

# Datensicherungskonzept terra CLOUD Backup

## Anforderungen an ein Datensicherungskonzept gemäß den Angaben des BSI

Der Verlust von Daten eines Unternehmens kann erhebliche Geschäftsauswirkungen haben und sogar existenzbedrohend für ein Unternehmen sein. Darüber hinaus wird die Datensicherung durch verschiedene Gesetzgebungen vorgeschrieben. Ein Unternehmen ist folglich verpflichtet sich gegen die vielfältigen Möglichkeiten eines Datenverlustes ausreichend abzusichern.

Um eine konsistente und unternehmensweite Datensicherung anzustreben ist eine zentrale Datenhaltung im Unternehmen anzustreben, sodass an zentraler Stelle automatisiert alle relevanten Daten des Unternehmens gesichert werden können. Eine angemessene Datensicherung sollte über fachlich qualifiziertes oder geschultes Personal gewährleistet werden. Dabei sollte die Datensicherung im möglichst hohen Grad automatisiert ablaufen. Diesbezüglich sollte auf entsprechende Systeme zurückgegriffen werden. Auch muss ein angemessener Lagerort für die Speichermedien zur Verfügung stehen.

Die durchgeführte Datensicherung muss durch einen benannten Verantwortlichen regelmäßig überprüft und eine korrekte Arbeitsweise sichergestellt werden.

Neben der Sicherstellung einer korrekten Arbeitsweise muss die Möglichkeit der Datenrekonstruktion sichergestellt werden: In regelmäßigen Abständen und nach jeder Änderung des Datensicherungsverfahrens. Sichergestellt werden müssen die Punkte:

- der Möglichkeit der Wiederherstellung,
- eine praktikable Umsetzung im Arbeitsalltag,
- eine ausreichende Dokumentation,
- sowie eine angemessene Zeitdauer zur Datenrekonstruktion.

Die Übungen sollten im Rahmen der Notfallvorsorge umgesetzt werden und in einen stetigen Revisions- und Verbesserungsprozess einfließen.

Beratung für:

- Datenschutz
- Informationssicherheit
- IT Sicherheit
- IT Management

GDI Gesellschaft für  
Datenschutz und  
Informationssicherheit mbH

### Anschrift

Fleyer Straße 61  
D - 58097 Hagen

### Kontakt

Tel: +49 (0) 2331 356 832 - 0  
Fax: +49 (0) 2331 356 832 - 1

info@gdi-mbh.eu  
www.gdi-mbh.eu

Geschäftsführer  
Dipl. Inform. Olaf Tenti

Ust-IdNr.: DE 27 630 67 01  
Amtsgericht Hagen  
HRB 8805

### Bankverbindung

Deutsche Bank AG Hagen  
Konto-Nr.: 710 25 1000  
BLZ.: 450 700 24  
IBAN: DE20450700240710251000  
BIC: DEUTDEDB450

## Der Gesetzgeber verpflichtet in vielen Punkten zur Datensicherung.

Der Bundesgerichtshof BGH schreibt in seiner Urteilsbegründung schon 1996 (BGH-Urteil von 1996 / x ZR 64/94) „...Datensicherung ist eine allgemein bekannte Selbstverständlichkeit (vgl. OLG Karlsruhe, CR 1996, 348f.). Angesichts der mannigfachen Gefahren eines Datenverlustes und der daraus regelmäßig folgenden schweren wirtschaftlichen Schäden für den EDV-Anwender gilt sie als unverzichtbar (vgl. Becker, NJW-CoR 1992, 17). Aus diesem Grund werden zumindest bei gewerblicher Nutzung einer EDV-Anlage – wie auch hier – zur Datensicherung besondere Sicherungsroutinen vorgesehen, die hinreichende Gewähr dafür bieten, dass in regelmäßigem Zeitabstand der Datenbestand des Anwenders auf einem besonderen Datenträger abgespeichert wird. ...“ Nach dem Urteil des Oberlandesgerichtes Hamm vom 01.12.2003 ist das Mindestmaß einer Datensicherung, eine tägliche Sicherung aller Daten und eine wöchentliche Vollsicherung. terra CLOUD Backup kann diese Anforderung erfüllen, in dem tägliche Sicherungen durchgeführt werden. Eine aktuelle synthetische Vollsicherung liegt - nach dem erfolgreichen Initialbackup bzw. erfolgreichen täglichen oder wöchentlichen Backups - auf dem Vault bereit. Weiterführende Informationen finden Sie unter „Vollständigkeit der terra CLOUD Backup Lösung“.

