten. Als operationelle Risiken gelten Rechtsrisiken, da sie zu Bußgeldern, Geldstrafen und Strafzahlungen führen können. Die Abwehrstrategie gegen solche Risiken ist die elektronische Dokumentation, um die Erfüllung der Pflichten in einem Streitfall beweisen zu können. Dies ist ein allgemeingültiger Grundsatz unternehmerischen Handelns und nicht auf Kreditinstitute beschränkt. Deshalb strahlt „Basel II“ mit der

Konsequenz der Dokumentationspflicht auch auf andere Unternehmen als Kreditinstitute aus.<sup>12</sup>

#### - **Sarbanes Oxley Act**

Unübersehbar gewinnt das Recht der USA über den Weg des Internets eine bestimmende Funktion. Ein Beispiel für diese Entwicklung ist der Sarbanes Oxley Act. Das zentrale Anliegen des „Sarbanes Oxley Act“ ist die „compliance“ des Finanz- und Rechnungswesens, um Investoren zu schützen. Nach der zentralen Vorschrift des Sec. 404 haben Unternehmen jährlich ihr internes Kontrollsystem prüfen zu lassen und über das Ergebnis in ihrem Abschluss zu berichten. Von den Regelungen des Sarbanes Oxley Act sind in Deutschland Unternehmen betroffen, die auf Grund der Inanspruchnahme des US-amerikanischen Kapitalmarktes an US-amerikanischen Börsen registriert sind und Unternehmen, die in Geschäftsbeziehungen mit US-Unternehmen stehen. Nach der US-amerikanischen Rechtsprechung reichen „Certain minimum contacts“ zwischen einem amerikanischen und ausländischen Unternehmen aus, die Zuständigkeit der US-Gerichte zu begründen. Entsprechend haben die US-Bundesstaaten „Long-Arm-Statutes“ erlassen, nach denen die Zuständigkeit amerikanischer Gerichte trotz Abwesenheit des ausländischen Beklagten angenommen wird. Damit ist für Unternehmen mit Sitz in Deutschland, die in Handelsbeziehungen mit US-Unternehmen stehen, das Risiko hoch, wegen Verletzung der Anforderungen des Sarbanes Oxley Act in den USA erfolgreich verklagt zu werden. Dies zwingt dazu, rechtserhebliche Dokumente nach den Grundsätzen der Ordnungsmäßigkeit vollständig elektronisch zu archivieren.

---

<sup>12</sup> Die Basel II-Regelungen wurden angesichts der Finanzkrise 2007/2008 durch Basel III ergänzt und überarbeitet. Die hier relevante Abwehrstrategie durch elektronische Dokumentation hat sich indes nicht geändert.

### 4.2.3 Zwischenergebnis

Hieraus ergeben sich als rechtliche Anforderung an die ordnungsmäßige Aufbewahrung folgende Prüfkriterien:

- ordnungsgemäße Speicherung der Dokumente im Archivsystem,
- jederzeitige Verfügbarkeit der Dokumente,
- die Integrität der Dokumente,
- Einsatz ordnungsmäßiger Speichersysteme und
- Vorhandensein einer ordnungsmäßigen Verfahrensdokumentation.

## 4.3 Ordnungsmäßigkeit des windream Archivs

Auf der Basis der so gewonnenen Prüfkriterien wird nachfolgend aus rechtlicher Sicht die Ordnungsgemäßheit der Software geprüft. Herzstück der Archivsoftware ist das „BLOB- (Binary Large Object) und Poolkonzept“. Es stellt gleichermaßen die Sicherheitsarchitektur des windream Archivsystems dar.<sup>13</sup>

### 4.3.1 Speichern der Dokumente im Archivsystem

Eine Archivierungssoftware muss sicherstellen, dass alle Dokumente und Daten im Archiv des Systems gespeichert werden. Dies ist durch einen Abgleich der Protokolle der Erfassungssoftware und der Protokolle des Speichersystems zu kontrollieren. Weiterhin stellt windream die Speicherung durch Transaktionen und Prüfsummen sicher.<sup>14</sup>

Darüber hinaus ist sicherzustellen, dass während des definierten Aufbewahrungszeitraums ein unberechtigtes oder versehentliches Löschen der Dokumente ausgeschlossen ist.

Die bearbeiteten Dokumente werden in dem Archivsystem integer gespeichert. Ist der definierte Bearbeitungszeitraum abgelaufen,

---

<sup>13</sup> Ziffer 3.4 des Sachverhalts.

