

---

## NUTZUNGSVERTRAG GEOVERIS

---

### ZWISCHEN:

- (1) **VdS Schadenverhütung GmbH**, Amsterdamer Str. 174, 50735 Köln

– "VdS" –

- (2) der in der Annahmeerklärung von VdS bezeichneten natürlichen oder juristischen Person

– "Kunde" –

Die Parteien zu (1) bis (2) werden nachfolgend auch gemeinsam als die "**Parteien**" und einzeln als eine "**Partei**" bezeichnet.

### VORBEMERKUNG

- (A) VdS betreibt in ihrem Geschäftsbereich „GeoExpertise“ u.a. das Informationsangebot "GeoVeris", das die bislang unter den Bezeichnungen "ZÜRS Solutions" und "Meteo-Info" betriebenen Angebote zur Abfrage von Geoinformationen und meteorologischer Informationen ("GeoVeris-Informationen" oder "GVI") umfasst.
- (B) Der Kunde ist ein Unternehmen / Einzelunternehmer, das/der im Rahmen seiner eigenen Geschäftstätigkeit in den Bereichen Finanzdienstleistungen, Versicherungen oder Immobilien auf Informationen zu orts- oder objektbezogenen Risiken angewiesen ist.

## 1. ABSCHLUSS DIESES VERTRAGES

1.1 Dieser Nutzungsvertrag kommt zustande, wenn

1.1.1 der Kunde auf einem von VdS angebotenen Weg, insbesondere über die Website [www.vds.de/](http://www.vds.de/) (Neukundenregistrierung GeoVeris), unter Angabe der hierfür vorgegebenen Daten ein Angebot auf Abschluss dieses Nutzungsvertrages abgibt und

1.1.2 VdS dieses Angebot durch ausdrückliche Erklärung gegenüber dem Kunden bestätigt.

1.2 VdS ist berechtigt, ein auf den Abschluss dieses Nutzungsvertrages gerichtetes Angebot des Kunden ohne Angabe von Gründen abzulehnen.

## 2. VERTRAGSGEGENSTAND

2.1 Mit Abschluss dieses Nutzungsvertrages verpflichtet sich VdS gegenüber dem Kunden nach Maßgabe dieses Nutzungsvertrags und der Nutzungsbedingungen GeoVeris (**Anlage 1** zu diesem Nutzungsvertrag) zur Bereitstellung von GeoVeris und

zur Einräumung bestimmter Nutzungsrechte an den GeoVeris-Informationen. Die Parteien schließen ergänzend die als **Anlage 2** beigefügte Vereinbarung über Auftragsverarbeitung.

- 2.2 GeoVeris wird dem Kunden über das Web-Interface von VdS (unter [www.geo-veris.de](http://www.geo-veris.de) und/oder einer anderen von VdS mitgeteilten Adresse) zur Verfügung gestellt.
- 2.3 Nach Abschluss dieses Nutzungsvertrages richtet VdS einen Zugang für den Kunden ein und stellt dem Kunden die dazugehörigen Log-In-Daten zur Verfügung. Auf Anfrage des Kunden kann VdS für den Kunden weitere Zugänge (insbesondere für einzelne vom Kunden unter Berücksichtigung der Nutzungsbedingungen definiert und VdS mitgeteilte Berechtigte Nutzer) einrichten.
- 2.4 Wenn und soweit der Kunde einen für ihn eingerichteten Zugang als "Sammelzugang" verwendet (also einen solchen Zugang durch mehrere Berechtigte Nutzer nutzen lässt), ist eine personalisierte Kontrolle des Zugriffs auf GeoVeris und entsprechende Auswertungen nicht möglich. Jede Nutzung von GeoVeris über einen vom Kunden als solchen verwendeten Sammelzugang gilt als Nutzung von GeoVeris durch den Kunden.
- 2.5 Der Kunde hat die Möglichkeit, über GeoVeris die in der Leistungsbeschreibung spezifizierten GeoVeris-Informationen auszuwählen und abzurufen. Der Abruf von GeoVeris-Informationen ist kostenpflichtig; die Vergütung für den Abruf von GeoVeris-Informationen ergibt sich aus der Preisliste. Leistungsbeschreibung und Preisliste werden dem Kunden mit Annahme seines Angebots auf Abschluss des Nutzungsvertrages und über GeoVeris zur Verfügung gestellt.
- 2.6 Der Kunde verpflichtet zur Einhaltung des Nutzungsvertrages und der Nutzungsbedingungen sowie zur Zahlung der Vergütung für die von ihm abgerufenen GeoVeris-Informationen.

