

**Rechtsgutachten des gingcom Archivsystems  
von Rechtsanwalt Dr. Ivo Geis**

**Glockengießerwall 26  
20095 Hamburg**

## **Auftrag**

Die gingcom GmbH

Saline 29

78628 Rottweil

hat mich beauftragt, das gingcom Archivsystem rechtlich zu begutachten.

Ich habe das Gutachten in der Zeit von Anfang März bis Ende Mai 2007 erstellt.

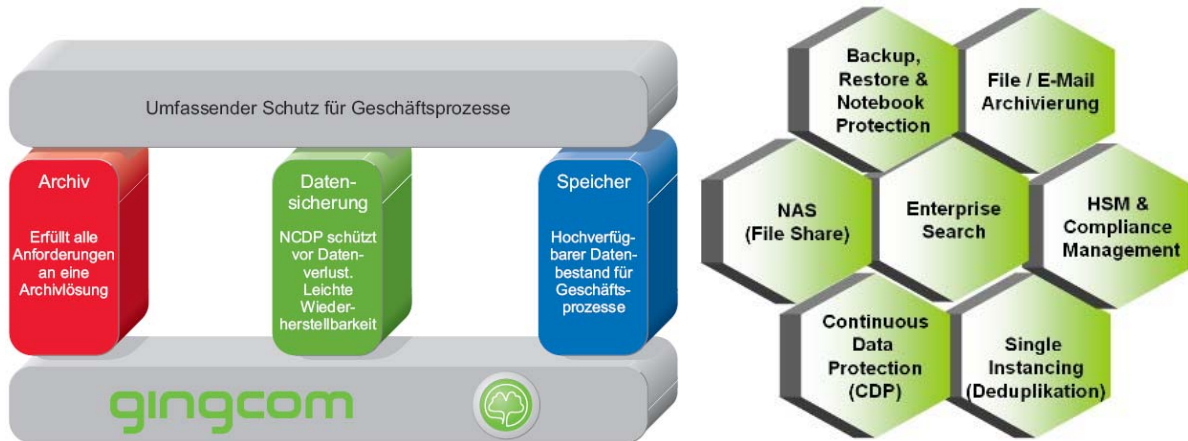
Auskunft ist mir von Herrn Steffen Reusch, Leiter Marketing, und Herrn Oliver Haug, Product Manager, erteilt worden.

## Inhalt

Auftrag .....	2
1.0 Sachverhalt: Die Speichersysteme der gingcom GmbH .....	4
1.1 gingcom Datenmanagement Funktionalitäten.....	4
1.1.1 File- und E-Mail Archivierung.....	5
1.1.2 NAS & HSM .....	5
1.1.3 Selbstüberwachung.....	6
1.1.4 Notebook Protection.....	7
1.1.5 Enterprise Search.....	8
1.1.6 CAS und Single Instancing .....	9
1.1.7 Die Definition der Aufbewahrungszeit der Archivdaten .....	10
1.1.8 Datenintegrität durch Unveränderbarkeit.....	11
1.1.9 Online- und Nearline Speicher .....	12
1.1.10 Such-, Abrufvorgänge und Audit Log: Protokollierung der Zugriffe .....	13
1.1.11 Zusammenfassung: Wert für die Rechtssicherheit.....	14
1.2 Near Continuous Data Protection (NCDP) .....	14
1.2.1 NCDP – Datensicherung .....	14
1.2.2 RPO – Liste .....	14
1.2.3 Zusammenfassung: Wert für die Rechtssicherheit.....	15
1.3 Dokumentation des gingcom Systems .....	15
1.4 Zusammenfassung .....	16
2.0 Rechtliche Bewertung .....	17
2.1 Rechtliche Anforderungen an die ordnungsmäßige elektronische Archivierung ....	17
2.1.1 Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme .....	17
2.1.2 Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen .....	21
2.1.3 Basel II, Sarbanes Oxley Act und Dokumentationspflicht .....	22
2.1.4 Ergebnis für gingcom .....	23
2.2 Vertragsabschluss durch elektronische Kommunikation .....	23
2.3 Die Beweisqualität elektronischer Dokumente .....	23
2.3.1 Freie Beweiswürdigung.....	24
2.3.2 Die Beweisqualität von gingcom .....	24
3.0 Ergebnis der rechtlichen Begutachtung und Zertifikat .....	25
3.1 Ordnungsmäßige Archivierung von Dokumenten .....	25
3.2 Rechtswirksamkeit elektronischer Erklärungen.....	25
3.3 Beweissicherheit elektronischer Dokumente .....	25
3.4 Zusammenfassung.....	25
Literaturverzeichnis.....	26
Glossar und Abkürzungen.....	27
Kurzbiographie und ausgewählte Publikationen.....	44

## 1.0 Sachverhalt: Die Speichersysteme der gingcom GmbH

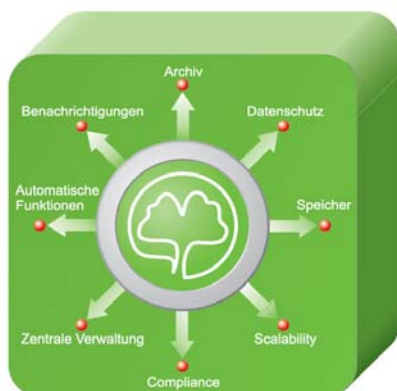
gingcom ist eine „All In One Box“ Lösung, die sehr flexibel eingesetzt werden kann. Idealerweise werden ganze Unternehmensprozesse abgedeckt. gingcom begleitet Daten von ihrer Entstehung über den gesamten Lebenszyklus bis hin zur Löschung oder dauerhaften Archivierung. gingcom kann stufenweise implementiert werden um z.B. heute einzelne Unternehmensbereiche abzudecken und morgen zukünftigen Entwicklungen Rechnung zu tragen, was einen optimalen Investitionsschutz bietet.



## 1.1 gingcom Datenmanagement Funktionalitäten

gingcom stellt eine Reihe von Datenmanagementfunktionalitäten zur Verfügung:

- 1.1.1 File und E-Mail-Archivierung
- 1.1.2 NAS & HSM
- 1.1.3 Selbstüberwachung
- 1.1.4 Notebook Protection
- 1.1.5 Enterprise Search
- 1.1.6 CAS und Single Instancing



### **1.1.1 File- und E-Mail Archivierung**

gingcom bietet zuverlässigen Schutz aller Server und Clients in einem Netzwerk.

Nachdem die entsprechenden Dateisysteme und Schutzmethoden ausgewählt wurden, sind diese Systeme mit der nahezu fortlaufenden Datensicherungstechnologie NCDP (Near Continuous Data Protection, vgl. 1.2.1) geschützt. Auf jedem Einzelsystem ist ein installierter Agent für die ständige Kommunikation mit dem gingcom Server verantwortlich. Für jedes System kann eine Gruppe von Schutzparametern und die Granularität entsprechend der jeweiligen Daten eingestellt werden. Es kann frei bestimmt werden, ob die Daten nur gesichert oder auch archiviert werden sollen, indem die entsprechenden Backup- und Archivierungsparameter eingestellt werden.

Microsoft Exchange ist inzwischen zur zentralen Plattform für die elektronische Bürokommunikation geworden. Um ein E-Mail-System vor einem potenziellen Datenverlust zu schützen, sollte ein Schwerpunkt auf ein umfassendes Backup aller relevanten Mailbox-Datenspeicher und Transaktionsprotokolle gelegt werden. gingcom bietet die Flexibilität, eine Microsoft Exchange-Datenbank ebenso wie einzelne E-Mails zu sichern bzw. zu archivieren, um sie dann bei Bedarf wiederherzustellen. Jeder Anwender kann E-Mail Daten in seinem Archiv anhand inhaltsbezogener oder anderer Informationen durchsuchen (zum Beispiel, Betreff/AN/Kopie An), um dann die dazugehörigen Daten abzurufen.

Der Wert für die Rechtssicherheit der File und E-Mail-Archivierung besteht in der hierdurch erreichten Datenintegrität.

### **1.1.2 NAS & HSM**

gingcom verfügt über eine integrierte NAS-Speicherlösung. Bei einem NAS (Network Attached Storage) werden Massenspeichereinheiten an ein lokales Netzwerk angeschlossen. Hierbei können Dateien von einem Client mit Zugriffsrechten abgespeichert werden. Anhand einer Reihe von Richtlinien für die jeweiligen Objekte werden die Dateisysteme in dem integrierten NAS-Dateibereich ständig auf Änderungen geprüft. Alle gingcom Schutzfunktionen gelten auch für die integrierte NAS-Speicherlösung.

Die HSM-Funktion (Hierarchical Storage Management) verwaltet Daten, die sich in der integrierten NAS-Speicherlösung befinden. Während das NAS den Speicherplatz für die gemeinsame Nutzung von Daten bietet, vereinfacht HSM die Datenspeicherung durch eine

vollautomatisierte Übertragung von Daten zwischen Online-Speicher und Archiv, also zwischen den Festplatten und den Archivbändern. Um eine ständige optimale Ausnutzung der NAS Speicherlösung zu gewährleisten, wurden so genannte „Watermarks“ festgelegt. Sobald der belegte Festplattenplatz die „High Watermark“ überschreitet, beginnt das HSM mit dem Verlagern von Daten aus dem NAS. Das Verlagern wird eingestellt, sobald die „Low Watermark“ erreicht ist.

Durch NAS und HSM wird die Integrität der Daten gesichert.

### **1.1.3 Selbstüberwachung**

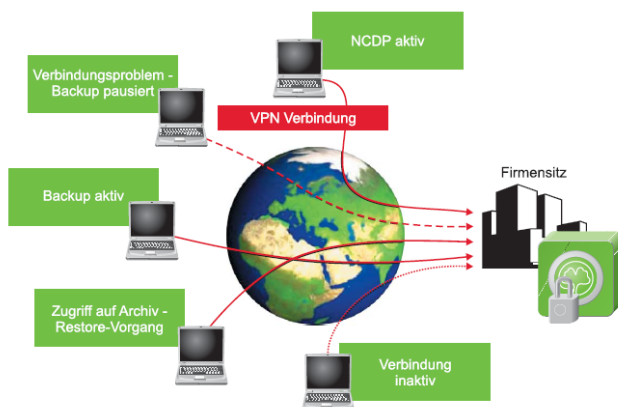
Die Selbstüberwachung zusammen mit Selbstheilungsfunktionen reduziert aktiv mögliche Fehlerursachen und Abweichungen bei laufenden Prozessen. Aufgetretene Störungen werden erkannt, gemeldet und wenn möglich automatisch behoben. Zu diesem Bereich der Selbstüberwachung zählen auch weitere automatisierte Funktionen wie Prüfungen der Datenbankkonsistenz und Datenredundanz. Zur Sicherstellung der Datenintegrität umfasst die interne gingcom Funktionalität auch regelmäßige Konsistenzprüfungen der internen Datenbanken und Prüfungen der Wiederherstellungsfähigkeit, um ununterbrochene Unternehmensprozesse und die gingcom Wiederherstellungsfähigkeit zu sichern. Für diese Tests werden Zufallsdaten ausgewählt und deren Hash-Wert überprüft. Auftretende Widersprüche lösen eine Benachrichtigung des Administrators per E-Mail und einen Eintrag im Ereignisprotokoll aus. Die gingcom Appliance führt außerdem regelmäßige Überprüfungen aller Sicherungen der internen Datenbanken und Konfigurationsdaten durch, um die Integrität der geschützten Daten und die Wiederherstellungsfähigkeit von gingcom selbst bei einem Datenausfall zu sichern. Alle Widersprüche werden im Ereignisprotokoll eingetragen und der Administrator wird benachrichtigt. Beide Prüfungen sind Teil der gingcom Selbstverwaltung.

Hierdurch wird die Integrität der Daten gesichert.

