



TECHNISCHE BESCHREIBUNG

VERSION 2.62

BvLArchivio® – Archivieren ohne Nachbearbeitung – einfach und schnell

BvLArchivio® ist ein Komplettsystem. **BvLArchivio®** ist für die revisionssichere Archivierung beliebiger elektronischer Dokumente konzipiert. Das Besondere an **BvLArchivio®** ist, dass das Betriebssystem bereits auf einer integrierten Festplatte vorhanden ist. Separat dazu gibt es eine Daten- und zwei Sicherungsplatten – diese strikte Trennung von Betriebssystem und Daten gewährleistet ein Höchstmaß an Datenschutz, da der sonst übliche unkontrollierte Datenzugang bei EDV-Administrationen entfällt.

Die Datenspeicherung erfolgt mittels entsprechender Clients über die Protokolle http oder ftp. Clients können Scanner, PCs oder externe Anwendungen sein.

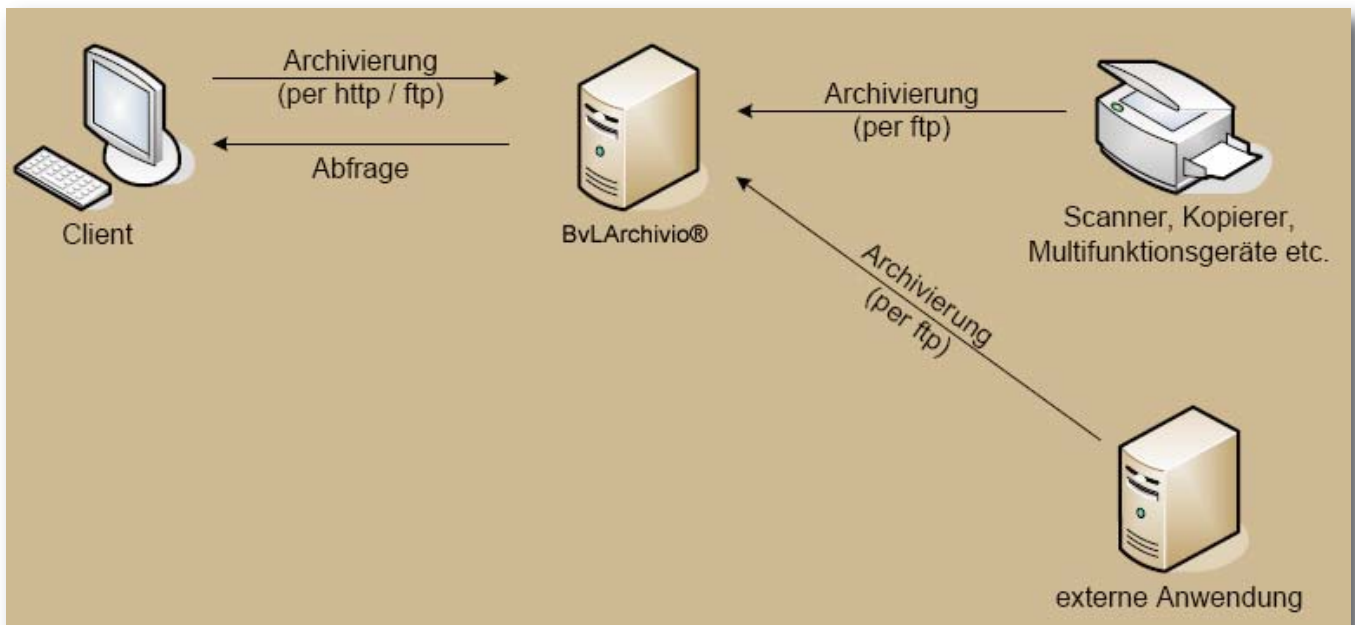
Der Zugriff auf die archivierten Dokumente und Dateien erfolgt über einen Webbrowser (http), mit dem durch Angabe von Suchbegriffen eine entsprechende Anfrage an die integrierte Suchmaschine gestellt wird. Im Ergebnis liefert **BvLArchivio®** eine verlinkte Trefferliste. Die entsprechenden Indexinformationen sind in **BvLArchivio®** in einer separaten Datenbank gespeichert.