Um einem Mitverschulden einer nicht ausreichenden Datensicherung gem. § 245 BGB entgegenzuwirken, muss die Datensicherung vom Reseller oder Endkunden (von hier an Auftraggeber genannt) regelmäßig überprüft werden und muss redundant angelegt sein. Es muss sichergestellt sein, dass die Datensicherung inklusive aller zu sichernden Daten auf vereinbarte Datensicherungsmedien geschrieben wird. Der Auftraggeber definiert die Zielmedien der Datensicherung beim Buchen des terra CLOUD Backups. Die Backupdaten liegen ausschließlich in Deutschland. Weiterführende Informationen wie terra CLOUD Backup diese Anforderung umsetzt finden Sie unter „Zuverlässigkeit der terra CLOUD Backup Lösung“.

Gemäß § 9 Bundesdatenschutzgesetz (BDSG) Anhang A wird eine Verfügbarkeitskontrolle und eine Weitergabekontrolle von Daten gefordert. Im Rahmen der Weitergabekontrolle (Nr. 4 der Anlage zu § 9 Satz 1 BDSG) ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener

Beratung für:

- Datenschutz
- Informationssicherheit
- IT Sicherheit
- IT Management

**GDI Gesellschaft für  
Datenschutz und  
Informationssicherheit mbH**

**Anschrift**

Fleyer Straße 61  
D - 58097 Hagen

**Kontakt**

Tel: +49 (0) 2331 356 832 - 0  
Fax: +49 (0) 2331 356 832 - 1

info@gdi-mbh.eu  
www.gdi-mbh.eu

Geschäftsführer  
Dipl. Inform. Olaf Tenti

Ust-IdNr.: DE 27 630 67 01  
Amtsgericht Hagen  
HRB 8805

**Bankverbindung**

Deutsche Bank AG Hagen  
Konto-Nr.: 710 25 1000  
BLZ.: 450 700 24  
IBAN: DE20450700240710251000  
BIC: DEUTDEDB450

Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle). Im Rahmen der Verfügbarkeitskontrolle (Nr. 7 der Anlage zu § 9 Satz 1 BDSG) ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. terra CLOUD Backup stellt diese Anforderungen unter anderem durch Verschlüsselung sowie Protokollierung der durchgeführten Aufgaben und Zugriffe sicher. Weiterführende Informationen finden Sie unter „Vertraulichkeit der terra CLOUD Backup Daten“ sowie unter „Integrität der terra CLOUD Backup Lösung“.

Gem. §§ 238 Abs. 2 HGB und 147 Abs. 3 AO müssen angemessene Fristen zur Wiederherstellung aller Daten in den Verträgen der Vertragspartner definiert sein. terra CLOUD Backup stellt diese Anforderung wie folgt sicher:

- der Auftraggeber kann eine sofortige Wiederherstellung der Daten über das Netzwerk anstoßen – in diesem Fall ist keine Zuarbeit mit der terra CLOUD GmbH (in Folge Auftragnehmer genannt), notwendig oder
- der Auftraggeber kann die Zusendung der Wiederherstellungsdaten auf Festplatte(n), Zusendung unter anderem per Kurier, auslösen.

Bei Kündigung des Backupservices können die Daten optional dem Auftraggeber per Festplatte zur Verfügung gestellt werden. Generell werden die von der Kündigung betroffenen Datensicherungen innerhalb von 14 Tage nach Kündigung gelöscht. Das Löschen der Daten erfolgt nach DOD 5220.22-M.