### 1.1.4 Notebook Protection

gingcom setzt unterschiedliche Technologien ein, um einen transparenten und automatischen Schutz der Unternehmensdaten ihrer mobilen Anwender zu erreichen. Der gingcom Notebookschutz ist Teil einer umfassenden Schutzstrategie für Dateisystem, Systemzustand und Microsoft Exchange Server Daten. Die einzige zusätzliche Voraussetzung für eine mobile Datensicherung ist eine bestehende VPN-Verbindung. Für einen erfolgreichen Schutz von Unternehmensdaten auf Notebooks wird auf dem Client ein Dateisystemagent eingesetzt. Sämtliche Richtlinienereinstellungen für Datenschutz und Datenaufbewahrung werden zentral vom gingcom Administrator verwaltet und finden auf den mobilen Clients wie auch auf stationären Rechnern im Firmenhauptquartier gleichermaßen Anwendung. Die Einstellungen sollten in Übereinstimmung mit Ihren Unternehmensanforderungen erfolgen. Sobald ein Agent installiert, Richtlinien erstellt sind und eine VPN-Verbindung besteht, wird das jeweilige Notebook automatisch geschützt. Da der gingcom CAS-Dienst eine Single Instancing Funktion beinhaltet, wird ein überflüssiger Datentransfer vermieden. Während des Datenübertragungsvorgangs wird die verfügbare Netzgeschwindigkeit laufend überwacht. Dem Anwender steht es frei, die Datenübertragung anzuhalten und später fortzusetzen. Ein mobiler Anwender kann jederzeit komfortabel nach seinen Daten suchen und sie über die gingcom Web-Benutzeroberfläche abrufen. Die Suchfunktion ist im Aufbau an verbreitete Suchmaschinen angelehnt und gestattet einem mobilen Arbeiter den schnellen Zugriff auf seine gespeicherten Dateien, immer vorausgesetzt, es besteht eine ausreichende Netzverbindung. Die Datensicherung beruht auf Richtlinien, die zentral vom Administrator verwaltet werden. Gleichzeitig werden auch die verschiedenen Nachteile von Fernverbindungen berücksichtigt. Mit gingcom wird für eine umfassende Datensicherung und den Archivzugriff durch mobile Anwender lediglich die bereits vorhandene VPN-Infrastruktur benötigt.

Beispiel: Notebook Infrastruktur mit zentral implementiertem gingcom Appliance.

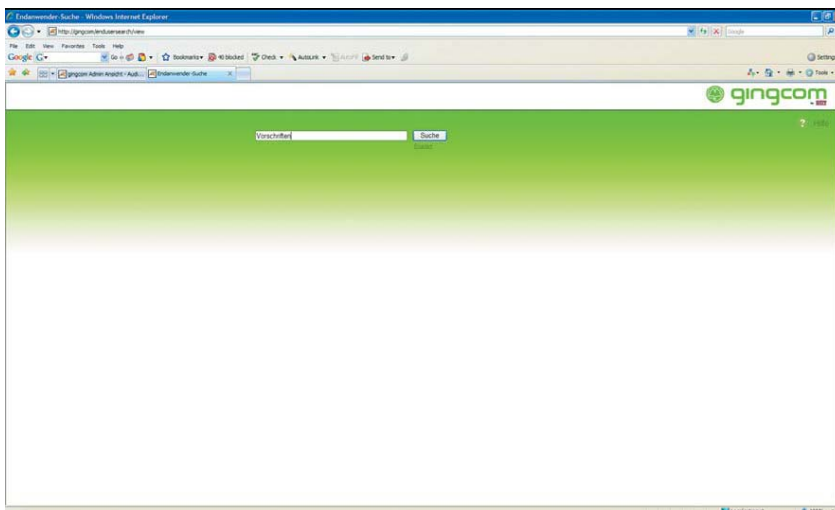


Das gingcom Konzept für die Sicherung mobiler Daten beruht auf einer zentralen Datenverwaltung durch Richtlinien, die auch für Außenstellen und bei mobilen Mitarbeitern angewendet werden können. Damit sind diese Mitarbeiter von allen Aufgaben der Datensicherung befreit. Ein Anwender kann einfach sein Notebook anschließen, eine Netzverbindung herstellen und wie gewohnt arbeiten, da die gingcom Prozesse im Hintergrund ablaufen und seinen gewohnten Arbeitsablauf nicht stören. Mobile Anwender können auf Ihre gespeicherten Daten jederzeit zugreifen und diese abrufen. Ein extern arbeitender Notebookanwender benötigt zur Wiederherstellung seiner Daten keine Unterstützung durch einen IT-Spezialisten. Er kann, soweit eine Netzwerkverbindung besteht, seine Backup oder Archiv Daten durchsuchen und selbst wiederherstellen. Mit der gingcom Web Oberfläche ist es dem Anwender möglich, die aktuellste Version der Daten oder eine der in gingcom gespeicherten Vorgängerversionen abzurufen.

Im Ergebnis wird durch Notebook Protection die Integrität der Daten gesichert.

### 1.1.5 Enterprise Search

Die gingcom Suche ist ähnlich aufgebaut wie bei bekannten Web-Suchmaschinen. Suche bietet eine standardmäßige Suche nach Schlüsselwörtern im Dokumentenkörper und auch eine erweiterte Suche nach Metadaten, zum Beispiel Verfasser/Eigentümer, Titel, Daten, Dateityp sowie E-Mail-Informationen wie Von, Zu, Kopie an.



Die durch eine Suchabfrage gefundenen Elemente werden in der Ergebnisliste angezeigt. Einzelheiten wie der Titel und der Dateiname des Dokuments und sein ursprünglicher Speicherplatz werden ebenfalls angezeigt. Gibt es von einem Objekt mehrere Versionen,

werden nach der Auswahl der ausgewählten Version in der Ergebnisliste detaillierte Informationen über die Datei angezeigt. Zu jedem aufgeführten Element gibt es einen Download Link, mit dem die ausgewählte Datei auf einem dem Anwender zugeordneten Download Bereich im Online-Speicher von gingcom bereitgestellt wird. Von dort kann die Datei dann an einen beliebigen Speicherplatz herunter geladen werden.

Ähnlich wie dem Endanwender stehen auch dem Administrator zwei Suchfunktionen zur Verfügung: Eine standardmäßige und eine erweiterte Suchfunktion. Die durch eine Suchabfrage gefundenen Elemente werden in der Ergebnisliste mit ihren jeweiligen Einzelheiten angezeigt. Sobald die Datenversion oder das ganze Dateiverzeichnis für eine Rückspeicherung ausgewählt ist, wird im Feld Download-Status deren Status angezeigt.

Im Ergebnis wird durch Enterprise Search die Wiedergabe der gespeicherten Daten gesichert.

#### **1.1.6 CAS und Single Instancing**

Bei CAS (Content Addressed Storage - inhaltsadressierte Speicherung) handelt es sich um die zu Grunde liegende Technologie für jede Art von Datentransfer zwischen gingcom Clients sowie Online- und Nearlinespeicherung. CAS besteht aus der CAS Objektdatenbank, der Medien- und Gerätedatenbank und den zugehörigen Journaldateien. Während der Datenübertragung berechnet CAS die benötigten Hash-Werte für Single Instancing und unterstützt nachfolgende Such- und Abruffunktionen. CAS implementiert daneben auch die Funktionalität für das Löschen ungültiger Objekte sowie der Medienkonsolidierung.

CAS ermöglicht eine Speicherverwaltung ohne Dateidoppelkopien (Single Instancing) durch Verweise auf die jeweils gespeicherten Kopien identischer Dateien. Dabei kommunizieren jeweils die Client Agenten mit dem CAS-Dienst und stellen so sicher, dass nur neue oder veränderte Dateien an gingcom übertragen werden. Diese Methode ermöglicht eine optimale Ausnutzung des vorhandenen Speicherplatzes und senkt den Bandbreitenbedarf. Sämtliche gingcom Datensicherungsvorgänge können über eine bestehende 10/100/1000-Mb/s-Infrastruktur ausgeführt werden, wie sie im Regelfall bei mittelständischen Firmen vorhanden ist. Alle gingcom Appliances verwenden SHA-1-Hash-Funktionen als Prüfsummen- und Verifizierungsalgorithmus für alle geschützten Daten, jeweils vor und nach der Speicherung in der mehrstufigen Speicherungsstruktur von gingcom. Jeder geschützten Datenversion wird ein eindeutiger Hash-Schlüssel zugewiesen, der damit Echtheit und Integrität sichert. Als Resultat einer jeden, auch noch so geringfügigen Veränderung der Datei

wird konsequent ein neuer Hash-Schlüssel erzeugt. Durch Vergleich der Hash-Schlüssel werden original und nachfolgende Versionen einer gleichen Datei zuverlässig unterschieden. Die Hash-Prüfung bildet zugleich die Grundlage für Single Instancing.

CAS und Single Instancing unterstützen die Wiedergabe der gespeicherten Daten und die Integrität.

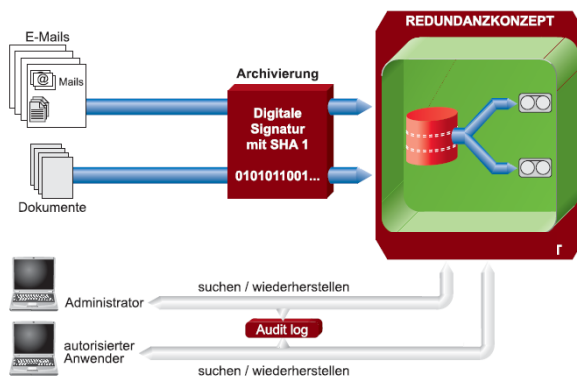
### **1.1.7 Die Definition der Aufbewahrungszeit der Archivdaten**

Bei der Einrichtung der Archivrichtlinien in gingcom wird ein geeigneter Wert für die Aufbewahrungszeit der Archivdaten (ART) gewählt. Diese Angabe richtet sich nach den jeweiligen Unternehmensanforderungen und den geltenden Vorschriften. Der als ART-Parameter (Aufbewahrungszeit für Archivdaten) angegebene Zeitraum überschreitet stets den im BRT-Parameter (Aufbewahrungszeit für Backup-Daten) angegebenen Zeitraum. Mit anderen Worten: Die Verfügbarkeit der Daten für eine eventuelle Rückspeicherung wird durch die Aufbewahrungszeit für Backup-Daten ausgedrückt, während die Aufbewahrungszeit für Archivdaten den Zeitraum für die langfristige Aufbewahrung angibt. BRT legt den Zeitraum fest, in dem Daten für eine Rückspeicherung mit der Suchlauffunktion (Browse) zur Verfügung stehen. ART legt den Zeitraum fest, in dem gespeicherte Daten mit der Suchfunktion (Search) durchsucht werden können. Zum Beispiel kann nach einer Datenversion mit einem abgelaufenen BRT nicht mehr mit der Browse-Funktion gesucht werden, sie wird jedoch immer noch im Speicher aufbewahrt. Es ist möglich solange mit der Search-Funktion nach diesen Daten zu suchen und diese abzurufen, bis der ART Wert für die Daten abgelaufen ist. Die jeweiligen Metadaten werden dann aus der Index-Datenbank entfernt und die abgelaufene Datenversion aus dem Speicher gelöscht. Das Löschen von E-Mails kann für ein Unternehmen negative Folgen haben. Durch Festlegen der passenden MS Exchange E-Mail-Richtlinien wird die E-Mail-Korrespondenz eines Unternehmens sicher archiviert. Die gingcom-Appliance erfasst Nachrichten aus Microsoft Exchange über eine so genannte Journaling-Mailbox und speichert diese sicher und langfristig, entsprechend den festgelegten Richtlinien. Durch die Konfiguration von Aufbewahrungsrichtlinien wird die gesamte E-Mail-Korrespondenz der angegebenen Anwendergruppen automatisch gespeichert. Über die Such-Funktion steht sie dann bei Bedarf autorisierten Anwendern oder zu Prüfzwecken zur Verfügung.

Als Wert für die Rechtssicherheit ergeben sich die Definition der Aufbewahrungsfristen.