Pro **BvLArchivio®**-Box können bis zu fünf Archive angelegt werden, die den Inhalt von etwa 20.000 Ordnern fassen können.

Um bei der Archivierung mit **BvLArchivio®** die Abbildung von Kategorien, Abteilungen oder sonstigen Ordnungskriterien zu unterstützen, gliedert sich die Ablage in fünf Archive (**BvLArchivio®** 1 bis 5). Für den Anwender sind die Archive voneinander getrennt, sowohl im Hinblick auf Ablage und Retrieval als auch Konfigurierbarkeit und Zugriffsschutz.

Das Wiederauffinden von Dokumenten wird von **BvLArchivio®** durch Metainformationen unterstützt, die bei der Speicherung von Dokumenten / Dateien eingegeben/geliefert werden können bzw. bei der OCR- oder Barcodeversion durch Texterkennung oder Barcodeerkennung automatisch generiert werden können.

Die folgende Abbildung stellt die Archivierungs- und Abfragekanäle von **BvLArchivio®** im internen Netzwerk schematisch dar:



BvLArchivio® ist ein Server. **BvLArchivio®** stellt ausgewählte Schnittstellen zur Verfügung und verfügt über einen Netzwerkanschluss, über den sowohl die archivierenden Geräte als auch abfragende Clients angeschlossen werden.

Betriebssystem und Anwendungssoftware von **BvLArchivio®** sind auf der internen Festplatte installiert. Für die Speicherung der Daten (archivierte Dokumente, Indexdatenbank) werden eine Datenfestplatte und eine Sicherungsfestplatte während des Betriebs verwendet. Als Datensicherungsmedium gehört eine weitere Sicherungsfestplatte zum Lieferumfang. Weitere Sicherungsplatten können jederzeit eingesetzt werden. Das Gehäuse ist vom Hersteller versiegelt, so dass für den Anwender kein Zugriff auf die Bestandteile der Lösung vorgesehen ist, mit Ausnahme der Daten- und Sicherungsfestplatte.

Es ist vorgesehen, dass die Sicherungsfestplatten im Wechsel betrieben werden, um – neben der spiegelbildlichen Archivierung auf der Daten- und Sicherungsfestplatte – die erweiterte Datensicherungsfunktion auszuschöpfen.

Das System wird vom Hersteller vorkonfiguriert, für den Anwender sind keine Erweiterungs- oder Einstellungsfunktionen vorgesehen, abgesehen von den üblichen Anwendereinstellungen.

Die maximale Kapazität einer **BvLArchivio®**-Speicherlösung wird durch die verfügbaren Festplattenkapazitäten definiert und liegt bei derzeit 500 GB. Die Kapazität ist nur durch die Festplattengröße begrenzt, die jederzeit und immer wieder durch Einsatz größerer Festplatten erhöht werden kann

Die Verarbeitung der Dateien im zentralen Eingang von **BvLArchivio®** erfolgt sequentiell nach dem FIFO-Prinzip (First In First Out), d. h. die zuerst in den Eingang gelangende Datei wird als erste archiviert. In mehreren Stufen werden die Dateien verarbeitet, wobei erst nach vollständiger Abarbeitung einer Datei die nächste in die Verarbeitung dieser Stufe gelangt. Mit dieser Methode kann die vollständige Archivierung der Dateien gewährleistet werden.