### **3. UMFANG DER ZULÄSSIGEN NUTZUNG DURCH DEN KUNDEN**

- 3.1 Der Kunde wird GeoVeris-Informationen ausschließlich im Rahmen seiner eigenen Geschäftstätigkeit zur Vorbereitung oder Durchführung eines rechtlich zulässigen Geschäftsvorgangs mit Bezug zu dem durch die GeoVeris-Informationen beschriebenen orts- oder objektbezogenen Risiko und zur Prüfung oder Bewertung dieses Risikos abrufen ("**Berechtigte Nutzung**").
- 3.2 Der Kunde wird den Zugriff auf GeoVeris und den Abruf von GeoVeris-Informationen ausschließlich eigenen Mitarbeitern gestatten ("**Berechtigte Nutzer**"), die der Kunde über die Regelungen dieses Nutzungsvertrages und der Nutzungsbedingungen – insbesondere im Hinblick auf den Umfang der Berechtigten Nutzung und

der zulässigen Weitergabe an Berechtigte Empfänger – informiert und zu der Einhaltung dieser Vorgaben verpflichtet hat.

- 3.3 Der Kunde wird GeoVeris-Informationen außer in den in den Nutzungsbedingungen ausdrücklich genannten Fällen ausschließlich als notwendigen Bestandteil von Informationen und Unterlagen des Kunden an eigene Endkunden oder (potentielle) Geschäftspartner im Zusammenhang mit einem konkreten Geschäftsvorfall ("**Berechtigte Empfänger**") weitergeben oder diesen gegenüber offenlegen wird; eine separate Weitergabe oder Offenlegung von GeoVeris-Informationen außerhalb der Berechtigten Nutzung ist nicht zulässig.

#### **4. NUTZUNGSBEDINGUNGEN, VEREINBARUNG ÜBER AUFTRAGSVERARBEITUNG**

Für die Bereitstellung von GeoVeris durch VdS sowie für die Nutzung durch den Kunden gelten Nutzungsbedingungen GeoVeris in Anlage 1. Mit Abschluss dieses Nutzungsvertrages schließen die Parteien zudem die Vereinbarung über Auftragsverarbeitung GeoVeris in Anlage 2.

# Anlage 1

## Nutzungsbedingungen GeoVeris

### 1. Anwendungsbereich der Nutzungsbedingungen

- 1.1 Diese Nutzungsbedingungen gelten für die Nutzung von GeoVeris durch Unternehmen, soweit diese mit VdS einen Nutzungsvertrag über die Nutzung von GeoVeris (jeweils oder zusammen „**Nutzungsvertrag**“) abgeschlossen haben („**Kunde**“).
- 1.2 Abweichende oder ergänzende Bedingungen eines Kunden finden keine Anwendung. Dies gilt auch dann, wenn ein Kunde VdS auf solche abweichenden oder ergänzenden Bedingungen ausdrücklich hingewiesen hat.

