

## 1 Übergabe und Löschung von DSGVO-relevanten Kundendaten

### 1.1 Nach fristgerechter, aber sehr kurzfristiger, Kündigung des zugrunde liegenden IT-Dienstleistungsvertrags

Datenübergabe und Datenlöschung von DSGVO-relevanten Kundendaten nach langjährigem Datenmanagement und Auftragsdatenverarbeitung durch profidata-IT als externer Dienstleister - nach einer fristgerechten Kündigung des Dienstleistungs-Vertrages.

### 1.2 Bedeutung gründlicher und gesetzeskonformer Arbeit

Die Datenaufbereitung und -übergabe ist ein komplexer Prozess, der sorgfältige Planung und Durchführung erfordert.


Fehler oder Nachlässigkeiten können zu rechtlichen Konsequenzen und Vertrauensverlust führen. Daher ist es wichtig, alle Schritte gründlich und gesetzeskonform durchzuführen.

### 1.3 Profidata-IT / Web-Link

<https://www.profidata-it.de/Szenario---Daten-%C3%9Cbergabe.html>

## 2 Server-Struktur(en) vor und nach Vertrags-Ende

### 2.1 Einleitungs-Grafik



Schematischer Vergleich der ursprünglichen  
VERA-SERVER-Landschaft  
mit dem  
aktuellen „Datenablage“-Server