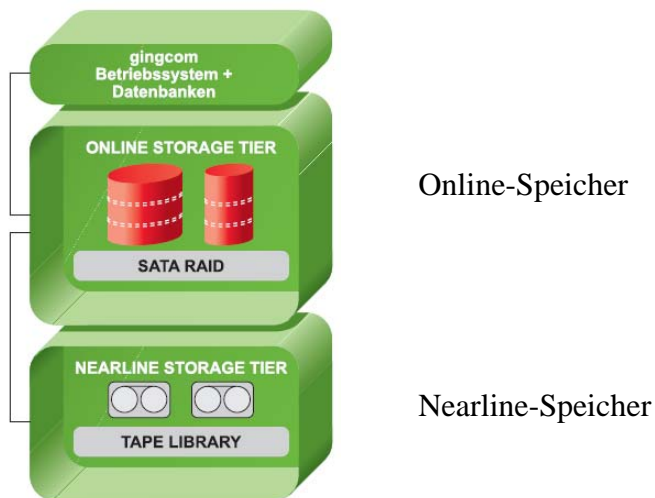
### 1.1.8 Datenintegrität durch Unveränderbarkeit

Mit einer Funktionalität, die für eine Unveränderbarkeit der Daten auf allen Speichermedien sorgt, stellt die gingcom-Appliance die Integrität der Daten sicher. Manipulationen an Daten im Archiv werden zuverlässig verhindert. Sucht zum Beispiel ein Anwender nach einer bestimmten E-Mail Nachricht und ruft er diese ab, bleibt die originale E-Mail-Version im Archiv unverändert bestehen. Die abgerufene E-Mail Nachricht wird als eine neue Datei entsprechend der jeweiligen Aufbewahrungsrichtlinien mit einem neuen Hash-Schlüssel gespeichert und kann so zuverlässig vom Original unterschieden werden. Dieser Vorgang stellt sicher, dass Dateien in der gingcom Appliance im Nachhinein nicht mehr verändert werden können. Jede Änderung eines Files, die in der gingcom Appliance gespeichert ist, zieht unweigerlich eine erneute Hash-Schlüssel Berechnung nach sich, was zur Folge hat, dass genau dieses File erneut als geänderte Version in gingcom abgelegt wird. Somit ist eine Manipulation von bereits gespeicherten Dateien nahezu ausgeschlossen. Auch die Mitglieder der Administratorengruppe sind nicht in der Lage bereits gespeicherte Dateien zu verändern.



### 1.1.9 Online- und Nearline Speicher

Der Aufbau des gingcom Systems gliedert sich in Online- und Nearline Speicher:



Der Nearline-Speicher enthält immer zwei unabhängige Kopien der gleichen Datenversion in getrennten Medienpools. Das bedeutet, dass jede Datei die im gingcom System abgelegt wird, mindestens zwei voneinander unabhängige Kopien hat, um die Datensicherheit zu erhöhen. Um Datenverlust zu verhindern und einen ununterbrochenen Betrieb des Unternehmens zu gewährleisten, wird in gingcom dieses strikte Datenredundanzkonzept verfolgt. Die Nearline-Speicherung setzt doppelte Archivdatenpools auf stets zwei unterschiedlichen Bändern ein, um sicherzustellen, dass Daten ständig verfügbar gehalten werden.

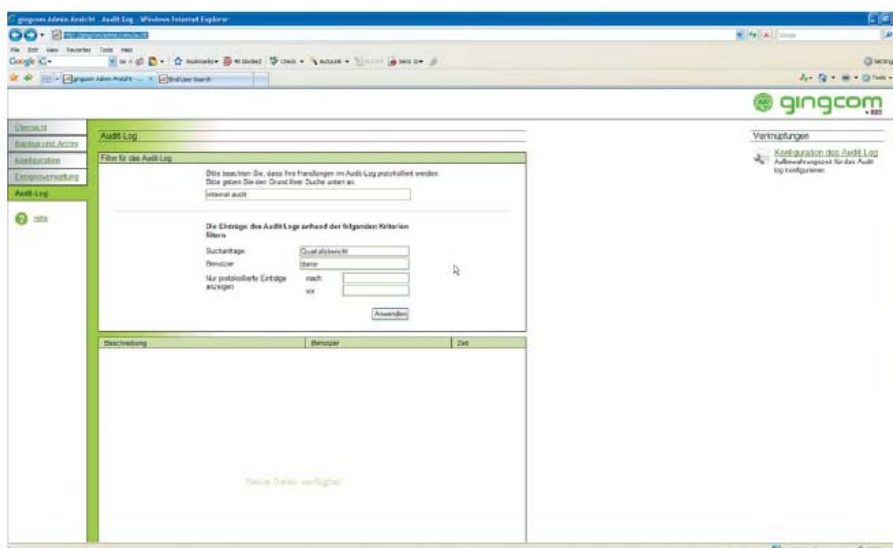
Im Online-Speicher werden alle Daten auf RAID-Datenträgern aufbewahrt und sind so vor einem Festplattenausfall geschützt. Der Schutz der integrierten NAS-Speicherlösung beruht ebenfalls auf RAID-5-Technologie mit sofortigem Ersatz (Hot Spare). Während eines Backup-Vorgangs werden die Daten zuerst in den Online-Speicher auf der Festplatte gesichert. Die zweite Sicherungskopie wird dann im ersten Datenpool im Nearline Speicher für eine zusätzliche Redundanz angefertigt. Dann wird die dritte Sicherungskopie auf den zweiten Datenpool gespeichert. Dieser zweite Datenpool ist ein Duplikat des ersten Datenpools. Erst wenn beide Datenpools ein geschütztes Objekt aufweisen, kann dieses Objekt aus dem Online-Speicher gelöscht werden, sollte mehr Festplattenplatz benötigt werden. Diese mehrstufige Schutzstrategie steigert merklich die Zuverlässigkeit und Sicherheit der gespeicherten Daten.

Als Wert für die Rechtssicherheit ergibt sich Datenintegrität.

### 1.1.10 Such-, Abrufvorgänge und Audit Log: Protokollierung der Zugriffe

Für den Abruf geschützter Dokumente und E-Mails aus dem Speicher steht die gingcom-Such-Funktion zur Verfügung, die jeder autorisierte Endanwender nutzen kann. Das bedeutet, dass jeder Anwender nach seinen eigenen E-Mails und Dateien suchen und diese dann abrufen kann. Allerdings hat der Administrator einen privilegierten Zugriff auf alle Daten im gingcom Speicher. Durch besondere Protokolldateien wird auch die Zugriffsüberwachung während der Such- und Abruf-Vorgänge eingehalten. Da auf archivierte E-Mails und Dateien nur per Suchabfrage zugegriffen werden kann, werden alle diese Aktivitäten protokolliert. Das Audit Log sorgt für eine Protokollierung der Zugriffe auf aufbewahrte Daten. Einmal aktiviert, kann das Audit Log nicht mehr deaktiviert werden. Jede Such- und Abrufaktion des Administrators bzw. von Mitgliedern der Auditors Group für archivierte Datenobjekte (Backup-Daten sind ausgeschlossen), wird ebenso wie jeder Zugriff auf das Audit Log protokolliert. Dies bedeutet, dass über das Audit Log alle Aktivitäten verfolgt werden. Das Audit Log registriert neben dem Titel der Suchabfrage die folgenden Informationen: Die Ergebnisliste der Objekt-Metadaten und den Zweck der Administratorsuche mit Zeitstempel und Anwenderkennung. Nur der Administrator und die Mitglieder der Auditors User Group können auf das Audit Log zugreifen.

Die folgende Abbildung zeigt das Audit Log als Teil der Benutzeroberfläche. Hier ist auch der Grund für den Zugriff auf das Audit Log anzugeben.



Als Wert für die Rechtssicherheit ergibt sich die Protokollierung des Zugriffs.

### **1.1.11 Zusammenfassung: Wert für die Rechtssicherheit**

Als Wert für die Rechtssicherheit ergeben sich entsprechend den Ziffern 1.1.1 bis 1.1.10

- Datenintegrität durch File und E-Mail Archivierung (1.1.1).
- Datenintegrität durch NAS & HSM (1.1.2).
- Datenintegrität durch Selbstüberwachung (1.1.3).
- Datenintegrität durch Notebook Protection (1.1.4).
- Wiedergabe durch Enterprise Search (1.1.5).
- Wiedergabe und Datenintegrität durch CAS und Single Instancing (1.1.6).
- Die Definition der Aufbewahrungszeiten für die Archivdaten (1.1.7).
- Datenintegrität durch Unveränderbarkeit (1.1.8).
- Datenintegrität durch Online- und Nearlinespeicher (1.1.9).
- Such- und Abrufvorgänge und Audit Log (1.1.10).

## **1.2 Near Continuous Data Protection (NCDP)**

### **1.2.1 NCDP – Datensicherung**

Die NCDP-Datensicherung (nahezu fortlaufende Datensicherung, Near Continuous Data Protection) überwindet die Beschränkungen der traditionellen Datensicherungstechnik, bei der Sicherung und Wiederherstellungen zu festgelegten Zeitpunkten erfolgen. Die fortlaufende Datensicherung (CDP, Continuous Data Protection) – auch fortlaufendes Backup genannt – beinhaltet normalerweise das sofortige automatische Kopieren und Speichern bei jeder Änderung an den Daten. gingcom verwendet NCDP, das auf dem gleichen Prinzip wie CDP beruht. Der Vorteil von NCDP besteht darin, dass kontinuierlich Datenänderungen überwacht werden und die erfassten Daten dann zu festgelegten Zeitpunkten – den Wiederherstellungszeitpunkten (Recovery Point Objective, RPO) – gesichert werden. NCDP stellt somit eine bedeutend geringere Systembelastung dar, weil alle in einem vorab definierten Zeitraum erfolgenden Änderungen zusammengefasst werden und die Datensicherung dann in einem einzelnen Vorgang durchgeführt wird.

Als Wert für die Rechtssicherheit ergeben sich Datenintegrität.

### **1.2.2 RPO – Liste**

NCDP verfolgt sämtliche Änderungen der Dateien innerhalb des Zeitraumes, festgelegt durch

den Parameter Wiederherstellungszeitpunkt– Vorgabe (RPO), und legt diese veränderten Dateien temporär in einer so genannten RPO Liste ab. Weiterhin wird ein erstes vollständiges Backup immer kurz nach der erfolgten Neuinstallation von gingcom in der Netzwerkdomäne gestartet. Ab diesem Zeitpunkt wird jede veränderte oder neu hinzugefügte Datei in die RPO Liste aufgenommen. Die in dieser Liste festgelegten Dateien werden dann innerhalb des Zeitraums durch gingcom gesichert, der durch den RPO-Wert festgelegt ist. Die RPO-Liste stellt sozusagen eine Datensicherungswarteschlange für alle neuen oder veränderten Dateien dar. Eine Datei wird sofort nach ihrer Änderung in die RPO-Liste aufgenommen. Dies setzt dann auch den RPO-Zähler für die Backup-Session in Gang. Sobald die RPO-Liste voll oder der RPO Zeitraum abgelaufen ist, werden die Daten gesichert. Als eine zusätzliche Schutzmethode für Daten nutzt gingcom noch ein Dateisicherungsverfahren, bei dem das gesamte Dateisystem-Verzeichnis durchlaufen wird (file system tree walk). Bei diesem Dateisystem-Verzeichnisdurchlauf wird das Dateisystem nach neuen oder veränderten Dateien durchsucht. Dabei wird ein Zeitplan beachtet, der in den Datensicherungsrichtlinien festgelegt wird. Werden neue oder veränderte Dateien gefunden, erfolgt eine sofortige Sicherung, nachdem der Verzeichnisbaum durchlaufen wurde. Der NCDP-Prozess überwacht kontinuierlich alle Dateiänderungen entsprechend der RPO-Vorgaben und stellt sicher, dass keine Änderung unbemerkt bleibt. Wiederhergestellte Daten sind deshalb mit exakt dem letzten Stand der verlorenen oder gelöschten Originaldaten verfügbar.

Als Wert für die Rechtssicherheit ergibt sich Datenintegrität.

### **1.2.3 Zusammenfassung: Wert für die Rechtssicherheit**

Durch NCDP Datensicherung (1.2.1) und RPO – Liste (1.2.2) entsteht Datenintegrität.