### 2. Leistungen von VdS

- 2.1 VdS verpflichtet sich gegenüber dem Kunden, die in diesen Nutzungsbedingungen geregelten Nutzungsrechte an GeoVeris und den aus GeoVeris gemäß dem Nutzungsvertrag abrufbaren Daten einzuräumen und GeoVeris dem Kunden über das Internet zugänglich zu machen.
- 2.2 Funktionalitäten und Leistungsumfang von GeoVeris, die für GeoVeris verwendete Datenbasis sowie die vom Kunden zu schaffenden technischen Voraussetzungen ergeben sich aus der Leistungsbeschreibung.
- 2.3 Der Anspruch auf Nutzung von GeoVeris besteht nur im Rahmen des aktuellen Stands der Technik und der VdS von Dritten eingeräumten Nutzungsrechte an Daten und Funktionalitäten. VdS behält sich vor, den Zugang zu sowie die Funktionalitäten und Nutzung von GeoVeris zeitweilig zu beschränken, wenn dies im Hinblick auf Kapazitätsgrenzen, die Sicherheit oder Integrität der technischen Infrastruktur oder zur Durchführung technischer Maßnahmen oder aufgrund der Beendigung zeitlich beschränkter Nutzungsmöglichkeiten (etwa für Analyse- und Kartendienste) erforderlich ist. VdS wird den Kunden soweit möglich über geplante Beschränkungen des Zugangs, von Funktionalitäten und/oder der Nutzung innerhalb von GeoVeris oder durch Mitteilung per E-Mail informieren.
- 2.4 VdS weist ausdrücklich darauf hin, dass in GeoVeris eine Vielzahl von unterschiedlichen Ausgangsdaten verschiedener Datenlieferanten eingeflossen sind, die z.T. mit unterschiedlichen Datenmodellen und –formaten gearbeitet haben und dass Gutachten von Dritten im Auftrag von VdS für den Lizenznehmer erstellt werden. Aufgrund des erheblichen Umfangs unterschiedlicher Ausgangsdaten ist es nicht unwahrscheinlich, dass diese Daten und die über GeoVeris abgerufenen Informationen Ungenauigkeiten und Fehler enthalten. VdS hat die Dienstleister für die Bereitstellung der Ausgangsdaten und für die Erstellung von Gutachten sorgfältig ausgewählt, hat aber auf Erhebung bzw. Erstellung von Ausgangsdaten ebenso wenig

Einfluss wie auf die Vollständigkeit und Richtigkeit der VdS zur Verfügung gestellten Daten. Zudem können künftig in GeoVeris mathematische Verfahren einbezogen werden, mit denen versucht wird, bestimmte zukünftige Naturereignisse vorherzusagen; diese Verfahren gewährleisten gleichwohl – wie jede Prognosetätigkeit – nicht, dass die Prognose auch tatsächlich eintritt. Darüber hinaus weist VdS zusätzlich darauf hin, dass sich die für meteorologische Anfragen und Analysen verwendeten Ausgangsdaten nicht stets auf meteorologische Parameter an dem vom Lizenzgeber angegebenen Ort beziehen, sondern ggf. auf Ausgangsdaten der nächstgelegenen Wetterstation(en) oder sonstiger Erfassungseinrichtung(en). Es ist nach alledem nicht unwahrscheinlich, dass die von GeoVeris ausgegebenen GeoVeris-Informationen von den tatsächlichen Gegebenheiten und Risiken abweichen. GeoVeris bildet auch nicht die Wirklichkeit ab, sondern soll lediglich einen unverbindlichen Anhaltspunkt für eine erste Orientierung geben. Insoweit gewährleistet VdS nicht die Fehlerfreiheit der in GeoVeris verarbeiteten Daten und der GeoVeris-Informationen, die durch den Berechtigte Nutzer eigenständig zu prüfen sind.

- 2.5 VdS ist berechtigt, den Zugang des Kunden und/oder einzelner oder mehrerer Berechtigter Nutzer zu GeoVeris zu sperren, wenn bei VdS die berechtigte Annahme besteht, dass der Kunde gegen den Nutzungsvertrag verstößt oder die dem Kunden eingeräumte Nutzungsmöglichkeit missbräuchlich, z.B. durch unbefugte Dritte, genutzt wird. VdS informiert den Kunden über die Sperrung nach ihrer Wahl schriftlich, in Textform oder beim Zugriff auf GeoVeris. Bestätigt sich die Annahme von VdS nicht, wird VdS den gesperrten Zugang wieder freigeben. Dem Kunden bleibt der Nachweis vorbehalten, dass der angenommene Verstoß nicht vorliegt. Für die Dauer einer berechtigten Sperrung von Anwendungen wird VdS von ihrer Leistungspflicht frei. Dem Kunden stehen aufgrund einer berechtigten Sperrung keine Ansprüche gegen VdS zu.

### **3. Einräumung von Nutzungsrechten**

- 3.1 VdS räumt dem Kunden während der Laufzeit des Nutzungsvertrages das zeitlich beschränkte, nicht ausschließliche, nicht übertragbare Recht ein, die über GeoVeris durch Berechtigte Nutzer abgerufenen GeoVeris-Informationen für Zwecke der Berechtigten Nutzung im Rahmen der in GeoVeris vorgesehenen Funktionalitäten und Nutzungsmöglichkeiten und unter Beachtung dieser Nutzungsbedingungen zu verarbeiten und zu nutzen.