**VERA-Server, Tools, Softwares,  
Umgebung, Integration und Sub-Systeme**

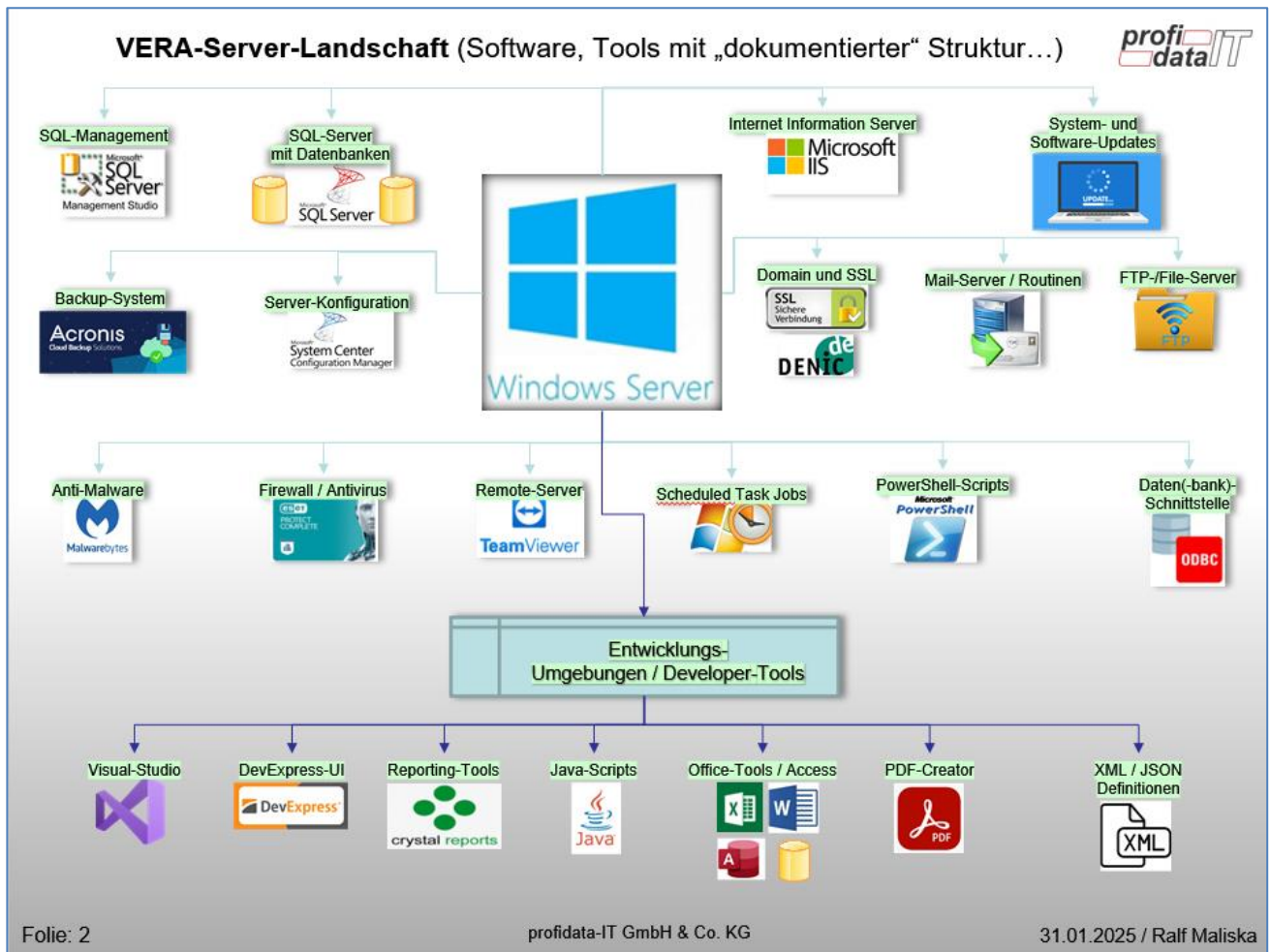
**VS.**

**Aktueller-Server nach Vertrags-Beendigung  
zum 31.12.2024**

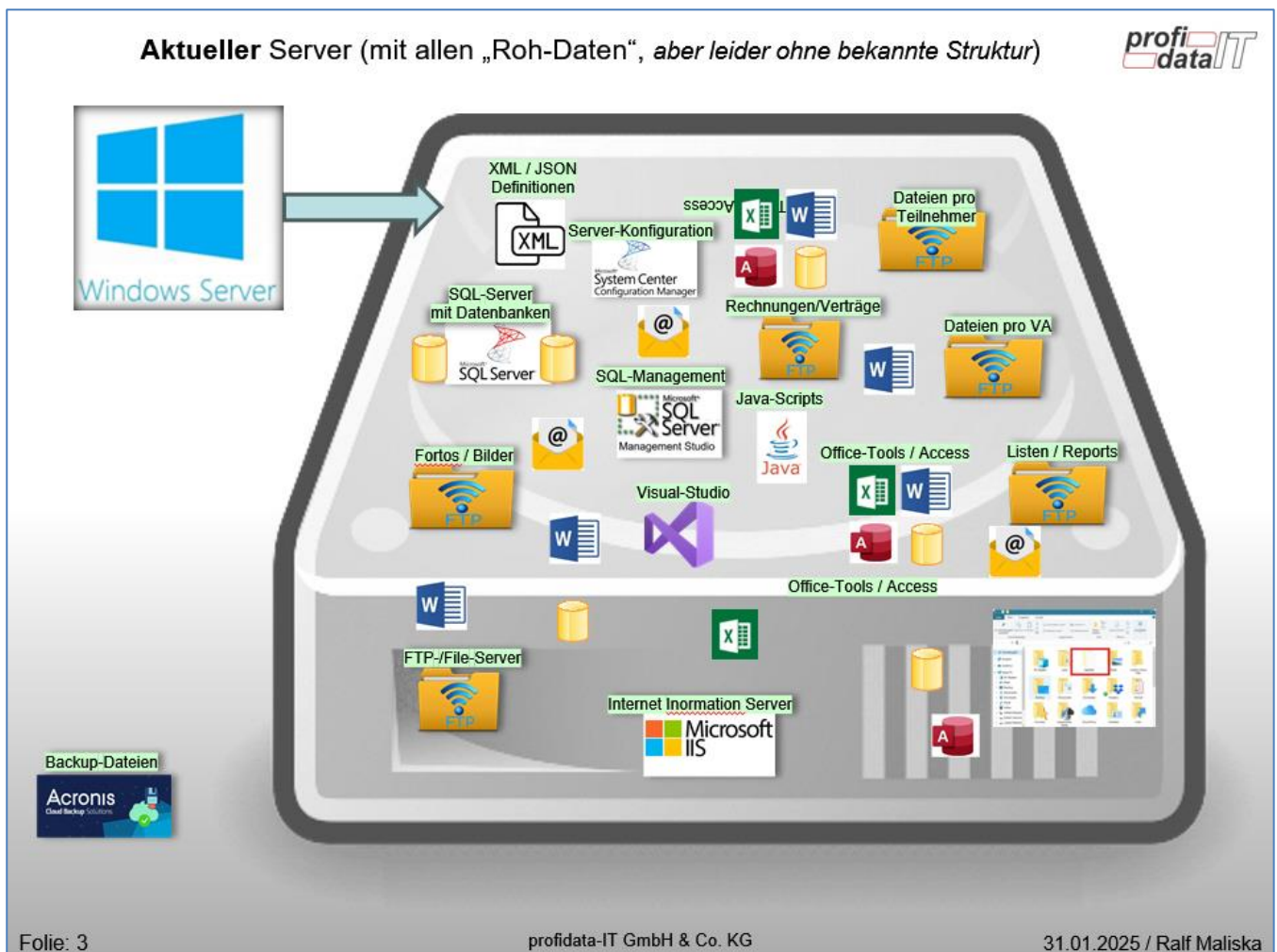
Entwicklungs-Stand 31.01.2025

Folie: 1      profidata-IT GmbH & Co. KG      31.01.2025 / Ralf Maliska