<sup>14</sup> Ziffer 3.4.3.1 des Sachverhalts

werden die Dokumente in das Archivsystem verschoben. In dem Archivsystem können die Dokumente nicht mehr bearbeitet und damit im Rechtssinne nicht mehr verändert werden. Hierfür bietet windream mehrere Schutzmöglichkeiten. Durch die Option „Nach Typzuordnung sofort archivieren“ werden die Dokumente in den angegebenen Archivspeicher direkt übertragen. Durch die Option „Datei nicht bearbeitbar“ wird die Bearbeitung des Dokuments auch bei anderslautenden Rechten und auch während der Bearbeitungszeit verhindert. Auch können während der Bearbeitungszeit die Rechte, das Dokument zu bearbeiten, auf Administratoren oder sogar auf den Hauptbenutzer eingeschränkt werden.<sup>15</sup> Das Bearbeiten und Löschen der Dokumente ist während des Archivierungszeitraums ausgeschlossen.<sup>16</sup>

windream ermöglicht daher systemseitig eine ordnungsgemäße Speicherung der Dokumente. Im Ergebnis ergibt der Ausschluss der Bearbeitung und der Ausschluss des Löschens archivierter Dokumente einen hohen Integritätswert.

### **4.3.2 Ordnungsgemäße Indexierung**

Weitere Voraussetzung für eine ordnungsgemäße Aufbewahrung ist, dass die Anforderungen an eine geordnete Ablage erfüllt sein müssen, um eine Wiederauffindbarkeit der Daten zu gewährleisten. Es ist sicherzustellen, dass jedem archivierten Dokument oder Datensatz eine eindeutige ID zugewiesen wird. Programmseitig ist die eindeutige Verknüpfung und deren Nachweisbarkeit zu gewährleisten.

windream setzt insoweit auf das BLOB-Prinzip. Mit BLOB (Binary Large Object) wird die Struktur bezeichnet, in der die zu archivierenden Dokumente abgelegt werden: Header, Data Parts und Trailer. Ein BLOB enthält drei Data Parts. Der erste Data Part enthält das Dokument, der zweite Data Part enthält die Dokumenteneigenschaften (falls gewünscht und konfiguriert) und der dritte Data Part die Inhaltsübersicht. Jeder Data Part wird über

---

<sup>15</sup> Ziffer 3 des Sachverhalts.

<sup>16</sup> Ziffer 3.4.4 des Sachverhalts.

eine Referenznummer identifiziert.<sup>17</sup> Die BLOBs werden mit einer BLOB-ID in Pools gespeichert. Ein Pool ist eine Speichereinheit zur Ablage von logisch ähnlichen BLOBs. Damit kann einem windream-Dokumenttyp ein bestimmter Pool zugewiesen werden. Die BLOB-ID ist ein weltweit eindeutiger Kennzeichner eines BLOBs. Sie setzt sich zusammen aus der World-ID, der Pool-ID und einer laufenden Nummer. Die World-ID ist ein weltweit eindeutiger Schlüssel für das Archiv und damit auch für die darin enthaltenen BLOBs. Sie wird von der windream GmbH vergeben und aus dem Lizenzschlüssel ermittelt. Die Pool-ID ist ein Kennzeichen für einen Objektspeicher-Pool und wird von den Systemadministratoren vergeben.<sup>18</sup> Jeder BLOB-Container besitzt eine Volume-ID, über die er vom System identifiziert wird.<sup>19</sup>

Durch dieses System ermöglicht windream eine eindeutige Referenzierung der archivierten Dokumente. Diese eindeutige Referenzierung bleibt auch durch das in windream-Version 5 neu implementierte Leistungsmerkmal des Single Instance Storage (SIS)<sup>20</sup> erhalten.

In der windream-Version 5 können Attribute eines Dokuments als änderbar gekennzeichnet werden.<sup>21</sup> Generell ausgeschlossen ist hier die Referenzierung des BLOBs. Weiterhin kann ein Attribut nur durch den windream-Hauptbenutzer als änderbar gekennzeichnet werden. Auch durch dieses neue Leistungsmerkmal bleibt somit die Integrität des windream ECM-Systems erhalten.

Das Leistungsmerkmal der „revisionssicheren Attribute“<sup>22</sup> ist somit für den Erhalt der Integrität nicht notwendig, schafft aber zusätzliche Sicherheit.