- 3.2 Die gemäß Ziff. 3.1 eingeräumten Nutzungsrechte für GeoVeris schließen das nicht ausschließliche Recht des Kunden ein, die GeoVeris-Informationen im Rahmen der eigenen Geschäftstätigkeit für die Berechtigte Nutzung zu verwenden bzw. durch Berechtigte Nutzer verwenden zu lassen sowie sie Berechtigten Empfängern zugänglich zu machen, wenn und soweit für die Berechtigte Nutzung erforderlich ist.

- 3.3 Es ist ferner ausdrücklich untersagt, GeoVeris-Informationen außerhalb der Berechtigten Nutzung zu verarbeiten und zu nutzen oder GeoVeris-Informationen an andere als die im Nutzungsvertrag bezeichneten Berechtigten Empfänger weiterzugeben. Sind im Nutzungsvertrag keine Berechtigten Empfänger bezeichnet, ist die Weitergabe von GeoVeris-Informationen nicht zulässig. Unzulässig ist es insbesondere, die GeoVeris-Informationen zu veröffentlichen, öffentlich zugänglich zu machen oder unter Verwendung der GeoVeris-Informationen eigene Datenbanken, Informationsdienste oder vergleichbare Informationssammlungen anzulegen und/oder diese zu vervielfältigen, zu verbreiten, zu veröffentlichen oder öffentlich zugänglich zu machen.
- 3.4 VdS ist berechtigt, die Nutzung bestimmter Bestandteile der GeoVeris-Informationen mit ergänzenden Nutzungsbeschränkungen zu versehen, insbesondere aufgrund entsprechender Anforderungen von Lizenzgebern der für die GeoVeris-Informationen verwendeten Daten. Informationen zu ergänzenden Nutzungsbeschränkungen werden dem Kunden bzw. dem Berechtigten Nutzer in Schrift- oder Textform oder innerhalb von GeoVeris mitgeteilt.
- 3.5 Bei der Berechtigten Nutzung ist auf die Quelle hinzuweisen: (aus: GeoVeris, © VdS). Soweit innerhalb von GeoVeris und/oder auf ausgegebenen GeoVeris-Informationen darauf hingewiesen wird, dass auch weitere Quellenangaben anzubringen sind, ist dies zu beachten.
- 3.6 Sämtliche vorgenannten Nutzungsrechte werden zeitlich beschränkt eingeräumt.
- 3.7 Die Rechteeinräumung endet
- 3.7.1 mit Beendigung des Nutzungsvertrages (insbesondere durch eine Kündigung durch VdS oder dem Kunden);
- 3.7.2 wenn VdS gegenüber dem Kunden schriftlich oder in Textform anzeigt, dass die Nutzung aus rechtlichen Gründen (insbesondere aufgrund von Nutzungsbeschränkungen durch Inhaber von Rechten an den für GeoVeris verwendeten Daten und/oder an der Plattform oder anderen technischen Komponenten, die für den Betrieb von GeoVeris notwendig sind) nicht mehr erfolgen darf; dies kann sich auf einzelne oder alle Komponenten von GeoVeris und/oder der GeoVeris-Informationen beziehen; oder
- 3.7.3 wenn ergänzende Bedingungen für die zeitliche Beschränkung der Rechteeinräumung eintreten, über die VdS den Nutzer innerhalb von GeoVeris (v.a. vor dem Abruf von GeoVeris-Informationen) informiert hat.
- 3.8 Mit Beendigung der Rechteeinräumung ist der Kunde zur Deaktivierung der bei ihm eingerichteten Abrufmöglichkeit und zur Löschung der entsprechenden beim Kunden (einschließlich aller Berechtigten Nutzer) vorhandenen GeoVeris-Informationen und datenschutzkonformer Vernichtung sonstiger Produkte, Datenträger

oder Dokumentationen (einschließlich etwaiger Sicherungskopien) verpflichtet. Hiervon ausgenommen sind bereits erstellten Vervielfältigungen, die aufgrund gesetzlicher oder vertraglicher Aufbewahrungspflichten (z.B. als Bestandteil einer Beratungsdokumentation) weiter aufzubewahren sind. Der Kunde ist auf Anfrage von VdS verpflichtet, die Löschung der GeoVeris-Informationen und der sonstigen Produkte, Datenträger oder Dokumentationen (einschließlich etwaiger Sicherungskopien) schriftlich zu bestätigen.