## 2.2 VERA-Server-Struktur **VOR** Kündigung des Vertrags




## 2.3 VERA-Server-Struktur **NACH** Kündigung des Vertrags



### 3 Fakten und Erläuterungen durch und bei profidata-IT.de

#### 3.1 Kompakt-Darstellung / Web-Hardcopy

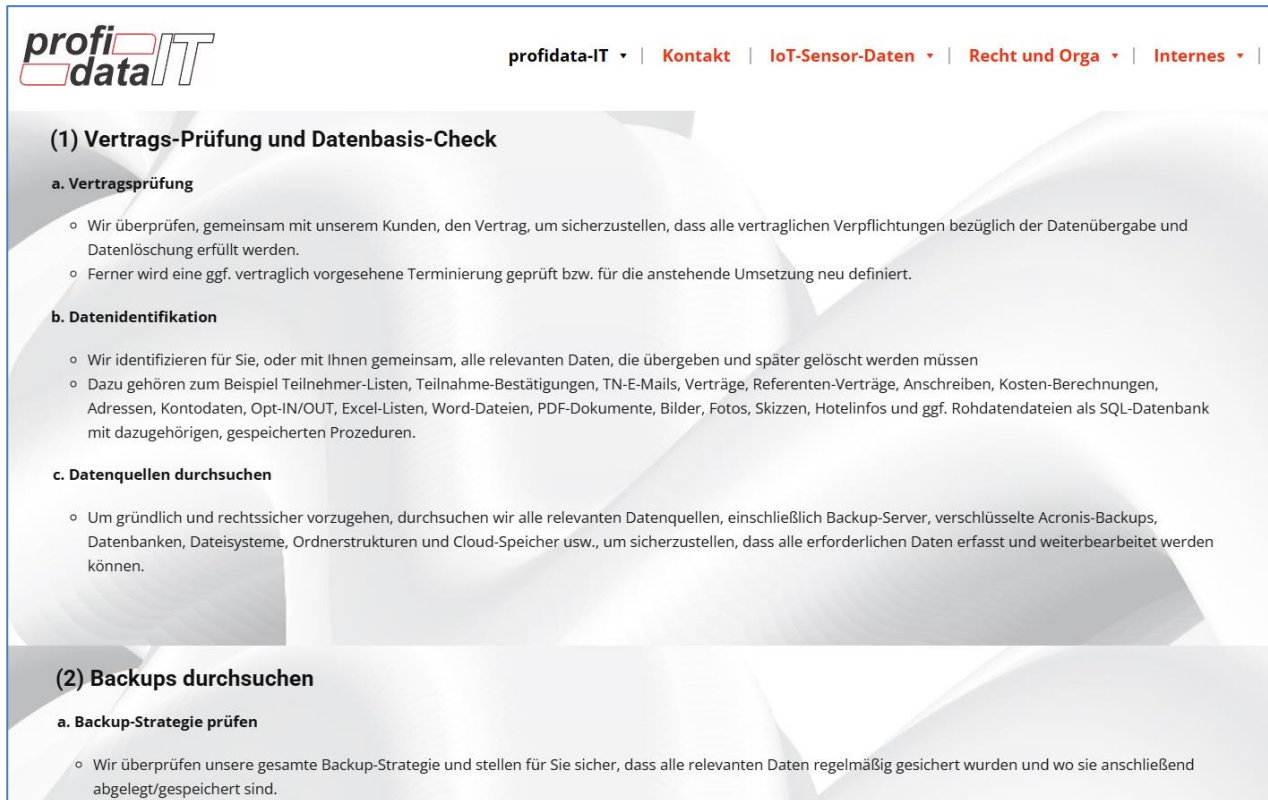


[profidata-IT](#) | 
 [Kontakt](#) | 
 [IoT-Sensor-Daten](#) | 
 [Recht und Orga](#) | 
 [Internes](#)