Der Verarbeitungs- und Archivierungsvorgang startet unverzüglich, da der entsprechende Dienst permanent den Eingang überwacht und bei Vorliegen neuer Dateien sofort die Verarbeitung startet. Insoweit hängt die Zeitspanne, die bis zur Archivierung einer Datei vergeht, maßgeblich von der Anzahl und Größe der zu archivierenden Dateien sowie dem Umfang der OCR-Erkennung bei gescannten Dokumenten, die den OCR-Prozess durchlaufen, ab. Bei der Archivierung von Dateien, die nicht von einem Scanner kommen und per ftp-Upload hochgeladen werden, startet die Verarbeitung unverzüglich nach Vorliegen der zu einer Datei gehörenden gleichnamigen Index- bzw. Schlagwortdatei, auch Metadatei genannt.

Tritt ein Fehler während der Archivierung auf, wird die entsprechende Datei in das Fehlerarchiv verschoben. Im Fehlerarchiv stehen pro Fehler verschiedene Informationen zur Verfügung, auf Grund derer die Fehlerursache analysiert werden kann.

Erst wenn die Datei indiziert, der Indexeintrag in der Datenbank gespeichert und schließlich die Datei verschlüsselt auf dem Archivdatenträger gespeichert wurde, erfolgt die systemseitige Löschung der Datei im temporären Verzeichnis. Sollte es also während der Archivierung zu einem Systemabsturz kommen, kann der Löschbefehl nicht abgesetzt und damit die Archivierung nicht abgeschlossen werden. Bei einem erneuten Systemstart wird die Archivierung an der Stelle wieder in Gang gesetzt, an der sie abgebrochen ist. Diese Maßnahme bewirkt zum Einen, dass die Vollständigkeit der Archivierung sichergestellt ist und zum Anderen, dass die Indexdatenbank konsistent bleibt.

Vollständigkeit und Zeitnähe der Speicherung in **BvLArchivio®** können durch das System gewährleistet werden.

BvLArchivio® speichert archivierte Daten immer in verschlüsselter Form.

Zusätzlich sind Dateiattribute zum Schutz gegen Löschen gesetzt.

Das System gestattet dem Nutzer den Zugriff auf das Archiv von außen nur über das Web-Interface sowie per ftp (http & ftp). Eine Lösch- oder Änderungsfunktion ist innerhalb des Web-Interfaces nicht verfügbar, sondern nur eine Retrieval-Funktion.

Nachdem Daten per ftp in den zentralen Eingang als temporärer Speicher gelangen, unterliegen sie einem Zugriffsschutz und sind für den Anwender nicht mehr änderbar. Eine versehentliche Archivierung kann somit nicht rückgängig gemacht werden.

Eine Änderung von archivierten Daten ist innerhalb des Systems nicht möglich. Weder die Web-Oberfläche noch das System an sich bieten dafür die entsprechende Funktionalität an.

BvLArchivio® kann gescannte Dokumente im TIFF-Format verarbeiten. Ein TIFF ist das übliche Quellformat, das von Scannern standardmäßig bereitgestellt wird. Während der internen Verarbeitung von **BvLArchivio®** wird das TIFF in ein PDF/A-Dokument umgewandelt.

PDF/A ist eine für die Langzeitarchivierung von elektronischen Dokumenten konzipierte Spezifikation. PDF/A liegt bei der ISO als Standard vor. Auf Grund ihres wachsenden Verarbeitungsgrads und der vielfach kostenfreien Verfügbarkeit von entsprechenden Viewern ist davon auszugehen, dass PDF/A langfristig lesbar bleibt.

Bei der Archivierung mit **BvLArchivio®** werden nur TIFF-Dateien umgewandelt. Alle übrigen Dateiformate werden nicht komprimiert und sofort ins Archiv verschoben.

PDF/A ist ein für die Langzeitarchivierung konzipiertes Dateiformat, das auch für die bildliche Aufbewahrung und Darstellung von rechnungslegungsrelevanten Belegen und Dokumenten dienen kann und immer häufiger im Archivierungsumfeld eingesetzt wird. Auf Grund seines zunehmenden Verbreitungsgrades und der vielfach kostenfrei erhältlichen Betrachtungssoftware ist ein Ende seiner Verwendung nicht abzusehen. Daher kann – aus heutiger Sicht – auch die Lesbarkeit über die gesamte Aufbewahrungsfrist hinweg gewährleistet werden.