---

<sup>17</sup> Ziffer 3.4.3 des Sachverhalts.

<sup>18</sup> Ziffer 3.4.2 des Sachverhalts.

<sup>19</sup> Ziffer 3.4.2 des Sachverhalts.

<sup>20</sup> Ziffer 3.5.1 des Sachverhalts.

<sup>21</sup> Ziffer 3.5.2 des Sachverhalts.

<sup>22</sup> Ziffer 3.5.3 des Sachverhalts.

### 4.3.3 Integrität der Dokumente durch das Checksummensystem

Die im Archiv aufbewahrten Systeme sind vor jeglicher Veränderung, die zu einer Verfälschung führen, zu schützen.

Datenmanipulationen werden durch ein Checksummensystem festgestellt. Für jeden Data Part wird eine Checksumme generiert. Bei der Anforderung von Dokumenten prüft das System die Checksummen der assoziierten Objekte. Falls das System bei der Prüfung Fehler im Sinne einer Dokumenten-Manipulation feststellt, wird eine entsprechende Meldung automatisch an den Endbenutzer geschickt, und autorisierte Administratoren werden per E-Mail benachrichtigt.<sup>23</sup>

Die Vollständigkeit der archivierten Dokumente kann über die Ablage der Archivobjekte (BLOBs) in Containern sowie die SHA-Prüfsummen nachgewiesen werden.

Das System erfüllt insoweit die gesetzlichen Anforderungen.

### 4.3.4 Ordnungsmäßige Speicherung

Durch die Einstellung im Lebenszyklus können alle Dokumente während ihres gesamten Archivierungszeitraums nicht gelöscht werden.<sup>24</sup> Nach Ablauf der Archivierungsperiode lassen sich Objekte nur dann aus dem Archiv entfernen, wenn sie in einem Pool mit hierarchischer Ablage gespeichert sind. Löschvorgänge sind auch auf änderbaren Medien in BLOB-Containern nach Ablauf des Lebenszyklus ausgeschlossen.<sup>25</sup> Bei einem Verlust der Datenbankdaten lassen sich die durch windream archivierten Objekte aus den Archivobjekten wieder rekonstruieren (Metadaten im XML-Format), da sie selbstbeschreibend („self contained objects“) sind.<sup>26</sup>

---

<sup>23</sup> Ziffer 3.4.3.1 des Sachverhalts.

<sup>24</sup> Ziffer 3 (Abbildung 3) des Sachverhalts.

<sup>25</sup> Ziffer 3.4.4 des Sachverhalts.

<sup>26</sup> Ziffer 3 (Abbildung 3) des Sachverhalts.

Für die verschiedenen Speichermedien, die das windream Archivsystem unterstützt, werden Pools unterschiedlicher Prototypen verwendet. Das windream Archivsystem speichert BLOBs anhand ihrer BLOB-IDs mit Hilfe von Mediensequenzen auf bestimmten Medien eines Pools. Damit Medien vom Archiv verwendet werden können, generiert das System bei der Initialisierung der Medien auch den Bezeichner des Mediums. Über diese Medienbezeichnung erfolgt die Zuordnung zu einer Mediensequenz. So legen Mediensequenzen fest, welche BLOBs auf welche Pools geschrieben werden.<sup>27</sup>

### 4.3.5 Lesbarmachung

Das ECM-System windream verfügt über mehrere Optionen, die sicherstellen, dass die Dokumente während der gesamten Aufbewahrungsfrist jederzeit lesbar sind. Zunächst ist zu beachten, dass windream alle Dokumente im Originalformat der assoziierten Anwendungen speichert und nicht, wie früher bei anderen Systemen durchaus üblich, in einem proprietären Dateiformat. Dadurch ist sichergestellt, dass die Dokumente zu jedem Zeitpunkt auch immer mit der jeweiligen Originalanwendung geöffnet werden können und somit lesbar sind.

windream stellt zudem eine Software-Komponente namens windream DocView zur Verfügung, die es erlaubt, Dokumente auch ohne verknüpfte Originalanwendung zu öffnen. Es handelt sich dabei um einen „Viewer“, der Dokumente der unterschiedlichsten Formate darstellen kann. Insgesamt stellt der Viewer mehrere Hundert Dokumentformate dar, zu denen selbstverständlich auch die gängigen Langzeitformate PDF und PDF/A gehören.