## **1.3 Dokumentation des gingcom Systems**

Die gingcom Appliance wird mit einer Reihe von Dokumentationen ausgeliefert. Schon im Vorfeld des eigentlichen Bezugs einer gingcom Appliance, ist der gingcom Concepts Guide in deutscher und englischer Sprache erhältlich. Der Concepts Guide liefert auf über 100 Seiten technisch detaillierte Informationen über die in gingcom angewendeten Verfahren und Methoden. Beschreibungen zu den einzelnen Modulen und deren Funktionalität sind ebenso vorhanden wie ausführliches und anschauliches Bildmaterial. Bei der Auslieferung ebenfalls enthalten ist ein Quick-Install Manual sowie der Administrators Guide.

## 1.4 Zusammenfassung

Im Ergebnis werden durch das gingcom-System die Datenintegrität gesichert, die Wiedergabe der archivierten Dokumente ermöglicht, die Aufbewahrungsfristen für die Archivdaten gewahrt und die Zugriffsrechte durch die Berechtigten ausgeübt.

Datenintegrität entsteht

- durch File und E-Mail Archivierung (1.1.1)
- durch NAS & HSM (1.1.2)
- durch Selbstüberwachung (1.1.3)
- durch Notebook Protection (1.1.4)
- durch CAS und Single Instancing (1.1.6)
- durch Unveränderbarkeit (1.1.8)
- durch NCDP Datensicherung (1.2.1) und
- die RPO – Liste (1.2.2).

Die Wiedergabe der archivierten Dokumente wird gesichert

- durch Enterprise Search (1.1.5) und
- durch CAS und Single Instancing (1.1.6).

Für die Aufbewahrungsfristen der Archivdaten wird der richtige Wert bestimmt (1.1.7).

Zugriffsrechte werden durch Such-, Abrufvorgänge und Protokollierung des Zugriffs durch Audit Log (1.1.10) gesichert.

Die Dokumentation des gingcom Systems besteht aus:

- Concepts Guide
- Quick Install Guide
- Administrators Guide (1.3)

## **2.0 Rechtliche Bewertung**

Das gingcom System wird hinsichtlich der rechtlichen Anforderungen an die ordnungsmäßige Archivierung (2.1), an den Vertragsabschluss durch elektronische Kommunikation (2.2) und an die Beweisqualität elektronischer Dokumente (2.3) untersucht.

### **2.1 Rechtliche Anforderungen an die ordnungsmäßige elektronische Archivierung**

Handelsbriefe und Buchungsbelege sind nach den Anforderungen des Handelsgesetzbuches (§ 257 Abs. 3 HGB) und der Abgabenordnung (§ 147 Abs. 2 AO) entsprechend den Grundsätzen ordnungsmäßiger Buchführung aufzubewahren. Diese Anforderung an die elektronische Archivierung hat das Bundesfinanzministerium mit den „Grundsätzen ordnungsmäßiger DV-gestützter Buchführungssysteme“ (2.1.1) und den „Grundsätzen zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen“ (2.1.2) konkretisiert. Die ordnungsmäßige Archivierung hat durch Basel II und den US - Sarbanes Oxley Act eine internationale Dimension erreicht (2.1.3). gingcom bietet Funktionalitäten, durch die Konformität mit den rechtlichen Anforderungen, auch Compliance genannt, hergestellt werden kann (2.1.4).

#### **2.1.1 Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme**

Allgemeingültige Regeln für die ordnungsmäßige Archivierung elektronischer Dokumente hat das Bundesfinanzministerium mit Schreiben vom 7.11.1995 “Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme” (GoBS)<sup>1</sup> formuliert. Für die ordnungsmäßige Archivierung kommt es auf den Einsatz ordnungsmäßiger Speichersysteme, die ordnungsmäßige Wiedergabe der Dokumente während der gesetzlichen Aufbewahrungsfrist und die ordnungsmäßige Verfahrensdokumentation an.

#### **- Ordnungsmäßige Speichersysteme**

Die Aufbewahrung von Unterlagen ist ordnungsmäßig, wenn die gesicherte Aufbewahrung gewährleistet ist und für die Dauer der Aufbewahrung die Informationen auf dem Speichermedium jederzeit abrufbar erhalten bleiben. Die Ordnungsmäßigkeit ist nicht von einem bestimmten Speichermedium abhängig. Zulässig und damit ordnungsmäßig im Sinne der handelsrechtlichen und steuerrechtlichen Aufbewahrungsvorschriften sind alle Speichermedien. Entscheidend für die Ordnungsmäßigkeit sind die hardwaremäßigen, softwaremäßigen und organisatorischen Sicherheitsfunktionen, die für das jeweilige

---

<sup>1</sup> BStBl. 1995 I, S. 738.

Speichermedium gesondert ausgeprägt sein können.<sup>2</sup> Entscheidend ist, dass durch ein Speichersystem die Daten vor Veränderungen geschützt werden und damit Datenintegrität entsteht.

gingcom bietet für die Datenintegrität ein vielfältiges System: durch File- und E-Mail Archivierung (1.1.1), durch NAS und HSM (1.1.2), durch Selbstüberwachung (1.1.3), durch Notebook Protection (1.1.4), durch CAS und Single Instancing (1.1.6), durch Unveränderbarkeit (1.1.8), durch NCDP (1.2.1), durch die RPO-Liste (1.2.2).

gingcom schützt mit der nahezu fortlaufenden Datensicherungstechnologie NCDP vor Datenänderungen.<sup>3</sup> Durch NCDP<sup>4</sup> werden die kontinuierlichen Datenänderungen überwacht und die erfassten Daten zu festgelegten Wiederherstellungszeitpunkten (Recovery Point Objectiv - RPO) gesichert.<sup>5</sup> Dieses System wird durch ein Datensicherungsverfahren ergänzt, bei dem das gesamte Dateisystem-Verzeichnis durchlaufen wird. Dieses „file system tree walk“ durchsucht das Dateisystem nach neuen oder veränderten Dokumenten, um sie zu sichern.<sup>6</sup> Durch NAS (Network Attached Storage) werden Massenspeichereinheiten (Filesharing) an ein lokales Netzwerk angeschlossen und die Dateisysteme ständig auf Änderungen geprüft. Die Daten, die sich in der NAS – Speicherlösung befinden, werden durch die HSM - Funktion (Hierarchical Storage Management) verwaltet. HSM überträgt die Daten zwischen Festplatte und Archivbändern. Sobald der Festplattenplatz eine „High Watermark“ überschreitet, verlagert das HSM die Daten aus dem NAS. Das Verlagern wird eingestellt, sobald die „Low Watermark“ erreicht ist.<sup>7</sup> Die Funktion der Selbstüberwachung prüft die Datenbankkonsistenz und Datenredundanz, prüft Fehler und meldet Störungen.<sup>8</sup> Auf Notebooks werden Unternehmensdaten durch Dateisystemagenten geschützt. Damit werden die Richtlinienereinstellungen für Datenschutz und Datenaufbewahrung zentral vom gingcom Administrator verwaltet.<sup>9</sup> Die Unveränderbarkeits – Funktionalität stellt sicher, dass jede Kopie oder Änderung eines Files eine erneute Hash – Schlüssel Berechnung nach sich zieht und damit dieses File als geänderte Version archiviert wird.<sup>10</sup> Der Aufbau des gingcom – Systems in die Bestandteile Nearline – Speicher und Online – Speicher ist ein weiterer Faktor

---

<sup>2</sup> GoBS VIII. b).

<sup>3</sup> hierzu Ziffer 1.1.1 File und E-Mail Archivierung.

<sup>4</sup> hierzu Ziffer 1.2.1 NCDP Datensicherung.

<sup>5</sup> Hierzu Ziffer 1.2.2 RPO – Liste.

<sup>6</sup> Hierzu Ziffer 1.2.2 RPO – Liste.

<sup>7</sup> Hierzu Ziffer 1.1.2 NAS & HSM.

<sup>8</sup> Hierzu Ziffer 1.1.3 Selbstüberwachung.

<sup>9</sup> Hierzu Ziffer 1.1.4 Notebook Protection.

<sup>10</sup> Hierzu Ziffer 1.1.8 Datenintegrität durch Unveränderbarkeit.

für die Datensicherheit. Der Nearline – Speicher enthält zwei unabhängige Kopien der gleichen Dateiversion. Dieses Datenredundanzkonzept setzt zwei unterschiedliche Bänder ein, um sicherzustellen, dass Daten ständig verfügbar gehalten werden. Im Online – Speicher werden alle Daten auf RAID – Datenträgern aufbewahrt und sind so vor einem Festplattenausfall geschützt. Diese mehrstufige Schutzstrategie wird um regelmäßige Konsistenzprüfungen der internen Datenbanken und die Prüfung der Wiederherstellungsfähigkeit ergänzt.<sup>11</sup> Jeder geschützten Datenversion wird eine SHA-1-Hash-Funktion zugewiesen. Für jede Änderung der Datei wird ein neuer Hash-Schlüssel erzeugt. Damit wird Echtheit und Integrität gesichert und das Original und die Kopie zuverlässig unterschieden.<sup>12</sup>

#### - **Ordnungsmäßige Wiedergabe durch Indexierung**

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. Diese Frist für das Lesbarmachen ist analog zu § 238 Abs. 1 Satz 2 HGB nach den Verhältnissen des Einzelfalles zu bestimmen.<sup>13</sup> Die Wiedergabe erfordert, dass nur Berechtigte zugreifen können. Dies kann nur durch die Vergabe von Zugriffsrechten sichergestellt werden.

gingcom sichert die Wiedergabe der archivierten Dokumente durch Enterprise Search (1.1.5) und durch CAS in Verbindung mit Single Instancing (1.1.6). Such- und Abrufvorgänge werden entsprechend den vergebenen Zugriffsrechten ausgeführt und die Zugriffe durch Audit Log protokolliert (1.1.10).

Das gingcom – System bietet für Endanwender und Administrator eine standardmäßige Suche nach Schlüsselwörtern und eine erweiterte Suche nach Metadaten. Die durch eine Suchabfrage gefundenen Elemente werden in einer Ergebnisliste angezeigt. Zu jedem aufgeführten Dokument besteht ein Download – Link, mit dem das Dokument auf einem dem Anwender zugeordneten Download Bereich im Online – Speicher herunter geladen wird.<sup>14</sup> Vor der Datenübertragung berechnet CAS die benötigten Hash - Werte für das Single Instancing. Single Instancing ermöglicht durch Verweise auf die jeweils gespeicherten Kopien

<sup>11</sup> Hierzu Ziffer 1.1.8 Datenintegrität durch Unveränderbarkeit.

<sup>12</sup> Hierzu Ziffer 1.1.6 CAS und Single Instancing.

<sup>13</sup> Ebenroth/Bonjou/Joost/Wiedemann, HGB Komm, München 2001, § 257 Rdnr. 25.