Die jeweiligen Rechte und Pflichten der Vertragspartner sind dem „terra CLOUD – Leistungsbeschreibung Backup“ Dokument im terra CLOUD Portal zu entnehmen. Zusätzlich sind die wichtigsten technischen und organisatorischen Sicherungsmaßnahmen zur sicheren Datensicherung und Datenhaltung in dem Dokument „terra CLOUD\_Backup\_Schnellstart“ definiert. Die beschriebenen Maßnahmen stellen das Mindestmaß der Sicherheitsmaßnahmen dar.

## Funktionsbeschreibung terra CLOUD Backup

### Übersicht zu Funktionen von terra CLOUD Backup

- Ende zu Ende Verschlüsselung
- FIPS-konforme AES-Verschlüsselung
- Schlüssel zur Entschlüsselung der Datensicherung liegt ausschließlich beim Auftraggeber

#### Beratung für:

- Datenschutz
- Informationssicherheit
- IT Sicherheit
- IT Management

**GDI Gesellschaft für  
Datenschutz und  
Informationssicherheit mbH**

#### **Anschrift**

Fleyer Straße 61  
D - 58097 Hagen

#### **Kontakt**

Tel: +49 (0) 2331 356 832 - 0  
Fax: +49 (0) 2331 356 832 - 1

info@gdi-mbh.eu  
www.gdi-mbh.eu

Geschäftsführer  
Dipl. Inform. Olaf Tenti

Ust-IdNr.: DE 27 630 67 01  
Amtsgericht Hagen  
HRB 8805

#### **Bankverbindung**

Deutsche Bank AG Hagen  
Konto-Nr.: 710 25 1000  
BLZ.: 450 700 24  
IBAN: DE20450700240710251000  
BIC: DEUTDEDB450

- Authentifizierung und Autorisierungsprozess der Berechtigten und Verantwortlichen Personen liegt beim Auftraggeber
- Alle Interaktionen müssen von dem Auftraggeber initiiert werden (zum Beispiel muss der Auftraggeber durch autorisierte Mitarbeiter die Löschung von Daten beantragen)
- Verschlüsselte Verbindung zur Verwaltung der Backup-Prozesse
- Rollenbasiertes Sicherheitskonzept zur Zugangssteuerung
- Protokollierung des Sicherungsprozesses und aller Wiederherstellungen
- Zutrittskontrollmechanismen
- Verfügbarkeit von Dateien und Systemen: Sicherstellung mittels redundanter Rechenzentrumsinfrastruktur, Clustertechnologien und der Option Backupdaten zweifach vorzuhalten in verschiedenen Brandabschnitten des deutschen terra CLOUD Rechenzentrum bzw. deutschen Partner-Rechenzentrum
- Einhaltung aller Anforderungen des BDSG

#### Detaillierte Funktionsbeschreibung von terra CLOUD Backup

##### Funktionalität der terra CLOUD Backup Lösung

- Subsite für Endkunden anlegen (nur durch Reseller)
- Benutzermanagement (Benutzer anlegen, Rechte vergeben)
- Sicherung einrichten und durchführen
- Wiederherstellung durchführen und
- Protokollierung

Die vorhandenen Funktionen eignen sich dabei zur Erledigung der oben genannten Szenarien. Voraussetzung ist eine störungsfreie Internetverbindung, funktionsfähige Systeme die gesichert werden und die Einhaltung der vorgeschriebenen Anforderungen wie sie im Bootcamp und im Webcast/Dokumentation vermittelt werden.

Ein unberechtigter Zugriff auf Backupdaten wird durch ein funktionsfähiges Benutzermanagement sowie durch technische Maßnahmen wie verschlüsselte Authentifizierung und verschlüsselte Backupdaten verhindert.

##### Zuverlässigkeit der terra CLOUD Backup Lösung

Das terra CLOUD Backup Portal bzw. Backupsystem stürzt in den bereits genannten Szenarien nicht ab. Fehlerhafte Eingaben führen bisher zu keiner Beeinträchtigung des Systems sondern werden intern abgefangen oder werden nicht akzeptiert/führen zu einer Fehlermeldung. Auf diese Weise werden Fehlbedienungen verhindert.