<p style="text-align: center;"><b>1</b></p> <p style="text-align: center;"><b>VERTRAGS-PRÜFUNG:</b></p> <p>Wir überprüfen, gemeinsam mit unserem Kunden, den Vertrag, um sicherzustellen, dass alle vertraglichen Verpflichtungen bezüglich der Datenübergabe und Datenlöschung erfüllt werden.</p>	<p style="text-align: center;"><b>2</b></p> <p style="text-align: center;"><b>BACKUPS DURCHSUCHEN:</b></p> <p>Wir überprüfen unsere gesamte Backup-Strategie und stellen für Sie sicher, dass alle relevanten Daten regelmäßig gesichert wurden und an welchen Stellen sie gespeichert wurden.</p>	<p style="text-align: center;"><b>3</b></p> <p style="text-align: center;"><b>DATEN-SICHERUNGENDURCHSUCHEN:</b></p> <p>Wir durchsuchen und strukturieren alle vorhandenen Daten-Sicherungen nach den benötigten und mit dem Kunden vorher definierten Daten, Dateien und Kunden-Datenbanken.</p>
<p style="text-align: center;"><b>4</b></p> <p style="text-align: center;"><b>DIVERSE SERVER DURCHSUCHEN:</b></p> <p>Wir analysieren und erstellen eine Liste aller Server, auf denen die relevanten Kunden-Daten und Kunden-Dateien gespeichert sein könnten.</p>	<p style="text-align: center;"><b>5</b></p> <p style="text-align: center;"><b>SQL-SERVER-DATEIEN:</b></p> <p>Wir führen die relevanten Daten aus den verschiedenen SQL-Server-Backups wieder zusammen, um eine <i>vollständige</i> und konsistente Daten-Sammlung zu generieren.</p>	<p style="text-align: center;"><b>6</b></p> <p style="text-align: center;"><b>DATEIEN ENTSCHLÜSSELN:</b></p> <p>Wirprüfen im Team, ob und wie die Dateien und Dokumente verschlüsselt wurden. Anschließend erfolgt das eigentliche Entschlüsseln der Dateien und Dokumente.</p>
<p style="text-align: center;"><b>7</b></p> <p style="text-align: center;"><b>DATEN STRUKTURIERT ABLEGEN:</b></p> <p>Wir legen die strukturierten Daten in sicheren und zugänglichen Formaten auf unseren internen Daten-Servern ab. Zur weiteren Verarbeitung.</p>	<p style="text-align: center;"><b>8</b></p> <p style="text-align: center;"><b>DATEN-ÜBERGABE IN TEILSCHRITTEN:</b></p> <p>Wir erstellen, gemeinsam mit unserem Kunden, einen Ablauf-Plan für die schrittweise Übergabe aller Kunden-Daten und Dateien.</p>	<p style="text-align: center;"><b>9</b></p> <p style="text-align: center;"><b>KONTROLLE DER DATEN-ÜBERGABE:</b></p> <p>Es erfolgt eine beidseitige Daten-Übergabe-Kontrolle in einem fest definierten Prüfungs-Zeitraum. Mit einer schriftlichen Abschluss-Bestätigung gelten die Daten als komplett und korrekt übertragen.</p>
<p style="text-align: center;"><b>10</b></p> <p style="text-align: center;"><b>NACH DATEN-ÜBERGABE LÖSCHEN:</b></p> <p>Wir erstellen, ein ganzheitliches Konzept zur sicheren Löschung der Daten aus unseren Systemen, Backup-Servern und sonstigen kooperierenden IT-Systemen.</p>	<p style="text-align: center;"><b>11</b></p> <p style="text-align: center;"><b>ENGPÄSSE UND HERAUSFORDERUNGEN:</b></p> <p>Es müssen diverse Engpässe einkalkuliert werden, darunter fallen Punkte wie das große Daten-Volumen, die Daten-Konsistenz, Sicherheits-Risiken und alle ergänzenden und rechtlichen Anforderungen und Vorgaben.</p>	<p style="text-align: center;"><b>12</b></p> <p style="text-align: center;"><b>WEITERES VON KUNDENSEITE:</b></p> <p style="text-align: center;">...</p>

## 4 Die Vorgehensweise / Reihenfolge und weitere Detail-Infos

Analog zur Webdarstellung (hier beispielhaft aus dem Webauftritt)



**(1) Vertrags-Prüfung und Datenbasis-Check**

**a. Vertragsprüfung**

- Wir überprüfen, gemeinsam mit unserem Kunden, den Vertrag, um sicherzustellen, dass alle vertraglichen Verpflichtungen bezüglich der Datenübergabe und Datenlöschung erfüllt werden.
- Ferner wird eine ggf. vertraglich vorgesehene Terminierung geprüft bzw. für die anstehende Umsetzung neu definiert.