<sup>14</sup> Hierzu Ziffer 1.1.5 Enterprise Search.

identischer Dateien eine Speicherverwaltung ohne Dateidoppelkopien. Durch diese Methode wird der vorhandene Speicherplatz optimal ausgenutzt und der Bandbreitenbedarf gesenkt.<sup>15</sup> Die gingcom – Suchfunktion ermöglicht es, jedem autorisierten Nutzer nach eigenen E-Mails und Dateien zu suchen und diese abzurufen. Durch Protokolldateien werden die Zugriffe während der Such- und Abrufvorgänge überwacht.<sup>16</sup> Jeder Zugriff auf archivierte Daten wird durch das Audit Log registriert. Das Audit Log registriert den Titel der Suchabfrage, die Ergebnisliste der Objekt – Metadaten und den Zweck der Administratorsuche mit Zeitstempel und Anwenderkennung.<sup>17</sup>

#### - **Aufbewahrungsfristen**

Die Aufbewahrungsfrist beträgt für empfangene Handelsbriefe und die Kopien versendeter Handelsbriefe 6 Jahre und für Buchungsbelege 10 Jahre (§ 257 Abs. 4 HGB). Die Aufbewahrungsfrist für Dokumente, deren Inhalt der vertraglichen oder deliktsrechtlichen Verjährung unterliegen, müssen über einen Zeitraum von mindestens 30 Jahren archiviert werden. Während dieses Zeitraums muss der Zugriff auf das Dokument möglich sein.

gingcom ermöglicht es, die Aufbewahrungsfristen der Archivdaten zu definieren. Mit den Archivrichtlinien wird entsprechend den Unternehmensanforderungen und den gesetzlichen Vorschriften die Aufbewahrungszeit der Archivdaten bestimmt (ART). Entsprechend diesen Richtlinien erfasst gingcom die Nachrichten aus Microsoft Exchange über eine Journaling Mailbox. Hierdurch wird die gesamte E-Mail-Korrespondenz der angegebenen Anwendergruppen automatisch gespeichert. Während der vorgegebenen Aufbewahrungsfrist steht sie dann über die Suchfunktion autorisierten Anwendern und zu Prüfzwecken zur Verfügung.<sup>18</sup>

#### - **Ordnungsmäßige Verfahrensdokumentation**

Die Anforderungen an die Verfahrensdokumentation sind in den „Grundsätzen ordnungsmäßiger DV-gestützter Buchführungssysteme“ (GoBS)<sup>19</sup> definiert worden. Nach Textziffer 6 müssen aus der Verfahrensdokumentation Inhalt, Aufbau und Ablauf des Verfahrens vollständig ersichtlich sein.<sup>20</sup>

---

<sup>15</sup> Hierzu Ziffer 1.1.6 CAS und Single Instancing.

<sup>16</sup> Hierzu Ziffer 1.1.10 Such- und Abrufvorgänge.

<sup>17</sup> Hierzu Ziffer 1.1.10 Audit Log: Protokollierung der Zugriffe.

<sup>18</sup> Hierzu Ziffer 1.1.7 Aufbewahrungszeit für Archivdaten.

<sup>19</sup> BStBl. I 1995, S. 738 ff.

<sup>20</sup> Hierzu Ziffer 1.3.

Die Dokumentation von gingcom - unter Ziffer 1.3 beschrieben - erfüllt diese Anforderungen durch eine umfassende und verständliche Beschreibung des Systems.

- **Ergebnis für gingcom**

Im Ergebnis bietet gingcom ordnungsmäßige Speichersysteme, ordnungsmäßige Wiedergabe durch Indexierung, ordnungsmäßige Verwaltung der Aufbewahrungsfristen und eine ordnungsmäßige Dokumentation.

### **2.1.2 Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen**

Ein originäres elektronisches Dokument muss nach den „Grundsätzen zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen“ (GDPdU)<sup>21</sup> für den Datenzugriff in elektronischer Form maschinell auswertbar vorgehalten werden.<sup>22</sup>

- **Datenzugriff**

Das Bundesfinanzministerium hat mit diesem Schreiben das Recht zum Zugriff auf originär digitale Unterlagen im Rahmen der Außenprüfung in Form des unmittelbaren Datenzugriffs, des mittelbaren Datenzugriffs und der Datenträgerüberlassung konkretisiert. Für den unmittelbaren Datenzugriff der Finanzbehörde muss der Steuerpflichtige nach Abschnitt I.2.a) GDPdU dem Prüfer die erforderlichen Hilfsmittel zur Verfügung stellen, damit er selbständig auf die Daten zugreifen kann. Für den mittelbaren Datenzugriff hat der Steuerpflichtige entsprechend den Angaben des Prüfers den Zugriff auf die Daten zu organisieren, Abschnitt I.2.b) GDPdU. Statt des unmittelbaren und mittelbaren Datenzugriffs kann die Finanzbehörde einen Datenträger verlangen, auf dessen Daten sie zugreifen kann.

- **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 III.1 Satz 2 GDPdU sind originär digitale Unterlagen die in das Datenverarbeitungssystem in elektronischer Form eingehenden Daten und die im Datenverarbeitungssystem erzeugten Daten; maschinell verwertbare Datenträger sind maschinell lesbare und auswertbare Datenträger. Wenn originär digitale Unterlagen auf

---

<sup>21</sup> BStBl 2001 I, S. 415.

<sup>22</sup> GDPdU Ziffer III Archivierung digitaler Unterlagen Nr. 1.

maschinell verwertbaren Datenträgern zu archivieren sind, dann dürfen sie nicht, so die Schlußfolgerung des Bundesfinanzministeriums, ausschließlich in ausgedruckter Form oder auf Mikrofilm aufbewahrt werden.<sup>23</sup>

- **Ergebnis für gingcom**

gingcom ermöglicht den Datenzugriff und die maschinelle Auswertbarkeit durch die ordnungsmäßige Wiedergabe, wie unter Ziffer 2.1.1 festgestellt. Im Ergebnis erfüllt gingcom damit die Anforderungen der GDPdU.

### 2.1.3 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.

- **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 und Aktionäre 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

---

<sup>23</sup> GDPdU III. Archivierung digitaler Unterlagen Ziffer 1.

Deutschland Unternehmen betroffen, die auf Grund der Inanspruchnahme des US-amerikanischen Kapitalmarktes an US-amerikanischen Börsen registriert sind und mit diesen gesellschaftsrechtlich verbundene Unternehmen. Dies zwingt dazu, rechtserhebliche Dokumente nach den Grundsätzen der Ordnungsmäßigkeit vollständig elektronisch zu archivieren.

#### - **Ergebnis für gingcom**

Die Anforderungen von Basel II und SOA entsprechen den Grundsätzen der Ordnungsmäßigkeit nach Handelsrecht und Steuerrecht, insoweit durch diese Vorschriften die vollständige und ordnungsmäßige Archivierung elektronischer Dokumente verlangt wird. Diese Anforderungen werden, wie unter Ziffer 2.1.1 und unter Ziffer 2.1.2 festgestellt, von gingcom erfüllt.

#### **2.1.4 Ergebnis für gingcom**

Die rechtlichen Anforderungen an die ordnungsmäßige Archivierung durch die GoBS (Ziffer 2.1.1) und die GDPdU (Ziffer 2.1.2) werden durch gingcom erfüllt. gingcom erfüllt auch die Anforderungen von Basel II und des Sarbanes Oxley Act insoweit durch diese Vorschriften die vollständige und ordnungsmäßige Archivierung elektronischer Dokumente verlangt wird (Ziffer 2.1.3).

### **2.2 Vertragsabschluss durch elektronische Kommunikation**

Rechtswirksames Handeln ist grundsätzlich formfrei. Eine elektronische Nachricht ist damit eine rechtswirksame Willenserklärung, mit der Rechte und Pflichten begründet werden.<sup>24</sup> Eine Sicherheitstechnik, wie elektronische Signaturen, ist für die formlose Erklärung nicht erforderlich. Für den Empfänger muss nur der Absender identifizierbar sein. gingcom ermöglicht damit die formfreie rechtswirksame elektronische Kommunikation.

### **2.3 Die Beweisqualität elektronischer Dokumente**

Die Beweisqualität elektronischer Dokumente wird im Rahmen der freien Beweiswürdigung durch die ordnungsmäßige Archivierung bestimmt (2.3.1). gingcom erfüllt die Anforderung der Ordnungsmäßigkeit und bietet damit Beweisqualität (2.3.2).

---

<sup>24</sup> Zur zivilrechtlichen Wirksamkeit elektronischer Erklärungen siehe die aktuelle Zusammenfassung von Mehrings, in Hoeren/Sieber (Hrsg.), Handbuch MultiMediarecht Teil 13.1 – Stand: 3. Ergänzungslieferung 2005

### 2.3.1 Freie Beweiswürdigung

Ein elektronisches Dokument ist nicht Urkunde, da es in materialisierter Form von dem Aussteller nicht unterzeichnet ist.<sup>25</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 durch Hinweise auf die Integrität und Authentizität des Dokuments bestimmt. Für die Beweisqualität elektronisch archivierter Dokumente spricht die Aufbewahrung nach den Grundsätzen der Ordnungsmäßigkeit. Mit der Aufbewahrung entsprechend diesen Grundsätzen soll die elektronische Dokumentation gegen Änderungen geschützt werden.<sup>26</sup> Deshalb gilt die ordnungsmäßige elektronische Archivierung entsprechend diesen Grundsätzen als Indiz für die Beweissicherheit.<sup>27</sup> Nach den GDPdU<sup>28</sup> hat der Steuerpflichtige für den Datenzugriff der Finanzbehörde auswertbare Daten bereitzuhalten. Hierzu sind Berechtigungskonzepte für die Finanzbehörde und die maschinelle Auswertbarkeit der Dokumente erforderlich. Nach den GoBS<sup>29</sup> wird die Integrität der elektronisch gespeicherten Dokumente für die Phase der Aufbewahrung und Wiedergabe sichergestellt. Diese Anforderungen der GDPdU und GoBS bilden ein Sicherheitskonzept, das die Beweisqualität des elektronisch archivierten Dokuments indiziert.

### 2.3.2 Die Beweisqualität von gingcom

gingcom sichert die Integrität der archivierten Dokumente, wie unter 2.1 „Rechtliche Anforderungen an die ordnungsmäßige elektronische Archivierung“ festgestellt, und bietet damit Beweissicherheit im Rahmen der freien Beweiswürdigung.

---

<sup>25</sup> Allgemeine Meinung: *Geis* in *Hoeren/Sieber*, Handbuch Multimediarecht, Teil 13.2 – Stand: 3. Ergänzungslieferung 2002; *Oertel*, MMR 2001, 419; *Zöller/Greger*, ZPO, 21. Aufl. 1999, § 371 Rdnr. 1; Begründung der Bundesregierung, BT-Drs. 14/4987, S. 23, 25.

<sup>26</sup> *Glanegger u.a./Kirnberger*, HGB-Komm, Heidelberg 2002, 6. Aufl., § 257 Rdnr. 3; *Münch Komm HGB/Ballwieser*, § 257 Rdnr. 16; *Heymann/Walz*, HGB-Komm, Berlin 1999, 2. Aufl., § 257 Rdnr. 6.

<sup>27</sup> *Ebenroth/Bonjou/Joost/Wiedemann*, HGB-Komm, München 2001, § 257 Rdnr. 1.

<sup>28</sup> Hierzu *Ziffer 2.2.2.*

<sup>29</sup> Hierzu *Ziffer 2.2.1.*

### **3.0 Ergebnis der rechtlichen Begutachtung und Zertifikat**

#### **3.1 Ordnungsmäßige Archivierung von Dokumenten**

gingcom erfüllt die Anforderungen an die ordnungsmäßige Archivierung durch die GoBS und die GDPdU. gingcom erfüllt auch die Anforderungen von Basel II und des Sarbanes Oxley Act insoweit durch diese Vorschriften die vollständige und ordnungsmäßige Archivierung elektronischer Dokumente verlangt wird (2.1).

#### **3.2 Rechtswirksamkeit elektronischer Erklärungen**

gingcom ermöglicht die rechtswirksame elektronische Kommunikation als formlose Erklärung (2.2).

#### **3.3 Beweissicherheit elektronischer Dokumente**

gingcom sichert die Beweisqualität elektronisch archivierter Dokumente im Rahmen der freien Beweiswürdigung (2.3).

#### **3.4 Zusammenfassung**

Zusammenfassend ist festzustellen, dass gingcom den rechtlichen Anforderungen in vollstem Umfang entspricht.