#### Beratung für:

- Datenschutz
- Informationssicherheit
- IT Sicherheit
- IT Management

**GDI Gesellschaft für  
Datenschutz und  
Informationssicherheit mbH**

#### **Anschrift**

Fleyer Straße 61  
D - 58097 Hagen

#### **Kontakt**

Tel: +49 (0) 2331 356 832 - 0  
Fax: +49 (0) 2331 356 832 - 1

info@gdi-mbh.eu  
www.gdi-mbh.eu

Geschäftsführer  
Dipl. Inform. Olaf Tenti

Ust-IdNr.: DE 27 630 67 01  
Amtsgericht Hagen  
HRB 8805

#### **Bankverbindung**

Deutsche Bank AG Hagen  
Konto-Nr.: 710 25 1000  
BLZ.: 450 700 24  
IBAN: DE20450700240710251000  
BIC: DEUTDEDB450

Die Rechenzentrumsinfrastruktur ist redundant aufgebaut um die Verfügbarkeit der Systeme zu erhöhen. Gebäudetechnisch sowie Applikationsseitig wurden Maßnahmen ergriffen um Datenverlust (zum Beispiel durch unautorisierte Zugriffe) zu vermeiden und die Verfügbarkeit der Systeme zu gewährleisten.

Eine 100% Sicherheit der Hardware/Storage kann nicht gewährleistet werden. Um eine erhöhte Verfügbarkeit der Daten zu gewährleisten, bietet terra CLOUD Backup die optionale Verwendung eines sekundären Backup Vaults (terra CLOUD Backup Tier 2) in einem anderen Brandabschnitt bzw. für Geo-Redundanz (terra CLOUD Backup Tier 3) einen sekundären Vault in einem anderen deutschen Rechenzentrum an. Alternativ kann der terra CLOUD Backup Satellite im Netzwerk des Endkunden aufgestellt werden. Dadurch werden Backupdaten lokal beim Endkunden gespeichert bevor diese in den terra CLOUD Backup Vault gesichert werden.

terra CLOUD Backup verwendet zur Datensicherung nur Speicherverfahren, die alle handelsrechtlichen und steuerrechtlichen Aufbewahrungsvorschriften in Hardware und Software einhalten.

Der Auftraggeber entscheidet bei Buchung von terra CLOUD Backup, welche Datensicherungsmedien (terra CLOUD Backup Tier 1 bis Tier 3, terra CLOUD Backup Satellite) verwendet werden. Der Auftraggeber kann nach Buchung des Backups den Tier wechseln bzw. einen zusätzlichen terra CLOUD Backup Satellite hinzufügen/stornieren.

### **Benutzbarkeit der terra CLOUD Backup Lösung**

Die Bedienoberfläche ist einfach gestaltet und der gängigen Praxis der Useability entsprechend aufgebaut und benannt. Zur Durchführung der wichtigsten Anwendungsbeispiele, sind wenige Klicks im terra CLOUD Backup Portal durch den Auftraggeber notwendig.

Die Aktionen und Felder sind in deutscher Sprache und benannt nach den Aktionen, damit diese verständlich sind.

Das System kann nach Teilnahme am Bootcamp (Session zu Backup) oder Durcharbeiten des Webcasts/Dokumentation durch den Auftraggeber verwendet werden. Die schnelle Erlernbarkeit ist gegeben.

### **Verfügbarkeit der terra CLOUD Backup Lösung und Backupdaten**

Die Online Backups sind 24 Stunden pro Tag, 7 Tage die Woche an 365 Tagen im Jahr über das terra Cloud Portal abrufbar (mit Einschränkung von angekündigten Wartungszeiträumen). Entscheidend sind die in dem

Beratung für:

- Datenschutz
- Informationssicherheit
- IT Sicherheit
- IT Management

**GDI Gesellschaft für  
Datenschutz und  
Informationssicherheit mbH**

#### **Anschrift**

Fleyer Straße 61  
D - 58097 Hagen

#### **Kontakt**

Tel: +49 (0) 2331 356 832 - 0  
Fax: +49 (0) 2331 356 832 - 1

info@gdi-mbh.eu  
www.gdi-mbh.eu

Geschäftsführer  
Dipl. Inform. Olaf Tenti

Ust-IdNr.: DE 27 630 67 01  
Amtsgericht Hagen  
HRB 8805

#### **Bankverbindung**

Deutsche Bank AG Hagen  
Konto-Nr.: 710 25 1000  
BLZ.: 450 700 24  
IBAN: DE20450700240710251000  
BIC: DEUTDEDB450

Vertrag zwischen Auftragnehmer und Auftraggeber vereinbarte Leistungspflichten.