Für die Speicherung der Indexdaten wird eine Datenbank genutzt. Diese verfügt über einen Indizierungs- und Abfragealgorithmus, der auch große Datenmengen schnell verarbeiten kann.

Für jeden Suchbegriff wird ein Indexeintrag mit Verweis auf den Dateinamen der archivierten Datei generiert.

Für die Indizierung werden bei der Archivierung **per http** in einem Webformular Suchbegriffe angegeben und dann mit der archivierten Datei verknüpft.

Bei der Archivierung **per ftp-Upload** muss pro zu archivierender Datei eine gleichnamige Textdatei hochgeladen werden. Diese Textdatei muss die gewünschten Suchbegriffe enthalten, wird jedoch selbst nicht archiviert. Erst nach bereitstellen der Textdatei startet die Archivierung.

Bei der Archivierung per Scanner werden TIFF-Dateien vor ihrer Archivierung automatisch durch einen OCR-Prozessor geleitet und anhand der erkannten Suchbegriffe indiziert. Verbindliche Maßgabe bei Archivierung von TIFF-Dateien oder gescannten Dokumenten ist eine Auflösung von 300 dpi. Scanner, Kopierer und ähnliche externe Geräte können als automatische Quelle von zu archivierenden Dokumenten eingesetzt werden, müssen jedoch nach dieser Maßgabe konfiguriert werden.

Die Indizierung von TIFF-Dateien kann über Steuerbefehle beeinflusst werden. Mit festgelegten Befehlen können eine begrenzte Anzahl Wörter der per OCR erkannten Dokumente als Suchbegriffe aufgenommen, eine Volltextindizierung veranlasst und zusätzliche Suchbegriffe angegeben werden. Dabei muss das Archiv angegeben werden, in das die jeweilige Datei verschoben werden soll.

Um eine Fehlindizierung und dadurch die Unauffindbarkeit der archivierten Dokumente zu verhindern, sind verschiedene Schutzmechanismen implementiert. So wird der Archivierungsversuch ohne Angabe von Suchbegriffen bei den angebotenen Archivierungskanälen verhindert. Auch bei weiteren auftretenden Fehlern während der Archivierung wird die Datei ins Fehlerarchiv verschoben. Zusätzlich legt **BvLArchivio®** begleitende Informationsdateien an, die die Fehlersuche und -analyse unterstützen.

BvLArchivio® stellt für den Zugriff auf die archivierten Dokumente eine Suchmaschine zur Verfügung. Eine Suchanfrage erfolgt durch Angabe von Suchbegriffen mit einer festgelegten Syntax zur Verfeinerung und Filterung der Ergebnisse. Gefundene Dokumente werden als verlinkte Trefferliste angezeigt und können einzeln abgerufen werden. Die Anzeige der Suchergebnisse berücksichtigt die Reihenfolge der Archivierung.

Sollen mehrere Dokumente gleichzeitig abgerufen werden (z. B. alle Rechnungen von 01.01. bis 31.12.), kann die Suchanfrage per Exportbefehl gestellt werden. Die gefundenen Dokumente werden in einem Exportverzeichnis per ftp zum Download bereitgestellt. Zum Schutz vor Massendownload des Archivs und zur Verhinderung der unverhältnismäßigen Beanspruchung der Hardware durch internes Umkopieren und Entschlüsseln der Dateien ist die maximale Anzahl gleichzeitig herunterladbarer Dokumente auf 5.000 begrenzt. Zusätzlich stehen in der beiliegenden Textdatei die für alle gerade exportierten Dateien gespeicherten Suchbegriffe zur Verfügung.

Mittels verschiedener Einstellungen kann die Abfragemöglichkeit einem Berechtigungskonzept unterworfen werden, so dass anfragende IP-Adressen

- von der Benutzung bestimmter Suchbegriffe ausgenommen sind (Blacklisting),
- keinen Export initiieren können oder
- nur bestimmte Suchbegriffe (Whitelisting) und -zeiträume verwenden dürfen.