Hamburg, den 1. Juni 2007

  
Rechtsanwalt Dr. Ivo Geis

## Literaturverzeichnis

### Literatur

Ballwieser, in: Münchener Kommentar zum HGB, München 2001;

Ebenroth/Bonjou/Joost/Wiedemann, HGB Kommentar, München 2001;

*Geis* in *Hoeren/Sieber*, Handbuch Multimediarrecht, Teil 13.2 – Stand: 3. Ergänzungslieferung 2005;

Glanegger u.a./*Kirnberger*, HGB-Komm, Heidelberg 2002, 6. Aufl.;

Heymann/*Walz*, HGB-Kommentar, Berlin 1999, 2. Aufl.;

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

*Mehrings*, in *Hoeren/Sieber* (Hrsg.), Handbuch MultiMediarrecht Teil 13.1 – Stand: 3. Ergänzungslieferung 2005;

*Zöller/Greger*, Kommentar zur Zivilprozessordnung, 21. Aufl. 1999;

## **Glossar und Abkürzungen**

### **Active Directory**

Ein Windows-spezifischer Begriff. Der Dateiverzeichnisdienst für Windows-Server. Dieser Dienst speichert Information über Objekte im Netzwerk und stellt diese Information befugten Administratoren und Benutzern zur Verfügung. Active Directory gibt den Netzwerkbenutzern Zugang zu erlaubten Ressourcen im gesamten Netzwerk, wobei ein eigenes Anmeldeverfahren zum Einsatz kommt. Administratoren erhalten eine intuitive hierarchische Sicht des Netzwerkes und können von einer einzigen Stelle aus alle Netzwerkobjekte verwalten.

### **Administratorsuche**

Teil der Administrator-GUI. Der Administrator erhält einfach zu bedienende Funktionen, um gesicherte oder archivierte Dateisysteme und E-Mail-Objekte von MS Exchange zu finden. Siehe auch **Browsen**.

### **Administrator**

Eine Person, die dafür verantwortlich ist, die gingcom Appliance zu verwalten. Zu dem Verantwortungsbereich des gingcom Administrators gehören die Einstellung der gingcom Umgebung, die Konfigurationsrichtlinien, Überwachen des Gerätebetriebs, das Sichern und Wiederherstellen von Daten sowie das Update der gingcom Appliance.

### **Administrator-GUI**

Eine Web-basierende Benutzeroberfläche zur zentralen Verwaltung von gingcom, welche Zugriff auf alle gingcom Funktionen bietet. Hierzu werden Administratorzugriffsrechte benötigt.

### **Agent**

Ein gingcom Softwaremodul, mit dem Daten entsprechend dem jeweiligen Datentyp erfasst und wiederhergestellt werden können. Dieses Modul erfüllt die gingcom Datenschutzaufgaben auf einem Client, entsprechend der jeweiligen Richtlinienvorgaben. Bei jedem Client mit unterstütztem Dateisystem werden der Dateisystemagent und der Systemzustandsagent installiert, während bei dem MS Exchange-Server der MS Exchange-

Server-Agent und der MS Exchange-E-Mail-Agent installiert werden. Siehe auch **Dateisystemagent, MS Exchange E-Mail Agent, MS Exchange Server Agent** und **Systemzustandsagent**.

### **Agenten-Datenbank**

Eine der internen Datenbanken von gingcom, in der die historischen Daten aller geschützten Client-Objekte abgebildet sind. Dient auch als Referenz für die Liste geschützter Systeme, die im Abschnitt Deployment der GUI angezeigt werden.

### **AO**

Abgabenordnung

### **Archivierte Daten**

Entsprechend der Archivierungsrichtlinien gespeicherte Daten.

### **Archivierung**

Ein auf Richtlinien basierender Prozess, bei dem Daten entsprechend der vorgegebenen Parameter gespeichert und geschützt werden. Bei der Archivierung wird die Dauer der Aufbewahrung festgelegt. Integrität und Zugänglichkeit der Daten bei der Datensuche bleiben gewahrt.

### **Audit Log**

Sowohl die Administratorsuche als auch das Audit Log (Prüfprotokoll) werden aufgezeichnet. Das Audit Log stellt sicher, dass jeder Zugriff auf geschützte archivierte Daten protokolliert wird. Einträge im Audit Log werden archiviert und können nicht mehr geändert werden.

### **Aufbewahrungszeit für Archivdaten (ART)**

Ein Richtlinienparameter, der definiert, ob und wie lange das Objekt archiviert wird. Durch Angabe des ART-Wertes wird die Aufbewahrungszeit für archivierte Daten definiert. Der Aufbewahrungszeitraum ist die Zeit, in der die gingcom Appliance die Daten im Archiv speichert und zwecks Wiederherstellung durch die Suchfunktion bereithält. Nach Ablauf der ART kann auf das Objekt nicht mehr zugegriffen werden und es wird dann schließlich aus dem Archiv entfernt.

**Backup**

Das gingcom Backup beruht auf Richtlinien und läuft in zwei Phasen ab. Zunächst legt gingcom eine Sicherungskopie der Daten an und speichert diese im Online-Speicher.

Während der zweiten Phase werden zwei weitere Kopien der gleichen Daten angefertigt und auf zwei getrennten Magnetbändern im Nearline-Speicher abgespeichert.

**Berichte**

Siehe auch **Statusbericht**.

**BGB**

Bürgerliches Gesetzbuch

**Browsen**

gingcom gestattet dem Administrator das Durchsuchen des gesicherten Dateisystems durch Auswahl des geschützten Clients, für den die Daten wieder hergestellt werden müssen. Ferner kann der Zeitpunkt gewählt werden, für den der Dateiverzeichnisinhalt angezeigt wird sowie das wiederherzustellende Objekt gewählt werden. Ein Durchsuchen der Daten in einem Dateisystem ist nur solange möglich, wie der BRT noch nicht abgelaufen ist. Siehe auch **Administratorsuche**.

**BStBl.**

Bundessteuerblatt

**CAS-Datenbank**

Hier werden objektbezogene Informationen aufbewahrt. Darunter fallen bspw. der berechnete Hash-Schlüssel für das Datenobjekt, die Anzahl der Kopien und ihr Speicherplatz auf den Bandmedien, die Datensicherungszeit sowie die dazugehörige Aufbewahrungsrichtlinie. Die CAS-Datenbank wird laufend überwacht und automatisch verwaltet, gesichert und bei Bedarf zurückgespeichert.

**Client**

Ein System, bei dem mindestens ein gingcom-Agent installiert wurde und dem eine Richtlinie zum Schutz von Objekten zugewiesen wurde. Ein gingcom Client kann eine Workstation, ein

Server, ein Notebook mit Windows OS oder ein MS Exchange-Server sein. Siehe auch **gingcom-Umgebung**.

### **Compliance-Datenverwaltung**

Eine Gruppe von Funktionen, die sich auf Regeln zur gingcom Datenverwaltung beziehen. Es handelt sich dabei um Aufbewahrungsrichtlinien für Dokumente und E-Mails, schnelles Wiederauffinden und autorisierten Zugang zu aufbewahrten Daten, Wahrung der Datenintegrität durch Unveränderbarkeit und Hash-Prüfung sowie mehrstufige Speicherung und vollautomatisierte Speicherroutinen.

### **CAS (content addressable storage)**

gingcom bedient sich des CAS-Konzeptes und sichert somit eine Speicherung und Abruf aller Daten anhand deren Inhalte anstatt nach dem physischen Speicherplatz. Das CAS-Design ermöglicht eine Speicherung ohne Doppelkopien (Single Instance Storage) und ermöglicht eine schnelle Suche nach geschützten Daten. Siehe auch Single **Instance-Speicherung** und **Hash-Prüfung**.

### **Datenschutz**

Schutz für Dateisysteme, den Systemzustand sowie Microsoft Exchange Daten durch Erstellen von Richtlinien. gingcom bietet NCDP für den Schutz von Dateisystemdaten und geplanten Backups für den Systemzustand und MS Exchange-Daten.

### **Datenredundanz**

gingcom stellt sicher, dass stets mindestens zwei Kopien der Daten zur Verfügung stehen. Zuerst werden die Daten von einem Client in den Online-Speicher kopiert. Danach werden sie in den ersten Datenpool im Nearline-Speicher kopiert. Dieser enthält die Duplikate aller online gespeicherten Daten. Dann wird die zweite Bandkopie auf dem zweiten Datenpool angefertigt. Dieser zweite Datenpool ist ein Duplikat des ersten Datenpools.

### **Dateinamenerweiterungen ausschließen**

Dieser Parameter der Dateisystemrichtlinien ist eine Liste von Dateinamenerweiterungen, die bei der Datensicherung nicht berücksichtigt werden sollen.

### **Dateinamenerweiterungen für NCDP ausschließen**

Dieser Parameter der Dateisystemrichtlinien ist eine Liste von Dateinamenerweiterungen, die bei dem NCDP-Prozess nicht berücksichtigt werden sollen. Im Gegensatz zum Dateisystem-Verzeichnisdurchlauf, bei dem alle neuen oder geänderten Dateien ungeachtet ihrer Dateinamenerweiterungen gesichert werden, sichert das NCDP keine Dateien mit Dateinamenerweiterungen, die durch diesen Parameter angegeben wurden.

### **Dateisystemagent**

Ein gingcom Softwaremodul, welches auf jedem Client mit unterstütztem Dateisystem installiert wird. Während des Backups überträgt es Daten aus den geschützten Dateisystemen in den Online-Speicher gemäß der in den Dateisystemrichtlinien vorgegebenen Parameter (und umgekehrt bei der Rückspeicherung).

### **Dateisystemrichtlinien**

Eine Gruppe von Parametern, mit denen die Schutz- und Aufbewahrungsregeln für die Dateisystemdaten festgelegt werden. Zu den Parametern des Dateisystems zählen: RPO, Dateisystem-Verzeichnisdurchlauf, Verzeichnisse ausschließen, Dateinamenerweiterungen ausschließen, Dateinamenerweiterungen für NCDP, BRT und ART ausschließen.

### **Einsatz (Deployment)**

Der Prozess der Installation der gingcom Agenten auf den Systemen in der gingcom-Domain und die Zuweisung von Richtlinien zu diesen Systemen. Sobald bei dem System ein Agent eingesetzt worden ist und Richtlinien gelten, wird das System zu einem geschützten gingcom-Client.

### **Endanwender**

Ein Benutzer eines gingcom-Client-Systems. Ein Endanwender darf nach eigenen gesicherten und archivierten Daten suchen und diese Daten dann abrufen.

### **Endanwender-Benutzeroberfläche (GUI)**

Mithilfe der Benutzeroberfläche können Endanwender nach ihren gesicherten und archivierten Daten suchen.

### **Endanwendersuche**

Siehe auch **Endanwender-Benutzeroberfläche (GUI)**.

**Ereignisprotokoll**

In einem Ereignisprotokoll werden die gingcom Aktivitäten und der gingcom Status aufgezeichnet. Diese werden vom Ereignismanager erfasst und in der Ereignisverwaltung der GUI dargestellt. Alle verzeichneten Fehler- und Statusmeldungen dienen der Überwachung und der Leistungsstatistik. Das Ereignisprotokoll dient auch der Benachrichtigung des Administrators, wenn sein Eingreifen infolge eines Ereignisses benötigt wird. Siehe auch **Ereignisverwaltung**.

**Ereignisverwaltung**

Die Ereignisverwaltung in der GUI zeigt alle vom Ereignismanager erfassten Ereignisse an. Diese Ereignisse können dann durchgesehen bzw. bestätigt werden.

**Ereignismanager**

Ein Softwaremodul, welches Zustandsinformationen aus verschiedenen Hardware- und Softwarekomponenten erfasst und sie an das Ereignisprotokoll weitergibt.

**Ereignismeldung**

Konfigurierte Empfänger erhalten E-Mail-Meldungen über Ereignisse der Klasse Alarme, die vom Administrator das Ausführen einer Maßnahme erfordern.

**GDPdU**

Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen

**Geschütztes Objekt**

Ein Dateisystem, ein Microsoft Exchange-Server oder ein Systemzustand, dem gingcom-Richtlinien zugewiesen wurden.

**Gesicherte Daten**

Entsprechend der Datensicherungsrichtlinien gespeicherte Daten.

### **gingcom-Backup**

Eine regelmäßige Sicherung der internen Datenbanken und Konfigurationsdaten von gingcom. Als Ergebnis werden zwei Sicherungskopien im Nearline-Speicher erstellt, wo zwei Wiederherstellungsmedienpools für die gesicherten Daten zugeteilt sind. Mindestens eine bestätigte widerherstellbare Backupgruppe der gingcom-Daten steht damit immer zur Verfügung, um eine zuverlässige Wiederherstellung einer gingcom Appliance zu gewährleisten. Siehe auch **Wiederherstellung**.