Es wird über das terra CLOUD Backup Portal auf die Backupdaten des jeweiligen Systems zugegriffen. Voraussetzung ist eine störungsfreie Internetverbindung.

Optional ist über den terra CLOUD Backup Satellite möglich lokale Sicherungen innerhalb des Firmennetzes des Endkunden vorzuhalten. Der Auftraggeber kann die aktuellen Sicherungen der gesicherten Systeme von diesem aus wiederherstellen.

### **Vertraulichkeit der terra CLOUD Backup Daten**

Durch das terra CLOUD Backup Portal können keine Veränderung oder Manipulation der Datensicherungen erfolgen. Über das Portal sind nur Einstellungen zum Backup und zur Wiederherstellung bzw. Benutzermanagement möglich.

Darüber hinaus können Mitarbeiter des Auftragnehmers die Backupdaten nicht verändern oder manipulieren, da diese Verschlüsselt vorliegen und es keine alternative Entschlüsselungsmethode gibt. Einzig durch Eingabe des Passworts, welches ausschließlich dem Auftraggeber bekannt ist, kann eine Entschlüsselung erfolgen.

Während des Vorhaltezeitraums für die Backupdaten können diese nur von Auftragnehmer, im (schriftlichen) Auftrag des Auftraggebers, gelöscht werden.

### **Integrität der terra CLOUD Backup Lösung**

Ein autorisierter Zugriff auf das TERRA CLOUD Backup Portal durch den Auftraggeber wird mittels personalisierten Kontonamen/Passwort ermöglicht. Bei der Wiederherstellung ist zusätzlich das Passwort notwendig, welches der Auftraggeber zur Verschlüsselung der Datensicherungen gesetzt hat.

Jeder Zugriff an dem Portal oder durch den Agenten zur Datensicherung auf das System wird erneut autorisiert und protokolliert.

Unter Voraussetzung einer störungsfreien Internetleitung seitens des Auftraggebers und zu sichernden Systemen, werden die Backups und Wiederherstellungen im zeitlichen Rahmen durchgeführt.

Beratung für:

- Datenschutz
- Informationssicherheit
- IT Sicherheit
- IT Management

**GDI Gesellschaft für  
Datenschutz und  
Informationssicherheit mbH**

#### **Anschrift**

Fleyer Straße 61  
D - 58097 Hagen

#### **Kontakt**

Tel: +49 (0) 2331 356 832 - 0  
Fax: +49 (0) 2331 356 832 - 1

info@gdi-mbh.eu  
www.gdi-mbh.eu

Geschäftsführer  
Dipl. Inform. Olaf Tenti

Ust-IdNr.: DE 27 630 67 01  
Amtsgericht Hagen  
HRB 8805

#### **Bankverbindung**

Deutsche Bank AG Hagen  
Konto-Nr.: 710 25 1000  
BLZ.: 450 700 24  
IBAN: DE20450700240710251000  
BIC: DEUTDEDB450

## Vollständigkeit der terra CLOUD Backup Lösung

Die Zeitpläne zur Datensicherung werden durch den Auftraggeber im terra CLOUD Backup Portal festgelegt. Der Auftraggeber kann den Zeitintervall (Stündlich bis Monatlich) der Backups festlegen. Die Vorhaltezeit der Backupdaten richtet sich nach der Konfiguration durch den Auftraggeber basierend auf den unternehmensinternen Aufbewahrungsrichtlinien. Eine maximale Anzahl von 41 Sicherungen pro Sicherungsobjekt ist konfigurierbar.