**b. Datenidentifikation**

- Wir identifizieren für Sie, oder mit Ihnen gemeinsam, alle relevanten Daten, die übergeben und später gelöscht werden müssen
- Dazu gehören zum Beispiel Teilnehmer-Listen, Teilnahme-Bestätigungen, TN-E-Mails, Verträge, Referenten-Verträge, Anschreiben, Kosten-Berechnungen, Adressen, Kontodaten, Opt-IN/OUT, Excel-Listen, Word-Dateien, PDF-Dokumente, Bilder, Fotos, Skizzen, Hotelinfos und ggf. Rohdatendateien als SQL-Datenbank mit dazugehörigen, gespeicherten Prozeduren.

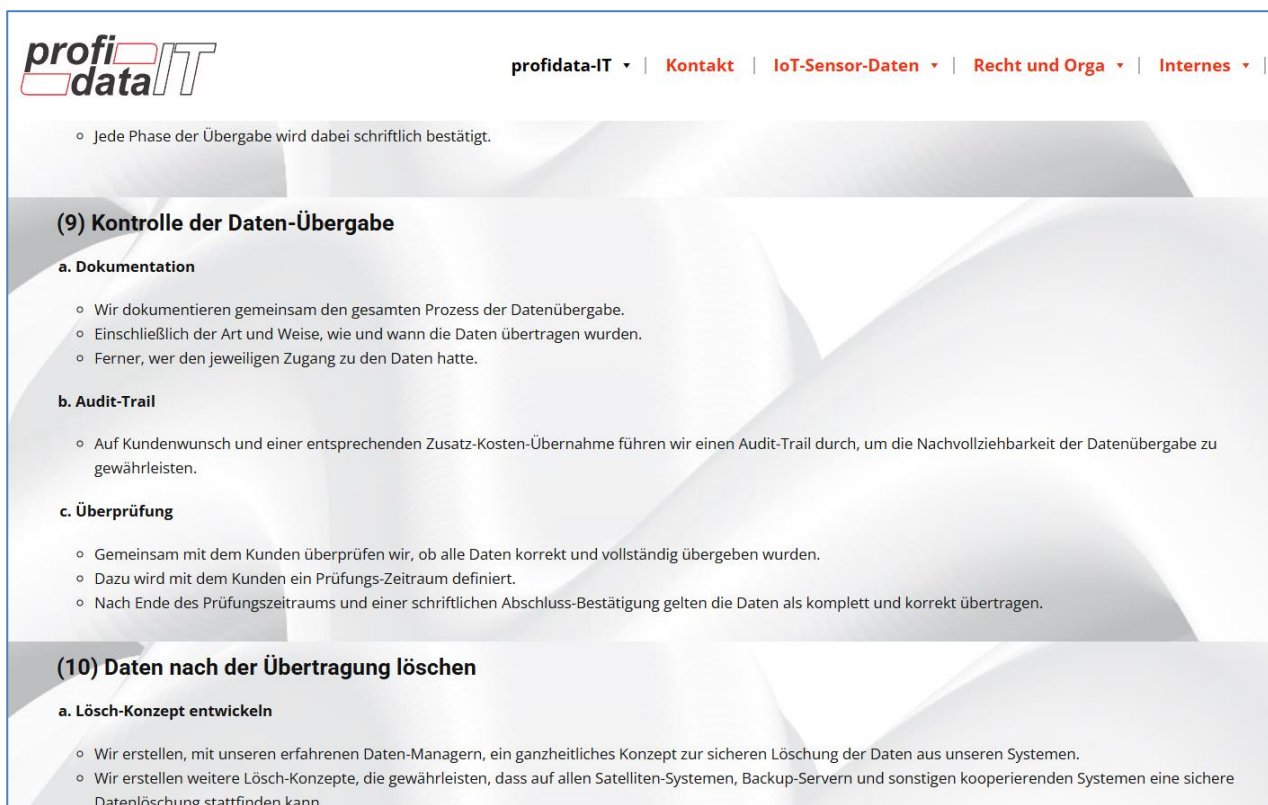
**c. Datenquellen durchsuchen**

- Um gründlich und rechtssicher vorzugehen, durchsuchen wir alle relevanten Datenquellen, einschließlich Backup-Server, verschlüsselte Acronis-Backups, Datenbanken, Dateisysteme, Ordnerstrukturen und Cloud-Speicher usw., um sicherzustellen, dass alle erforderlichen Daten erfasst und weiterbearbeitet werden können.