### **gingcom-Umgebung**

Eine gingcom-Umgebung besteht aus dem gingcom-Server und seinen Clients. Dies können Workstations und Notebookcomputer mit Windows OS und Microsoft Exchange Servern sein. Eine gingcom-Umgebung wird zentral durch die Administrator-GUI verwaltet. Siehe auch **Client**.

### **GoBS**

Grundsätze ordnungsmäßiger DV-gestützter Speicherbuchführung

### **GUI**

Je nach dem Anwender-Typ stehen zwei unterschiedliche Bedieneroberflächen (GUI) zur Verfügung. Die Administrator-GUI bietet eine zentrale Bedienungsfläche für die gingcom-Appliance. Die Endanwender-GUI bietet Such und Abruffunktionen für geschützte Daten.

### **Hash-Prüfung**

gingcom verwendet SHA-1-Hash-Funktionen als Prüfsummen- und Verifizierungsalgorithmus für alle geschützten Daten, jeweils vor und nach der Speicherung in der mehrstufigen Speicherungsstruktur von gingcom. Jeder geschützten Datenversion wird ein eindeutiger Hash-Schlüssel zugewiesen, der damit Echtheit und Integrität sichert. Hash-Funktionen sorgen für Single Instancing und schnelles Abrufen geschützter Daten. Siehe auch **Single Instance-Speicherung**.

### **HGB**

Handelsgesetzbuch

### **Hierarchisches Speicher Management (HSM)**

HSM verwaltet Daten im NAS-Dateibereich durch vollautomatisierte Übertragung von Daten zum bzw. vom Online-Speicher in das Archiv (und umgekehrt), also zwischen den Festplattendatenträgern und den Archivbändern. HSM überwacht ständig die Festplattennutzung und gibt aus dem NAS Daten gemäß einer so genannten „Watermark“ frei. Siehe auch **NAS-Dateibereich**, **High Watermark** und **Low Watermark**.

### **High Watermark**

Ein HSM-Richtlinienparameter, der den oberen Wert für die Festplattennutzung im NAS-Dateibereich festlegt. Wird dieser Wert erreicht, beginnt das HSM mit der Freigabe von Daten, die bereits in gingcom über einen Backup verfügen. Siehe auch **Low Watermark** und **Watermark**.

### **Inkrementeller Backup**

Dieser Parameter der MS Exchange-Server-Richtlinien legt den Zeitraum zwischen zwei aufeinander folgende inkrementelle Backups von MS Exchange fest. Während eines inkrementellen Backups für Microsoft Exchange werden nur die Transaktionsprotokolldateien gesichert, die seit der letzten vollständigen bzw. inkrementellen Datensicherung neu erzeugt wurden. Protokolldateien, die älter als der aktuelle Prüfpunkt sind, werden nach Abschluss des inkrementellen Backups gelöscht. Siehe auch **Vollständiges Backup**.

### **Indexer**

Ein Dienst, der Informationen aus gesicherten Daten extrahiert und diese in der Indexer-Datenbank abspeichert. Indexing-Informationen für Dokumente und E-Mails enthalten Daten wie Dateiname, Worte aus dem Textkörper, den Dateieigentümer und das Datum, womit eine Volltextsuche von Dokumenten ermöglicht wird. Für binäre Dateien wird nur der Dateiname indiziert.

### **Indexer-Datenbank**

Diese Datenbank speichert inhaltsbezogene Informationen zu allen indizierbaren, gesicherten und archivierten Objekten und gestattet so eine Volltextsuche. Für archivierte Objekte, deren Inhalte nicht indiziert werden können, speichert sie auch Metadaten ab, etwa Dateiname, Archivzeit, Zugriffsberechtigungsinformationen und Dateigröße.

## **Installation**

Siehe auch **Einsatz**.

## **Konfigurationsdaten**

Diese Daten werden für den einwandfreien Betrieb von gingcom benötigt. Dabei handelt es sich um die folgenden Informationen: Festplattenverbundpartitionierung, Netzwerkkonfiguration, Domain-Zugehörigkeit, eine Liste geschützter Systeme und deren Richtlinien, Lizenzdetails und Anwenderkonfiguration. Die gingcom-Konfiguration ist Teil der gingcom-Datensicherung und dient einer Wiederherstellung von gingcom.

## **Konsistenzprüfung**

Eine der Funktionen von gingcom für die Selbstverwaltung. Die Konsistenz der CAS-Datenbank wird regelmäßig mithilfe eines automatischen Prozesses überprüft. Bei diesem Prozess werden die Inhalte der CAS-Datenbank mit den im Online- und Nearline-Speicher gespeicherten Daten verglichen. Alle gefunden Widersprüche werden im Ereignisprotokoll eingetragen und der Administrator wird benachrichtigt. Es wird automatisch eine Maßnahme zur Reparatur der jeweiligen Datenbank eingeleitet. Siehe auch **Wiederherstellungsprüfung** und **Selbstverwaltung**.

## **Low Watermark**

Ein HSM-Richtlinienparameter, der den unteren Wert für die Festplattennutzung im NAS-Dateibereich festlegt. HSM stellt die Freigabe von Dateien ein, sobald die Low Watermark erreicht ist. Siehe auch **High Watermark** und **Watermark**.

## **Medien- und Geräte-Datenbank**

Diese Datenbank enthält alle Informationen zu den verwendeten Medien und Geräten, einschließlich aller relevanten Ressourceninformationen wie bspw. Konfigurationsparameter, Ressourcenmerkmale, gegenwärtiger Status, Gebrauchsstatistiken sowie Beziehungen zu anderen Ressourcen.

## **Medienkonsolidierung**

Bei diesem Vorgang werden Daten mit noch gültiger Aufbewahrungszeit automatisch von Medien, auf denen die Aufbewahrungszeit von mehr als 40 % der Daten abgelaufen ist, auf

ein anderes Bandmedium verlagert. Das Medium, von dem aus die Daten mit einer noch gültigen Aufbewahrungszeit umgespeichert wurden, wird dann neu formatiert und kann weiterverwendet werden.

### **Medien-Pool**

Alle Medien, die dem Schutz von Anwenderdaten und gingcom-Appliance-Daten dienen, werden entsprechend ihrem Gebrauchsmuster in sechs Medienpools verteilt. Zwei Datenpools enthalten unabhängige Duplikate aller Anwenderdaten, die schon im Online-Speicher vorhanden sind. Zwei Wiederherstellungs-Medienpools enthalten stets mindestens eine gültige widerherstellbare Backup-Gruppe der gingcom Appliance Daten. Der Ersatzmedienpool enthält Medien, die als Ersatz für korrupte Medien benutzt werden, während der unbenutzte Medienpool weitere Medien für andere Medienpools bereithält, wenn ein neues Medium benötigt wird.

### **Mehrstufige Speicherung**

Das gingcom-Datenspeicherungssystem beruht auf zwei Speicherungsarten: Festplattenbasierte Online-Speicher stellen dabei die erste Stufe dar. Diese Stufe teilt sich auf in Hochleistungs-SAS- und Hochkapazitäts-SATA-Datenträger. Die zweite Stufe ist ein Nearline-Speicher, eine Bandbibliothek mit großer Kapazität u.a. für Langzeitarchivierung.

### **Microsoft Exchange E-Mail-Agent**

Ein auf einem Microsoft Exchange-Server installiertes gingcom Softwaremodul. Durch den E-Mail-Agenten werden E-Mail-Nachrichten, die von der MS Exchange-Journaling-Mailbox erfasst wurden abgespeichert. Dabei werden die Parameter beachtet, die in den MS Exchange-E-Mail-Richtlinien erstellt wurden. Geschützte Nachrichten können mithilfe der gingcom Suchfunktion (Search) gefunden und abgerufen werden.

### **MMR**

MultiMedia und Recht (Zeitschrift)

### **MS Exchange-E-Mail-Richtlinien**

Eine Gruppe von Parametern, welche die Backuphäufigkeit für E-Mails festlegen, die von der entsprechend konfigurierten Journaling-Mailbox erfasst wurden (dies ist ein Parameter für die

vollständige Datensicherung). Die Parameter legen auch die Aufbewahrungszeit für archivierte E-Mails (den ART-Parameter) fest.

### **MS Exchange-Server-Agent**

Ein auf einem Microsoft Exchange-Server installiertes gingcom Softwaremodul. Dieses Softwaremodul wird für die Sicherung von MS Exchange-Daten im Online-Speicher verwendet. Dabei werden die Parameter beachtet, die in den MS Exchange-Server-Richtlinien erstellt wurden.

### **MS Exchange-Server-Richtlinien**

Eine Gruppe von Parametern - im Einzelnen: (1) Der Parameter für einen vollständigen Backup, (2) die Häufigkeit des inkrementellen Backups (Parameter für inkrementellen Backup) für Microsoft Exchange-Datenspeicher, (3) einen Zeitraum, für den die gesicherten Daten zwecks Wiederherstellung aufbewahrt werden (der BRT-Parameter).

### **NAS-Dateibereich**

Dieser Bereich befindet sich im SATA-Festplattenverbund unter dem Namen gingcom NAS und bietet allen autorisierten Netzanwendern zusätzlichen Speicherplatz, um ihre Daten abzuspeichern. Die Daten im NAS werden durch den HSM verwaltet. Siehe auch **Hierarchisches Speicher Management (HSM)**.

### **Nahezu fortlaufende Datensicherung (NCDP)**

Der Prozess der laufenden Verfolgung und Sicherung aller Änderungen auf dem Dateisystem gemäß der RPO Parameter. Durch NCDP können verschiedene Dateiversionen wiederhergestellt werden. Siehe auch **RPO** und **Versionierung**.

### **Nearline-Speicher**

Ein Teil der mehrstufigen Speicherung von gingcom, dies ist die zweite Speicherstufe. Der Nearline-Speicher ist eine Bandbibliothek für die Speicherung von Backup- und Archivkopien von Datenversionen, die bereits im Online-Speicher vorhanden sind. Der

Nearline-Speicher enthält stets zwei unabhängige Kopien der gleichen Datenversion in getrennten Medienpools.

### **Online-Speicher**

Ein Teil der mehrstufigen Speicherung von gingcom, dies ist die erste Speicherstufe. Der Online-Speicher besteht aus einem SAS-RAID-Festplattenverbund mit hoher Leistung und einem SATA-RAID-Festplattenverbund mit hoher Kapazität. Der Online-Speicher ist ein Aufbewahrungsort für geschützte Daten und dient auch als NAS-Dateibereich.

### **Point-in-Time Restore**

Ein Prozess der Wiederherstellung von Daten in einem bestimmten Zustand, der zu einem angegebenen Datum und Zeit vorhanden war. Siehe auch **Versionierung**.

### **Recovery Storage Group**

Ein spezifischer Begriff für MS Exchange Server. Es handelt sich hierbei um ein Merkmal, wodurch eine zweite Kopie einer Exchange Mailbox-Datenbank auf dem gleichen Server wie die ursprüngliche Datenbank oder auf einem anderen Exchange-Server der gleichen Gruppe angefertigt werden kann. Dies kann auch bei laufendem Betrieb der ursprünglichen Datenbank und Anschluss an Clients erfolgen. Diese Möglichkeit erlaubt die Wiederherstellung von Daten aus einer älteren Sicherungskopie der Datenbank, ohne den Anwenderzugriff auf aktuelle Daten zu behindern.

### **Richtlinien**

Eine Gruppe von Parametern, mit denen die Schutz- und Aufbewahrungsregeln gemäß dem Objekt festgelegt werden. Jeder Objekttyp benötigt seine eigenen Richtlinien. Es gibt daher Richtlinien für Dateisysteme, MS Exchange- Server, MS Exchange-E-Mail sowie den Systemzustand. gingcom stellt vorab festgelegte Richtlinien für alle Objekttypen zur Verfügung und erlaubt dem Administrator, aufgabenspezifische Richtlinien einzurichten und diese unter Konfiguration in der GUI zu verwalten.