Weiterhin wird zu jedem in windream abgelegten Dokument automatisch der Volltext extrahiert und zusätzlich zum Dokument archiviert. Der extrahierte Volltext repräsentiert die textuellen Informationen des Original-Dokuments.<sup>28</sup>

---

<sup>27</sup> Ziffer 3.4.1.1 des Sachverhalts.

<sup>28</sup> Ziffer 3 des Sachverhalts.

Optional kann auch die Konvertierungssoftware „windream Rendition Service“ zum Einsatz kommen. Dieses serverbasierte Dienstprogramm wandelt in windream gespeicherte Dokumente automatisiert in das PDF- oder PDF/A-Format um und archiviert die auf diese Art transformierten Dokumente zusätzlich zu den Originaldokumenten ebenfalls in windream.

#### **4.3.6 Ordnungsmäßige Verfahrensdokumentation**

Die Verfahrensdokumentation ist transparent aufgebaut, vermittelt die Komplexität des Systems in einer lesbaren und verständlichen Form.

#### **4.3.7 Ergebnis für windream**

Das windream Archivsystem erfüllt damit die rechtlichen Anforderungen an die ordnungsmäßige Archivierung.

### **4.4 Die Beweisqualität elektronischer Dokumente**

Die Beweisqualität elektronischer Dokumente wird, wie bei allen Beweismitteln, vom Grundsatz der freien Beweiswürdigung bestimmt.

#### **4.4.1 Freie Beweiswürdigung**

Ein elektronisches Dokument ist nicht Urkunde, da es in materialisierter Form von dem Aussteller nicht unterzeichnet ist.<sup>29</sup> Damit unterliegt das elektronische Dokument, dessen Beweis gemäß § 371 Abs. 1, S. 2 ZPO durch Vorlegung oder Übermittlung einer Datei angetreten wird, als Objekt des Augenscheins der freien Beweiswürdigung des Gerichts. Die freie Beweiswürdigung wird bestimmt durch Hinweise auf die Vertraulichkeit, die Integrität und Authentizität des Dokuments.

---

<sup>29</sup> Allgemeine Meinung: *Ortner* in *Hoeren/Sieber*, Handbuch Multimediarecht, Teil 13.2 Rd. 19 *m.w.Nw* – Stand: Oktober 2020



#### **4.4.2 Beweisqualität der ordnungsmäßigen Archivierung**

Für die Beweisqualität elektronisch archivierter Dokumente spricht die Aufbewahrung nach den Grundsätzen der Ordnungsmäßigkeit. Mit der Aufbewahrung entsprechend diesen Grundsätzen werden, wie dargestellt, elektronische Dokumente gegen unberechtigte oder versehentliche Änderungen geschützt. Dem ordnungsgemäß aufbewahrten Dokument bleibt folglich seine originäre Beweiskraft erhalten.

#### **4.4.3 Die Beweisfunktion des windream Archivsystems**

Wie unter Ziffer 4.3 festgestellt, entspricht das windream Archivsystem den Anforderungen an die ordnungsmäßige Aufbewahrung. Ordnungsmäßige Aufbewahrung ist das entscheidende Indiz für die Beweisqualität elektronisch archivierter Dokumente. Damit bleibt den im windream Archivsystem aufbewahrten Dokumenten ihre originäre Beweiskraft vollumfänglich erhalten.

### **4.5 Die Rechtslage in der Republik Österreich**

#### **4.5.1 Republik Österreich**

Die elektronische Archivierung ist nach dem Recht der Republik Österreich zulässig. Nach § 131 Abs. 3 der Bundesabgabenverordnung (BAO) können zur Führung von Büchern und Aufzeichnungen Datenträger verwendet werden. Erforderlich ist nach dieser Vorschrift, dass die inhaltsgleiche, vollständige und geordnete Wiedergabe bis zum Ablauf der gesetzlichen Aufbewahrungsfrist jederzeit gewährleistet ist und die vollständige und richtige Erfassung aller Geschäftsvorfälle durch entsprechende Einrichtungen gesichert ist.

Diese gesetzliche Anforderung ist durch das Fachgutachten „Ordnungsmäßigkeit von IT-Buchführungen“ vom 23. März 2011 des „Fachsenats für Datenverarbeitung der Kammer der Wirtschaftstreuhänder“ näher bestimmt worden. Nach Absatz 1 der

Vorbemerkung sind auch computergestützte Systeme zugelassen, wenn diese die Anforderungen, die durch die Grundsätze ordnungsmäßiger Buchführung an sie gestellt werden, erfüllen. Das entspricht auch der Regelung in § 190 Absatz 5 UGB.