**(2) Backups durchsuchen**

**a. Backup-Strategie prüfen**

- Wir überprüfen unsere gesamte Backup-Strategie und stellen für Sie sicher, dass alle relevanten Daten regelmäßig gesichert wurden und wo sie anschließend abgelegt/gespeichert sind.



- Jede Phase der Übergabe wird dabei schriftlich bestätigt.

**(9) Kontrolle der Daten-Übergabe**

**a. Dokumentation**

- Wir dokumentieren gemeinsam den gesamten Prozess der Datenübergabe.
- Einschließlich der Art und Weise, wie und wann die Daten übertragen wurden.
- Ferner, wer den jeweiligen Zugang zu den Daten hatte.

**b. Audit-Trail**

- Auf Kundenwunsch und einer entsprechenden Zusatz-Kosten-Übernahme führen wir einen Audit-Trail durch, um die Nachvollziehbarkeit der Datenübergabe zu gewährleisten.

**c. Überprüfung**

- Gemeinsam mit dem Kunden überprüfen wir, ob alle Daten korrekt und vollständig übergeben wurden.
- Dazu wird mit dem Kunden ein Prüfungs-Zeitraum definiert.
- Nach Ende des Prüfungszeitraums und einer schriftlichen Abschluss-Bestätigung gelten die Daten als komplett und korrekt übertragen.

**(10) Daten nach der Übertragung löschen**

**a. Lösch-Konzept entwickeln**

- Wir erstellen, mit unseren erfahrenen Daten-Managern, ein ganzheitliches Konzept zur sicheren Löschung der Daten aus unseren Systemen.
- Wir erstellen weitere Lösch-Konzepte, die gewährleisten, dass auf allen Satelliten-Systemen, Backup-Servern und sonstigen kooperierenden Systemen eine sichere Datenlöschung stattfinden kann.

## 4.1 (1) Vertrags-Prüfung und Datenbasis-Check

### a. Vertragsprüfung

- Wir überprüfen, gemeinsam mit unserem Kunden, den Vertrag, um sicherzustellen, dass alle vertraglichen Verpflichtungen bezüglich der Datenübergabe und Datenlöschung erfüllt werden.
- Ferner wird eine ggf. vertraglich vorgesehene Terminierung geprüft bzw. für die anstehende Umsetzung neu definiert.

### b. Datenidentifikation

- Wir identifizieren für Sie, oder mit Ihnen gemeinsam, alle relevanten Daten, die übergeben und später gelöscht werden müssen
- Dazu gehören zum Beispiel Teilnehmer-Listen, Teilnahme-Bestätigungen, TN-E-Mails, Verträge, Referenten-Verträge, Anschreiben, Kosten-Berechnungen, Adressen, Kontodaten, Opt-IN/OUT, Excel-Listen, Word-Dateien, PDF-Dokumente, Bilder, Fotos, Skizzen, Hotelinfos und ggf. Rohdatendateien als SQL-Datenbank mit dazugehörigen, gespeicherten Prozeduren.

### c. Datenquellen durchsuchen

- Um gründlich und rechtssicher vorzugehen, durchsuchen wir alle relevanten Datenquellen, einschließlich Backup-Server, verschlüsselte Acronis-Backups, Datenbanken, Dateisysteme, Ordnerstrukturen und Cloud-Speicher usw., um sicherzustellen, dass alle erforderlichen Daten erfasst und weiterbearbeitet werden können.

## 4.2 (2) Backups durchsuchen

### a. Backup-Strategie prüfen

- Wir überprüfen unsere gesamte Backup-Strategie und stellen für Sie sicher, dass alle relevanten Daten regelmäßig gesichert wurden und wo sie anschließend abgelegt/gespeichert sind.

### b. Backups durchsuchen

- Anschließend durchsuchen wir alle vorhandenen Backups nach allen benötigten Daten.
- Dies kann sowohl lokale als auch die beschriebenen Cloud-Backups umfassen.

### c. Datenwiederherstellung

- Wir versuchen nun auch sicher zu stellen, dass alle relevanten Daten aus den Backups wiederhergestellt werden können.
- Bei technischen Problemen werden wir diese so gut wie möglich beheben.