Das Backup wird als synthetisches volles Backup vorgehalten. Dadurch ist eine Wiederherstellung der gesamten Datensicherung zu einem bestimmten Zeitpunkt möglich, ohne inkrementelle Backups wiederherstellen zu müssen. Die Zeitspanne der Wiederherstellung richtet sich maßgeblich nach der Netzwerk - Verbindungsgeschwindigkeit. Sollte eine Rücksicherung über Netzwerk keine Option sein, besteht die Möglichkeit das Backup in die terra CLOUD wiederherzustellen oder die Daten zur Wiederherstellung auf einer Festplatte, z.B. per Kuriersendung, zu erhalten. Die Rücksicherung erfolgt über das Kundenportal und wird vom Auftraggeber initiiert.

Optional kann der terra CLOUD Backup Satellit bei einem Endkunden in dessen Firm Netzwerk eingerichtet werden. Dadurch werden Backupdaten lokal zwischengespeichert. Es erlaubt dem Endkunden größere Flexibilität in Hinsicht auf Datensicherungen, Übertragung der Datensicherungen an den terra CLOUD Backup Vault sowie lokale Wiederherstellung.

## Ablaufsystematik der Datensicherung:

Die Initialsicherung wird durch den Auftraggeber im terra CLOUD Backup Portal konfiguriert und gestartet. Die Initialdaten können über Netzwerk übertragen werden. Alternativ kann der Auftraggeber die Daten per Festplatte an den Auftragnehmer senden oder per FTP Server in kleineren Schritten hochladen. Für die beiden zuletzt genannten Optionen spielt der Auftragnehmer die bereits verschlüsselten Daten in den Backupspeicher (Vault) des Auftraggebers ein.

Die Backupdaten werden vor Verlassen des gesicherten Systems bereits verschlüsselt. Das Passwort zur Entschlüsselung der Datensicherungen befindet sich ausschließlich in den Händen des Auftraggebers. Es liegt in der Verantwortung des Auftraggebers geeignete Sicherungsmaßnahmen gegen den Verlust des Passwortes zu ergreifen. Dem Auftraggeber ist

Beratung für:

- Datenschutz
- Informationssicherheit
- IT Sicherheit
- IT Management

**GDI Gesellschaft für  
Datenschutz und  
Informationssicherheit mbH**

### Anschrift

Fleyer Straße 61  
D - 58097 Hagen

### Kontakt

Tel: +49 (0) 2331 356 832 - 0  
Fax: +49 (0) 2331 356 832 - 1

info@gdi-mbh.eu  
www.gdi-mbh.eu

Geschäftsführer  
Dipl. Inform. Olaf Tenti

Ust-IdNr.: DE 27 630 67 01  
Amtsgericht Hagen  
HRB 8805

### Bankverbindung

Deutsche Bank AG Hagen  
Konto-Nr.: 710 25 1000  
BLZ.: 450 700 24  
IBAN: DE20450700240710251000  
BIC: DEUTDEDB450

bewusst, dass ein Verlust des Passwortes gleichbedeutend mit dem Verlust sämtlicher Datensicherungen ist. Seitens des Auftragnehmers werden sämtliche Zugriffe durch den Auftraggeber und jede Datenübertragung protokolliert.

Der Auftragnehmer kann nicht mit personenbezogenen Daten des Auftraggebers in Kontakt kommen, da diese nur verschlüsselt beim Auftragnehmer liegen. Das Entschlüsselungspasswort liegt allein beim Auftraggeber.

## Installationsvoraussetzungen für terra CLOUD

### Backup von EVault

Die Installation der Managementumgebung entspricht der Anforderung im Dokument „Director Operations Guide“ Kapitel 2 „Install and Upgrade Director“. Dabei wurden die Hardware Anforderungen aus den entsprechenden „Director7 - Release Notes“ eingehalten bzw. übertroffen. Benutzerkonten wurden wie im Dokument Director Operations Guide angelegt mit „Least Privileg“ Konten. Die Firewalls wurde für die Agentenkommunikation zu den Vaults auf Ports 2546 und 2547 entsprechend konfiguriert.