Die Datenstruktur der Indexdatenbank ist einfach gehalten. Den gespeicherten Suchbegriffen ist direkt der Dateiname des entsprechenden Dokumentes auf dem Archivdatenträger zugeordnet. Das System kann mit dem Dateinamen direkt auf das Dateisystem zugreifen und damit die unverzügliche Lesbarmachung gewährleisten.

Um Datenverluste durch Plattendefekte zu verhindern, sind die Archivdatenträger redundant ausgelegt. In Verbindung mit der regelmäßigen Synchronisation und einer angemessenen Lagerung der Archivdatenträger untereinander, welches in der Verantwortung des Anwenders liegt, vermag das System das Risiko des Datenverlusts durch Festplattendefekte wirksam zu minimieren.

Das implementierte Berechtigungskonzept erlaubt die Steuerung des Zugangs zu den einzelnen Archiven. Jedes Archiv erfordert bei Zugang die Angabe einer bestimmten, vom Anwender änderbaren Nutzer-Passwort-Kombination, die sowohl bei Zugang per ftp als auch per http angegeben werden muss. Zusätzlich kann die Berechtigung zur Archivierung von der Eingabe eines bestimmten Schlüsselwortes abhängig gemacht werden. Nur wenn der Nutzer, der archivieren will, autorisiert ist und er das entsprechende Schlüsselwort bei der Archivierung angibt, wird der Befehl ausgeführt. Bei fehlender oder falscher Angabe des Schlüsselworts wird der Archivierungsversuch verworfen.

Neben dem Zugangsschutz für die einzelnen Archive sowie der separaten Autorisierung der Archivierung sieht **BvLArchivio®** die Möglichkeit vor, die Abfragemöglichkeiten einzuschränken. Es können ein oder mehrere Suchbegriffe in ihrer Reihenfolge zwingend vorgegeben oder bestimmte Suchbegriffe explizit verboten werden. Die Durchsetzung dieser Regeln wird mit Hilfe der IP-Adresse des anfragenden Clients erreicht, für den die Reglementierung des Zugangs erfolgen soll.

Ferner ist die Firewall des Betriebssystems mit sehr restriktiven Einstellungen aktiviert.

Port 80 (http) steht für die Kommunikation mit dem Archiv über das Web-Interface zur Verfügung, Port 20 und 21 (ftp) für die Archivierung und den Export. Alle übrigen Ports sind in den gefilterten Zustand versetzt und bieten damit einen hohen Schutz gegen Angriffe auf Netzwerkebene.

Archivierte Daten werden verschlüsselt auf den Archivdatenträgern abgelegt. Damit ist es möglich, die Daten insbesondere bei Verlust der Archivdatenträger oder Betrieb der Archivdatenträger in einem anderen System wirksam vor Zugriff und Einsichtnahme zu schützen, da der Schlüssel individuell für jeden Anwender eingerichtet wird und die Daten daher nur im Originalsystem gelesen werden können. Mittels EFS sind sowohl Daten als auch die Programmlogik verschlüsselt und damit wirksam vor unbefugtem Zugriff bzw. nicht autorisierter Einsichtnahme geschützt.

Betriebssystem und Anwendung sind auf der internen Festplatte gespeichert, die im unzugänglichen Gehäuse des **BvLArchivio®- Servers** verbaut ist. Das Gehäuse ist mit einem Siegel geschützt. Zum Öffnen des Gehäuses ist es erforderlich, das Siegel zu entfernen. Da das Siegel sich aber nicht rückstandsfrei entfernen lässt und damit beim Öffnen des Gehäuses zerstört wird, kann eine mögliche Manipulation der Hardware leicht nachgewiesen werden.