## 4.3 (3) Daten-Sicherungen durchsuchen

### a. Sicherungs-Protokolle prüfen

- Zuerst überprüfen wir die vorhandenen Sicherungs-Protokolle der verfügbaren Datensicherungen, um sicherzustellen, dass alle relevanten Daten korrekt gesichert wurden.

### b. Sicherungen durchsuchen

- Wir durchsuchen und strukturieren alle vorhandenen Sicherungen nach den benötigten und mit dem Kunden vorher definierten Daten, Dateien und Kunden-Datenbanken.

### c. Daten-Wiederherstellung

- Wir vergewissern uns und Stellen anschließend sicher, dass alle relevanten Daten aus den Sicherungen wiederhergestellt werden können.

## 4.4 (4) Die verschiedenen Server durchsuchen

### a. Server-Liste erstellen

- Wir analysieren und erstellen eine Liste aller Server, auf denen relevante Daten gespeichert sein könnten.
- Hierbei handelt es sich auch um kommerzielle Backup-Systeme und intern/extern gehostete „NAS“-Systeme.
- Diese Server-Liste dient unseren Kollegen als Basis für das weitere Daten-Management.

### b. Server-Liste durchsuchen

- Mit der o.a. internen Server-Liste (IP-Adressen, Kennwörter, Verschlüsselung, Daten-Ablage-Struktur, Firewall etc.) durchsuchen wir jeden Server nach den benötigten Kunden-Daten.
- Dies kann sowohl die physischen als auch etliche virtuelle Server umfassen.

### c. Daten-Extraktion

- Es wird erfahrungsgemäß in vielen Fällen notwendig sein die relevanten Daten auf den Servern (oder einem identischen Puffer-System) zu extrahieren.
- Das ist für uns ein sehr zeitaufwendiger und daten-kritischer Prozess.
- Anschließend erfolgt eine Prüfung, ob nach dem Extrahieren alle relevanten Daten von den Servern wiederhergestellt, vollständig und korrekt sind

## 4.5 (5) SQL-Server-Dateien zusammenführen und Backups wiederherstellen

### a. SQL-Server-Backups prüfen

- Wir überprüfen alle relevanten Backups der unterschiedlichen, verwendeten SQL-Server-Datenbanken.
- Hierbei beachten und verarbeiten wir die unterschiedlichen Backup-Varianten; Vollbackup, inkrementelles Backup und differenzielles Backup.

### b. SQL-Daten zusammenführen

- Wir führen die relevanten Daten aus den verschiedenen SQL-Server-Backups wieder zusammen, um eine *vollständige* Datensammlung zu erstellen.

### c. SQL-Daten wiederherstellen

- Wir testen die kumulierten SQL-Backups und stellen damit sicher, dass alle relevanten Daten aus den SQL-Server-Backups wiederhergestellt werden können.

## 4.6 (6) Dateien und Dokumente entschlüsseln

### a. Verschlüsselung prüfen

- Wir prüfen im Team, ob und wie die Dateien und Dokumente verschlüsselt wurden.
- Da der Daten(be)stand bis zu 10 Jahre zurück liegen kann, sind hierbei die unterschiedlichsten Verschlüsselungen und Verschlüsselungs-Systeme zu erwarten.

### b. Entschlüsselungs-Schlüssel und Authentifikations-Methoden bereitstellen

- Wir versuchen sicher zu stellen, dass alle notwendigen Schlüssel und Methoden zur Entschlüsselung der Dateien und Dokumente zur Verfügung stehen.

### c. Dateien entschlüsseln

- Anschließend erfolgt das eigentliche Entschlüsseln der Dateien und Dokumente, um sicherzustellen, dass sie anschließend vom Auftraggeber lesbar und vollständig sind.

## 4.7 (7) Daten strukturieren und lokal ablegen

- a. **Daten-Strukturierung**
  - Wir organisieren und dokumentieren die Daten in einer logischen Struktur, z.B. nach Veranstaltung, Teilnehmer oder Datum.
  - Die Organisation der eigentlichen VA- und TN-Daten erfolgt in SQL-Tabellen mit entsprechenden Beziehungen und u.a. Primär-Schlüsseln.
- b. **Daten-Validierung**
  - Die so generierten Datenstrukturen und Daten-Tabellen werden auf ihre Richtigkeit, Konsistenz und ggf. referentielle Integritäten geprüft.
- c. **Daten-Ablage**
  - Wir legen danach die strukturierten Basis-Daten in einem sicheren und zugänglichen Format auf unseren internen Daten-Servern, zur weiteren Verarbeitung und Verteilung, ab.