### **RAID5-Level**

Festplattentechnologie für gingcom-Online-Speicher, verfügt über eine Ersatzfestplatte (Hot Spare). RAID 5 Level steht für Hochleistung und Fehlertoleranz und sorgt für einen Schutz gegen einen Festplattenausfall im Verbund. Fällt eine Festplatte aus, steht automatisch ein

Ersatz für die Rekonstruktion von Daten der fehlerhaften Festplatte bereit. Die gingcom Appliance kann somit ohne Datenverlust weiterarbeiten. Sobald die defekte Festplatte ersetzt wird, wird eine neue Festplatte dann zur Ersatzfestplatte.

## **RPO**

Siehe auch **Wiederherstellungszeitpunkt (RPO)**.

## **RPO-Liste**

Eine Backupwarteschlange für alle geänderten Dateien, die überwacht und im Rahmen des NCDP-Prozesses gesichert werden. Eine Datei wird sofort nach ihrer Änderung in die RPO-Liste aufgenommen. Sobald die Liste voll oder die Zeit abgelaufen ist, werden die Daten aus der Warteschlange gesichert. Siehe auch **RPO**.

## **Rückspeicherung**

Ein Prozess, der das ausgewählte Dateisystem rekonstruiert und die Systemzustands- bzw. MS Exchange-Datenversionen aus geschützten Systemen an die Speicherstelle zurückspeichert, die im Rückspeicherungsassistenten gewählt wurde. Die Speicherstellen, die für die Rückspeicherung verfügbar sind, hängen vom ausgewählten Objekttyp ab. Geschützte Daten können in verschiedenen Versionen wiederhergestellt werden. Siehe auch **Point-in-Time Restore** und **Versionierung**.

## **SAS-Festplattenverbund**

Ein SAS-RAID-Festplattenverbund dient der Speicherung von Daten, die für den ordnungsgemäßen Betrieb von gingcom benötigt werden, im Speziellen für die internen Datenbanken und Konfigurationsdaten. SAS-Laufwerke zeichnen sich durch Hochleistung und Zuverlässigkeit aus.

## **SATA-Festplattenverbund**

Ein SATA-RAID-Festplattenverbund dient der Aufbewahrung von Daten der gingcom-Clients, die schnell wiederhergestellt werden sollen. SATA-Laufwerke zeichnen sich durch hohe Kapazität aus und werden auch für den NAS Dateibereich benutzt.

### **Selbstverwaltung**

Die gingcom Selbstverwaltung bietet eine enge Überwachung des Betriebs und der Komponenten von gingcom. Jeder Ausfall bzw. Fehler wird dem Ereignismanager gemeldet. Wenn möglich, werden automatische Maßnahmen ausgelöst. Dies umfasst auch regelmäßige Konsistenzprüfungen der internen Datenbanken und Prüfungen der Wiederherstellungsfähigkeit, um ununterbrochene Unternehmensprozesse und die gingcom Wiederherstellungsfähigkeit zu sichern. Siehe auch **Konsistenzprüfung** und **Wiederherstellungsprüfung**.

### **Single Instance-Speicherung**

Beruhend auf der CAS-Technologie verwendet gingcom die Hash-Prüfung für die Speicherung von maximal einer Kopie der gleichen Daten im gingcom Onlinespeicher. Zwei oder mehr identische Dateien werden durch Verweise auf eine einzelne gespeicherte Kopie der Datei ersetzt. Dies führt zu einer enormen Ersparnis an Festplattenkapazität und zu verbesserter Leistung. Siehe auch **Hash-Prüfung**.

### **Single Instancing**

Siehe auch **Single Instance-Speicherung**.

### **Statusbericht**

Konfigurierte Empfänger erhalten regelmäßig einen Statusbericht über den gingcom-Status und dessen Umgebung.

### **Storage Group**

Ein spezifischer Begriff für MS Exchange Server. Eine Sammlung von Mailbox-Speichern und öffentlichen Ordnerspeichern, die eine Gruppe von Transaktionsprotokolldateien gemeinsam nutzen. Exchange verwaltet jede Speicherungsgruppe durch einen getrennten Serverprozess.

### **Systemzustandsagent**

Ein auf jedem Client installiertes gingcom Softwaremodul. Während des Backups überträgt dieser Agent für den Betrieb der geschützten Systeme wichtige Daten, bspw. Registry, Boot und Active Directory auf Domain Controller, in den Online-Speicher. Dabei werden die Parameter beachtet, die in den Systemzustandsrichtlinien erstellt wurden. Bei einer

Rückspeicherung an die ursprüngliche Speicherstelle ersetzt der Systemzustandsagent die vorhandenen Systemzustandsdaten mit den wiederhergestellten Daten. Bei einer Rückspeicherung an die Alternativ-Speicherstelle überträgt der Systemzustandsagent die Daten an die angegebene Speicherstelle. Dort hat der Administrator darauf Zugriff.

### **Systemzustandsrichtlinien**

Eine Gruppe von Parametern, welche die Häufigkeit des Backups (Parameter für Dateisystem-Verzeichnisdurchlauf) für die Systemzustandsdaten und einen Zeitraum festlegen, für den die gesicherten Daten für eine Wiederherstellung aufbewahrt werden (der BRT-Parameter).

### **Tray Icon**

Dieses Symbol befindet sich in der Windows-Systemleiste jedes gingcom-Clients. Der Endanwender kann damit das Backup steuern, anhalten und wieder fortsetzen sowie seine geschützten Daten abrufen. Dazu ist für mobile Anwender eine bestehende VPN-Verbindung nötig. Siehe auch **Virtual Private Network (VPN)**.

### **Verzeichnisse ausschließen**

Dieser Parameter der Dateisystemrichtlinien beschreibt eine Liste von Verzeichnissen, die bei der Datensicherung nicht berücksichtigt werden sollen.

### **Vollständiges Backup (Full Backup)**

Ein Richtlinienparameter für Microsoft Exchange Server. Bei den Richtlinien für MS Exchange E-Mail legt der Parameter Vollständiger Backup den Zeitraum zwischen zwei aufeinander folgenden Journaling Mailbox-Backups fest. Während des Journaling Mailbox Backup werden E-Mails, die durch die entsprechend konfigurierte Journaling Mailbox erfasst wurden, gesichert und die Mailbox daraufhin gelöscht. Bei den Richtlinien für MS Exchange Server legt der Parameter Vollständiger Backup den Zeitraum zwischen zwei aufeinander folgenden vollständige MS Exchange Backups fest. Während des vollständigen MS Exchange Backup werden die ausgewählten Speicherungsgruppen und die entsprechenden Transaktionsprotokolle gesichert. Transaktionsprotokolle, die älter als der aktuelle Prüfpunkt sind, werden nach Abschluss des vollständigen Backups gelöscht. Siehe auch **inkrementeller Backup**.

### **Versionierung**

Beim Einsatz von NCDP können geschützte Daten zu bestimmten Zeitpunkten wiederhergestellt werden. Das bedeutet, vielfache Versionen geschützter Daten werden gespeichert und können vom Anwender wiederhergestellt werden. Der Anwender kann dann diese unterschiedlichen Versionen durchsuchen und zu früheren Versionen geschützter Daten zurückkehren. Der Zeitraum für die Aufbewahrung einer bestimmten Version, nach der gesucht werden kann, wird mit dem BRT-Parameter festgelegt. Siehe auch **Point-in-Time Restore** und **Rückspeicherung**.

### **Virtual Private Network (VPN)**

Ein nicht-öffentliches Netz, das innerhalb eines öffentlichen Netzes konfiguriert wird. VPN ist für den Fernzugriff auf gingcom-Appliance erforderlich. Die Netzverbindung wird laufend mithilfe des gingcom Tray Icons überwacht. Siehe auch **Tray Icon**.

### **Watermark**

Ein HSM-Richtlinienparameter. HSM gibt Daten aus dem NAS in die Nearline-Speicher gemäß der angegebenen Werten für den Parameter für „High Watermark“ und „Low Watermark“ frei. Siehe auch **High Watermark** und **Low Watermark**.

### **Wiederherstellung (gingcom-Wiederherstellung)**

Ein Prozess der Wiederherstellung von Daten, die für den Betrieb von gingcom erforderlich sind. Zu diesem Zweck wird das letzte im Nearline-Speicher gespeicherte gingcom-Backup verwendet. Siehe auch **gingcom-Backup**.

### **Wiederherstellungszeitpunkt (RPO)**

Ein Parameter der Dateisystemrichtlinien, die den NCDP-Prozess definieren. RPO stellt den Zeitpunkt dar, zu dem Daten wiederhergestellt werden müssen. Dies ist ein annehmbarer Zeitraum zwischen dem jetzigen Zeitpunkt und dem Alter der wiederherzustellenden Daten. Dieser Zeitraum ist definiert als größtmöglicher Zeitraum für Dateien auf dem geschützten Dateisystem, die nach einer Veränderung zu sichern sind. Siehe auch **nahezu fortlaufende Datensicherung (NCDP)** und **RPO-Liste**.

**Wiederherstellungsprüfung**

Eine der Funktionen von gingcom für die Selbstverwaltung. Ein automatischer Prozess, der periodisch die Wiederherstellungsfähigkeit der internen Datenbanken und Konfiguration von gingcom sowie die Anwenderdaten überprüft, um eine zuverlässige Rückspeicherung zu gewährleisten.

**ZPO**

Zivilprozessordnung

**Zugriffskontrolle**

Ein gingcom Sicherheitsmechanismus, der den Active Directory Service zur Benutzerauthentifizierung einsetzt. Der Zugang zu bestimmten gingcom Funktionen und geschützten Daten wird je nach dem bezeichneten Anwender und der Gruppen eingeschränkt. Ein gingcom Administrator erhält Zugang zu allen gingcom Funktionen und geschützten Daten, während ein Endbenutzer seine geschützten Daten lediglich durchsuchen und abrufen darf.

## **Kurzbiographie und ausgewählte Publikationen**

Dr. Ivo Geis – Jahrgang 1943 - ist Rechtsanwalt in Hamburg und arbeitet im Recht der Informationstechnologie mit dem Schwerpunkt in den Themen Rechtsfragen der elektronischen Kommunikation, Dokumentation und des Datenschutzes. Zu diesen Themen nimmt Dr. Geis auch in seinen Veröffentlichungen Stellung. Ehrenamtlich ist Dr. Geis Leiter des „Arbeitskreises „Rechtsfragen der digitalen Kommunikation“ der AWW Arbeitsgemeinschaft für wirtschaftlichen Verwaltung e.V. in Eschborn. Von Anfang des Jahres 1998 bis zum Anfang des Jahres 2003 war Dr. Geis Vorsitzender der Hamburgischen Datenschutzgesellschaft e.V.

Zivilprozessrechtliche Aspekte des elektronischen Dokumentenmanagements,  
Computer und Recht 1993, 653 ff.

Rechtsfragen der elektronischen Archivierung,  
Betriebswirtschaftliche Blätter 1997, 492 ff.

Rechtsfragen der Telearchivierung medizinischer Dokumente,  
Datenschutz und Datensicherheit, 1997, 582 ff.

Rechtliche Betrachtung eines digitalen Personalaktensystems,  
Geis, Grenzer, Jänicke, Lohn+Gehalt, 2003, 40 ff.

Die Rechtssicherheit des elektronischen Geschäftsverkehrs unter dem Aspekt der Revision,  
Revision, 2003, 5 ff.

Das Recht der E-Mail-Kommunikation

In: Recht und Praxis des elektronischen Geschäftsverkehrs

AWV-Verlag 2003

Kommentar zum Signaturgesetz

In: *Spindler, Schmitz, Geis*: Teledienstegesetz, Beckverlag, München 2004

Rechtssicherheit des elektronischen Geschäftsverkehrs

Verlag Recht und Wirtschaft GmbH, Heidelberg 2004

E-Mail: Rechtsaspekte der elektronischen Unternehmenskommunikation

Frankfurter Allgemeine Zeitung, Seite „Recht und Steuern“, Ausgabe 18. Mai 2005

Signatur sucht Anwendung – heute: die elektronische Archivierung

- Die Rechtslage in Deutschland, Österreich und der Schweiz –

AWV Informationen November/Dezember 2006.