Zum Schutz vor Datenverlust und unberechtigter Veränderung verfügt das System über eine Daten- und eine Sicherungsfestplatte. Um die beabsichtigte Redundanz der Datenhaltung bei auftretenden Fehlern auch im laufenden Betrieb aufrechterhalten zu können, verfügt das System über eine selektive Abschaltung der Archivierungs- und Retrieval-Funktionalität. Bei Fehlen (z. B. plötzliches Herausziehen der Platte oder Plattendefekt) der Sicherungsfestplatte ist die Abfrage von Dokumenten weiterhin möglich, das Archivieren dagegen nicht mehr. Wird die Datenfestplatte nicht mehr erkannt, ist weder Archivieren noch Abfragen möglich. Das System schützt sich damit vor inkonsistenter Datenhaltung, da die Datenfestplatte maßgeblich für den Datenbestand ist.

Ein weiterer Schutzmechanismus ist die interne Zuordnung der Festplatten und Erkennung als Daten- oder Sicherungsfestplatte, losgelöst von der Einsteckreihenfolge und –position der Festplatte somit korrekt erkannt, unabhängig davon, ob der obere oder der untere SATA-Schacht für die Daten- bzw. Sicherungsfestplatte verwendet wird.

Wie empfohlen, sollte **BvLArchivio®** an eine USV angeschlossen werden, um abrupte Stromausfälle und dadurch bedingte eventuelle Datenverluste zu vermeiden.

Zusätzlich wird empfohlen, **BvLArchivio®** in einem entsprechend gesicherten Raum aufzustellen und den Zutritt möglichst restriktiv zu gestalten. Auch die Sicherungsfestplatte sollten unter angemessenen physischen Bedingungen und zusätzlich räumlich getrennt vom Server, z. B. in einem Tresor oder abschließbaren Raum, aufbewahrt werden.

BvLArchivio® ist so konzipiert, dass die Daten mindestens dreifach vorhanden sind. Auf der Datenfestplatte, die als Drehscheibe für die Datensicherung und Wiederherstellung dient, befindet sich der vollständige Datenbestand. Auf dem Datenbestand der Datenfestplatte werden außerdem die Suchanfragen bearbeitet. Zweiter Speicherort der Daten ist die Sicherungsfestplatte. Zudem wird eine zweite Sicherungsfestplatte mitgeliefert, auf der sich bei regelmäßigem Wechsel zwischen den zwei Sicherungsfestplatte ebenfalls ein kompletter Datenbestand befindet.

BvLArchivio® schreibt den regelmäßigen Wechsel der mitgelieferten Sicherungsfestplatten vor. Im Prinzip wird die Wiederherstellbarkeit täglich respektive bei jedem Neustart getestet, da ein automatischer Abgleich zwischen der Daten- und der eingesetzten Sicherungsfestplatte durchgeführt wird. Bei Plattendefekten würde dieser Abgleich scheitern. Das System fährt daraufhin nicht wieder hoch. Mit einer neuen Platte kann das System den Abgleich vollständig durchführen.

Bei Ausfall des Servers können die Platten problemlos in eine baugleiche Austauschereinheit eingesetzt und dort betrieben werden.

Die Datenfestplatten enthalten alle wesentlichen Datenbestände. Dazu gehören sowohl die archivierten Dateien als auch die Indexdatenbank, die zur Wiederauffindbarkeit der Dateien erforderlich ist.

Um einen ausreichenden Schutz vor Datenverlust zu erreichen, muss der Anwender dafür Sorge tragen, dass die Sicherungsfestplatten entsprechend regelmäßig ausgetauscht werden.

Um dem Löschungs- bzw. Sperrungsgebot des BDSG (Bundesdatenschutzgesetzes) nachzukommen, müssen Daten zeitnah (nach Hinfälligkeit der Berechtigung zur Speicherung) bzw. nach Ablauf der gesetzlich zulässigen Aufbewahrungsfrist aus dem System entfernt werden können.

BvLArchivio® ist so konzipiert, dass das Löschen von Dateien innerhalb des Systems nicht möglich ist. Für datenschutzrechtlich relevante Szenarien muss das Löschen also außerhalb des Systems vorgenommen werden. Da die Dateien verschlüsselt abgelegt sind, müssen die entsprechenden Dateien vorher identifiziert und lokalisiert werden.