Die Funktionalität der Managementumgebung wurde nach erfolgreicher Installation geprüft indem:

- Login getestet wurde
- Vault für Testkunden angelegt wurde
- Konto und Benutzer für Testkunden angelegt wurde
- Korrekte Lizenzverwaltung nach Anlegen eines Testkunden geprüft wurde
- Das im Portal angelegte Backup (gesicherter Computer sichtbar/korrekt; Safesets sichtbar/korrekt; Logs sichtbar) korrekt angezeigt wurde
- Jobs des Backup korrekt angezeigt wurde.

Die Installation des Portals entspricht den Anforderungen im Dokument „Portal Installation and Configuration Guide“. Wie im Kapitel 2 „Prerequisites“ geschrieben, wurden die Netzwerkkarten mit den entsprechenden Protokollen konfiguriert und die Firewall für die entsprechenden Ports konfiguriert. Es wurden nur die in Kapitel 2.1 geforderten Komponenten für den Webserver des Portals installiert.

Die Installation des Portals erfolgte gemäß den Anweisungen in Kapitel 3. Der Report Server u.a. zur Erstellung von Status Reports der Backups

Beratung für:

- Datenschutz
- Informationssicherheit
- IT Sicherheit
- IT Management

**GDI Gesellschaft für  
Datenschutz und  
Informationssicherheit mbH**

**Anschrift**

Fleyer Straße 61  
D - 58097 Hagen

**Kontakt**

Tel: +49 (0) 2331 356 832 - 0  
Fax: +49 (0) 2331 356 832 - 1

info@gdi-mbh.eu  
www.gdi-mbh.eu

Geschäftsführer  
Dipl. Inform. Olaf Tenti

Ust-IdNr.: DE 27 630 67 01  
Amtsgericht Hagen  
HRB 8805

**Bankverbindung**

Deutsche Bank AG Hagen  
Konto-Nr.: 710 25 1000  
BLZ.: 450 700 24  
IBAN: DE20450700240710251000  
BIC: DEUTDEDB450

wurde nach Kapitel 4 installiert. Wie in Kapitel 8 verlangt wurde die Funktionalität des Portals nach erfolgreicher Installation geprüft indem:

- Login getestet wurde.
- Site für ein Testkunden angelegt wurde
- Administrativer Benutzer angelegt wurde
- Computer hinzugefügt wurde
- Backup Job hinzugefügt wurde und
- Report erstellt und von Admin eingesehen wurde.

Es sind keine technischen Möglichkeiten bekannt, die außerhalb der Benutzeroberfläche des Portals dem Auftraggeber die Möglichkeit geben, eigene oder fremde Daten im terra CLOUD Backup Vault zu verändern oder zu manipulieren.

Die Backupdaten verlassen den zu sichernden Server bereits verschlüsselt und können von Mitarbeitern des Auftragnehmers nicht entschlüsselt werden.

## Zusammenfassung

Die korrekte Installation zur Sicherstellung der ordnungsgemäßen Funktion laut Hersteller wurde basierend auf „Installationsvoraussetzung für terra CLOUD Backup von EVault“ überprüft.

Der Auftragnehmer hat keinen Zugriff auf die Daten des Auftraggebers.

Hagen, 30.9.15   
( Ort, Datum, Unterschrift - Olaf Tenti )

**GDI mbH**  
Gesellschaft für Datenschutz  
und Informationssicherheit mbH  
Fleyer Str. 61  
58097 Hagen  
Tel: 02331 / 35 68 32 - 0

Beratung für:

- Datenschutz
- Informationssicherheit
- IT Sicherheit
- IT Management

**GDI Gesellschaft für  
Datenschutz und  
Informationssicherheit mbH**

### Anschrift

Fleyer Straße 61  
D - 58097 Hagen

### Kontakt

Tel: +49 (0) 2331 356 832 - 0  
Fax: +49 (0) 2331 356 832 - 1

info@gdi-mbh.eu  
www.gdi-mbh.eu

Geschäftsführer  
Dipl. Inform. Olaf Tenti

Ust-IdNr.: DE 27 630 67 01  
Amtsgericht Hagen  
HRB 8805

### Bankverbindung

Deutsche Bank AG Hagen  
Konto-Nr.: 710 25 1000  
BLZ.: 450 700 24  
IBAN: DE20450700240710251000  
BIC: DEUTDE33HAN30