## 4.8 (8) Daten-Übergabe in Teilschritten

- a. **Übergabe-Plan erstellen**
  - Wir erstellen, gemeinsam mit unserem Kunden, einen Ablauf-Plan für die schrittweise Übergabe der Daten.
  - Dieser Übergabe-Plan wird schriftlich erstellt und von beiden Parteien bestätigt.
- b. **Teil-Schritte definieren**
  - Gemeinsam werden auch die einzelnen Schritte der Datenübergabe definiert.
  - z.B. nach Datenkategorien oder Zeiträumen.
- c. **Daten-Übergabe durchführen**
  - Wir führen die Daten-Übergabe, in den vorab definierten Teilschritten, durch.
  - Jede Phase der Übergabe wird dabei schriftlich bestätigt.

## 4.9 (9) Kontrolle der Daten-Übergabe

- a. **Dokumentation**
  - Wir dokumentieren gemeinsam den gesamten Prozess der Datenübergabe.
  - Einschließlich der Art und Weise, wie und wann die Daten übertragen wurden.
  - Ferner, wer den jeweiligen Zugang zu den Daten hatte.
- b. **Audit-Trail**
  - Auf Kundenwunsch und einer entsprechenden Zusatz-Kosten-Übernahme führen wir einen Audit-Trail durch, um die Nachvollziehbarkeit der Datenübergabe zu gewährleisten.
- c. **Überprüfung**
  - Gemeinsam mit dem Kunden überprüfen wir, ob alle Daten korrekt und vollständig übergeben wurden.
  - Dazu wird mit dem Kunden ein Prüfungs-Zeitraum definiert.
  - Nach Ende des Prüfungszeitraums und einer schriftlichen Abschluss-Bestätigung gelten die Daten als komplett und korrekt übertragen.



## 4.10 (10) Daten nach der Übertragung löschen

### a. Lösch-Konzept entwickeln

- Wir erstellen, mit unseren erfahrenen Daten-Managern, ein ganzheitliches Konzept zur sicheren Löschung der Daten aus unseren Systemen.
- Wir erstellen weitere Lösch-Konzepte, die gewährleisten, dass auf allen Satelliten-Systemen, Backup-Servern und sonstigen kooperierenden Systemen eine sichere Datenlöschung stattfinden kann.

### b. Daten-Löschung durchführen

- Wir nutzen kommerzielle und individuelle Tools und Methoden, um alle Kunden-Daten sicher zu löschen.
- Dieses wird auch das Überschreiben der Daten und die physische Zerstörung von Backup- Speichermedien umfassen.

### c. Lösch-Bestätigung

- Es wird mit dem Kunden ein Daten-Lösch-Zeitraum definiert.
- Nach Ende des eigentlichen Lösch-Vorgangs und einer schriftlichen Abschluss-Bestätigung gelten die Daten als komplett und korrekt gelöscht.

## 4.11 (11) Potenzielle Engpässe und Herausforderungen

### a. Daten-Volumen

- Die großen und langjährig angefallenen Datenmengen werden die Datenaufbereitung und -übertragung verlangsamen.
- Es müssen ausreichend Zeit und Ressourcen eingeplant und bereitgestellt werden.

### b. Daten-Konsistenz

- Die unterschiedlichen Datenformate und -quellen werden zu Inkonsistenzen führen.
- Eine gründliche und professionelle Daten-Bereinigung, Daten-Aufbereitung und Daten-Management sind für das Ergebnis fundamental entscheidend und eine Voraussetzung.

### c. Sicherheits-Risiken

- Die sichere Übertragung und Zwischen-Speicherung der Daten ist essenziell, um Datenschutzverletzungen zu vermeiden.
- Gerade in der Daten-Aufbereitungs-Phase, in denen u.a. die Daten unverschlüsselt weiterverarbeitet werden, muss mit allergrößter Sorgfalt vorgegangen werden.
- Nach Ende des eigentlichen Lösch-Vorgangs und einer schriftlichen Abschluss-Bestätigung gelten die Daten als komplett und korrekt gelöscht.

### d. Rechtliche Anforderungen

- Während des gesamten Workflows müssen beide Vertrags-Seiten sicherstellen, dass alle Schritte im Einklang mit der DSGVO und anderen relevanten Datenschutzgesetzen erfolgen.

## 4.12 (12) Weiteres von Kundenseite

### a. ...

- ...