Um das gezielte Löschen von Dateien dennoch zu unterstützen, bietet das System eine Exportfunktion an. Mittels Exportfunktion werden die durch eine Suchanfrage ausgewählten Dateien in das Exportverzeichnis des Archivsystems gestellt und können dort per ftp abgerufen werden. Zusätzlich stellt die Exportfunktion eine Indexdatei zur Verfügung, die alle gefundenen und exportierten Dateien einschließlich aller dazu gespeicherten Suchbegriffe sowie des Dateinamens auf dem Archivdatenträger auflistet. Mit Hilfe dieser Dateiliste kann – auch automatisiert – die Löschung der datenschutzrechtlich relevanten Dateien erfolgen.

Die Löschung der Daten muss sowohl auf der Datenfestplatte als auch auf allen Sicherungsfestplatten vorgenommen werden, bevor das System wieder in Betrieb genommen wird, da andernfalls der Sicherungsmechanismus die Daten wiederherstellt.

Dateien können zwar außerhalb des Systems und bei Kenntnis der Ablagesystematik gelöscht werden. Die Indexdaten bleiben jedoch erhalten und können nicht selektiv gelöscht werden, da sie verschlüsselt sind. Gelöschte Dateien sind dem Zugriff wirksam entzogen, der Verweis darauf in der Indexdatenbank bleibt dennoch erhalten und zeigt damit an, dass die Datei archiviert und wieder gelöscht wurde.

Mit dieser Methode können die Daten wirksam gelöscht werden sowie vor weiterem Zugriff geschützt werden. Als begleitende Maßnahme bei Einsatz der Löschung empfehlen wir die Berücksichtigung des Vier-Augen-Prinzips sowie die Dokumentation des Vorgehens. Den Anforderungen des BDSG kann dadurch wirksam entsprochen werden.

Auf Grund der von der KPMG durchgeführten Prüfung, nach dem vom Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW) veröffentlichten Prüfungsstandard PS 880, **ist BvLArchivio® mit dem Zertifikat PS880 ausgestattet.** **BvLArchivio®** ermöglicht eine Speicherung und Abfrage von elektronischen Dokumenten, die den deutschen Grundsätzen ordnungsmäßiger Buchführung entspricht. Grundlage der Prüfung waren die Bestimmungen nach den gesetzlichen Vorschriften des Handels- und Steuerrechts (§§ 238 ff. HGB sowie §§ 140 - 148 AO), die Grundsätze ordnungsmäßiger Buchführung (GoB), das Schreiben des Bundesfinanzministers (BMF) vom 7. November 1995 zu den "Grundsätzen ordnungsmäßiger DV-gestützter Buchführungssystemen" (GoBS), das BMF-Schreiben vom 16. Juli 2001 zu den "Grundsätzen zum Datenzugriff und der Prüfbarkeit digitaler Unterlagen (GDPdU), die Stellungnahme zur Rechnungslegung des Fachausschusses für Informationstechnologie (FAIT) des Instituts der Wirtschaftsprüfer in Deutschland e.V. (IDW) "Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie" (IDW RS FAIT 1), die IDW-Stellungnahme zur Rechnungslegung des FAIT "Grundsätze ordnungsmäßiger Buchführung beim Einsatz elektronischer Archivierungsverfahren" (IDW RS FAIT 3), der IDW-Prüfungsstandard "Abschlussprüfung bei Einsatz von Informationstechnologie" (IDW PS 330), sowie der IDW-Prüfungsstandard "Erteilung und Verwendung von Softwarebescheinigungen" (IDW PS 880).



BvL Bürosysteme Vertriebs GmbH

Müllerstrasse 138d
13353 Berlin

Tel. (030) 454 781-0
Fax (030) 454 781-781

WWW.BVLARCHIVIO.DE
SERVICE@BVLARCHIVIO.COM