Für die elektronische Archivierung verlangt der Fachsenat

- eine geordnete Aufbewahrung während der Aufbewahrungsfristen,
- die Lesbarmachung der aufbewahrten Unterlagen,
- eine Verfahrensdokumentation für die Nachvollziehbarkeit der Buchführung und
- die Einhaltung der für Kriterien analog zur ordnungsgemäßen Buchführung.
  - Nachverfolgbarkeit der Verfahrensschritte,
  - vollständige Aufzeichnung der Vorgänge in zeitlicher Reihenfolge,
  - sachliche Ordnung und
  - Verfahrensdokumentation in übersichtlicher Form.

Im Wesentlichen entsprechen die Anforderungen, die der Fachsenat formuliert, den Ausführungen in den GoBD. Auch hier ist die Verpflichtung verankert, dass Geschäftsvorfälle sich in ihrer Entstehung verfolgen lassen. Damit ist die Verfügbarkeit der Dokumente angesprochen, die auch nach deutschem Archivierungsrecht besteht. Nach Randziffer 20 darf eine Buchung nicht in einer Art verändert werden, dass der ursprüngliche Inhalt nicht mehr feststellbar ist. Damit ist die auch nach deutschem Recht gleichermaßen bestehende Anforderung der Integrität formuliert. Die Beweisqualität elektronisch archivierter Dokumente ist nicht gesetzlich geregelt. Wie im deutschen Zivilprozessrecht gelten elektronisch archivierte Dokumente nicht als private Urkunden nach § 294 der österreichischen ZPO, da sie nicht von dem Aussteller unterschrieben sind. Dies ist nur in materialisierter Form möglich. Sie unterliegen damit der freien Beweiswürdigung gemäß § 272

Abs. 1 der österreichischen ZPO. Diese freie Beweiswürdigung wird wie in dem deutschen Recht nach den Grundsätzen der ordnungsmäßigen Archivierung bestimmt.

#### **4.5.2 Zwischenergebnis**

Im Ergebnis gelten damit im deutschen und österreichischen Zivilprozessrecht dieselben Anforderungen für die Beweisqualität elektronischer Dokumente: Die Dokumente müssen integer und lesbar archiviert sein. Anders als in Deutschland besteht für Österreich nicht eine dem § 146 AO und der GoBD entsprechende Regelung, wonach originäre elektronische Dokumente maschinell auswertbar zu archivieren sind.

### **4.6 Rechtssicherheit des integrierten Enterprise-Content-Management-Systems windream nach den rechtlichen Kriterien der Republik Österreich**

Wie gezeigt ist das integrierte Archiv des Enterprise-Content-Managementsystem windream geeignet, die gesetzlichen Anforderungen an eine ordnungsgemäße Aufbewahrung nach den Kriterien der deutschen Rechtsvorschriften (HGB, BGB, AO, VDG, GoBD) in vollem Umfang zu erfüllen.

Im Folgenden ist also die Fragestellung zu klären, ob die dargestellten Bestimmungen der Republik Österreich mit den Bestimmungen der Bundesrepublik Deutschland vergleichbar sind oder sogar inhaltlich übereinstimmen.

#### **4.6.1 Das Recht der elektronischen Archivierung der Republik Österreich im Vergleich mit dem Recht der Bundesrepublik Deutschland**

Sowohl im deutschen wie auch im österreichischen Recht wird von Unternehmen eine „ordnungsgemäße Buchführung“ verlangt. Dieses zunächst zivilrechtliche Erfordernis macht sich sodann der Fiskus zu eigen und setzt bezüglich der Besteuerung auf dieser Buchführung auf und konkretisiert sie näher. Die enge Verzahnung zwischen diesen beiden Systemen (HGB + AO in Deutschland und

UGB + BAO) kommt nicht von ungefähr. 1862 wurde das im Deutschen Bund geltende „Allgemeine Deutsche Handelsgesetzbuch“ als „Allgemeines Handelsgesetzbuch“ im Kaisertum Österreich eingeführt. Die Kernbestimmungen sind noch heute vergleichbar. Hierzu zählen auch die Buchführungspflichten. Auch in Österreich wurden die konkreten Anforderungen an eine elektronische Buchführung nicht im Gesetz geregelt, sondern an den „Fachsenat für Datenverarbeitung der Kammer der Wirtschaftstreuhänder“ ausgelagert. Im Ergebnis verwundert es auch nicht, dass die vom Fachsenat formulierten Anforderungen an ein ordnungsgemäßes IT-System den Anforderungen der GoBD entsprechen.

Ein Vergleich dieser Anforderungen zeigt, dass die österreichischen Anforderungen vollständig in den Anforderungen der GoBD aufgehen.

#### **4.6.2 Fazit**

Da die Anforderungen des Fachsenats für Datenverarbeitung der Kammer der Wirtschaftstreuhänder nicht über die Anforderungen der GoBD hinausgehen, können die rechtlichen Ausführungen für die GoBD ohne weiteres auf das österreichische Recht übertragen werden.

Das windream Archivsystem ist somit geeignet, die in der Republik Österreich geltenden rechtlichen Bestimmungen zur ordnungsgemäßen elektronischen Aufbewahrung in vollem Umfang zu erfüllen.

## 5 Ergebnis der rechtlichen Begutachtungen Deutschland, Österreich

### 5.1 Ergebnis der Prüfung durch Dr. Ivo Geis

Das windream Archivsystem ermöglicht es,

- rechtswirksame elektronische Erklärungen und Dokumente (4.1)
- nach den handelsrechtlichen und steuerrechtlichen Grundsätzen (4.2)
- ordnungsmäßig zu archivieren (4.3) und
- damit deren Beweisqualität zu sichern (4.4).

Die ordnungsmäßige Archivierung (4.3) kann mit windream in beliebiger Konfiguration auf optischen Medien durchgeführt werden. Bei der Verwendung der Konfiguration „Ablage der Archivobjekte in Containern“ (3.4.2) können auch änderbare Medien (z. B. Festplatten, RAID, NAS, SAN) als Ablage (4.3.3) für die ordnungsgemäße Archivierung verwendet werden. Die neuen Leistungsmerkmale (3.5) wurden optimal und unter Beibehaltung der Rechtssicherheit in das Gesamtsystem integriert.

**Damit erfüllt das windream Archivsystem die rechtlichen Anforderungen der deutschen und österreichischen Gesetzgebung optimal und auf höchstem Niveau.**

Hamburg, den 20.05.2011



Rechtsanwalt Dr. Ivo Geis

## 5.2 Ergebnis der Prüfung durch Prof. Dr. Wolfgang Hackenberg

Seit der Begutachtung des windream Archivsystems im Jahre 2011 durch Herrn Dr. Ivo Geis wurden gesetzliche Bestimmungen geändert. Diesen Änderungen wurde in dieser Version des Rechtsgutachtens Rechnung getragen. Die Anforderungen an die Rechtssicherheit eines Archivsystems haben sich indes nicht verändert. Da sich auch die grundlegenden Verfahrenskonzepte und -abläufe der windream Software nicht geändert haben, ermöglicht das windream Archivsystem bei sachgerechter Anwendung nach wie vor vollumfänglich die Einhaltung der gesetzlichen Anforderungen an eine ordnungsgemäße Aufbewahrung von Dokumenten der Republik Österreich und der Bundesrepublik Deutschland.

Eningen unter Achalm, 01.06.2023



Prof. Dr. Wolfgang Hackenberg

## 6 Literaturverzeichnis und Abkürzungen

### 6.1 Literatur

*Ortner* in *Hoeren/Sieber*, Handbuch Multimediarecht, Teil 13.2 –  
Stand: Juli 2017.

*Oertel*, Elektronische Form und notarielle Aufgaben im  
elektronischen Rechtsverkehr, MMR 2001, 419.

*Kitz*, in *Hoeren/Sieber* (Hrsg.), Handbuch MultiMediarecht Teil 13.1  
– Stand: Juli 2017.

### 6.2 Abkürzungen

|        |  |
|--------|--|
| AO     | Abgabenordnung   |
| BGB    | Bürgerliches Gesetzbuch  |
| BStBl. | Bundessteuerblatt  |
| HGB    | Handelsgesetzbuch  |
| MMR    | MultiMedia und Recht (Zeitschrift)                                     |
| BAO    | Bundesabgabenordnung   |
| GoBD   | Grundsätze zur ordnungsmäßigen Führung und<br>Aufbewahrung von Büchern |
| UStG   | Umsatzsteuergesetz   |
| EStG   | Einkommensteuergesetz  |
| UGB    | Unternehmensgesetzbuch   |