- 3.9 VdS behält sich vor, die Einhaltung der vorstehenden Nutzungsbeschränkungen durch geeignete Maßnahmen (insbesondere die Implementierung von Testdaten in den GeoVeris-Datenbestand) zu überprüfen.

#### **4. Nutzung nur durch berechtigte Nutzer**

- 4.1 Der Kunde stellt durch geeignete technische und organisatorische Maßnahmen sicher, dass die Nutzung von GeoVeris und der GeoVeris-Informationen nur durch Berechtigte Nutzer erfolgen kann.
- 4.2 Der Kunde wird insbesondere sicherstellen, dass jeder Berechtigte Nutzer GeoVeris nur nach Eingabe einer Benutzerkennung und eines Passwortes nutzen kann.
- 4.3 Darüber hinaus hat der Kunde Berechtigte Nutzer vor dem erstmaligen Zugang zu GeoVeris ausdrücklich auf die Einhaltung der Regelungen des Nutzungsvertrags zu verpflichten und VdS die Einhaltung dieser Verpflichtung auf Verlangen nachzuweisen. VdS behält sich ausdrücklich vor, den Kunden bzw. den Berechtigten Nutzern eine elektronische Lösung zur Abgabe der Erklärung (etwa im Rahmen des GeoVeris-Zugangs) zur Verfügung zu stellen.

#### **5. Vergütung**

- 5.1 Der Kunde ist verpflichtet, für die Nutzung von GeoVeris nach Maßgabe des Nutzungsvertrages das in der Preisliste festgelegte Entgelt an VdS zu zahlen. Sofern nicht anders angegeben, sind sämtliche Preisangaben Nettopreise ohne die gesetzliche Umsatzsteuer.
- 5.2 VdS ist berechtigt, die Preisliste anzupassen und wird den Kunden hierüber unter Beachtung einer Frist von drei Monaten schriftlich oder in Textform informieren. Der Kunde ist berechtigt, diesen Vertrag unter Beachtung einer Frist von zwei Wochen zu dem von VdS in der angepassten Preisliste genannten Anpassungstermin zu kündigen.
- 5.3 VdS ist berechtigt, die angefallenen Entgelte für jeden Abruf von GeoVeris-Informationen unmittelbar nach dem Abruf gegenüber dem Kunden in Rechnung zu stellen.

5.4 Entgelte sind innerhalb von 14 Tagen nach Rechnungseingang auf das in der Rechnung angegebene Konto zur Zahlung fällig, sofern in der Rechnung von VdS keine längere Zahlungsfrist angegeben wird.

## **6. Vertragsdauer, Kündigung**

6.1 Der Nutzungsvertrag kommt mit Annahme des auf den Abschluss des Nutzungsvertrages gerichteten Angebots durch ausdrückliche Erklärung von VdS zustande und wird auf unbestimmte Zeit geschlossen. Während der Laufzeit kann der Nutzungsvertrag von jeder Partei unter Beachtung einer Kündigungsfrist von einem Monat zum Ende eines jeden Kalendermonats gekündigt werden.

6.2 Das Recht zur Kündigung aus wichtigem Grund bleibt unberührt. Ein wichtiger Grund liegt insbesondere dann vor, wenn

6.2.1 der zwischen VdS und dem von VdS beauftragten Dienstleister für den Betrieb von GeoVeris abgeschlossene Vertrag, gekündigt, aufgehoben oder auf andere Weise beendet wird,

6.2.2 der zwischen VdS und dem Gesamtverband der Deutschen Versicherungswirtschaft e.V. (GDV) bestehende Vertrag über den Betrieb von GeoVeris gekündigt, aufgehoben oder auf andere Weise beendet wird,

6.2.3 eine staatliche Stelle die weitere Nutzung von für den Betrieb von GeoVeris relevanten Daten aus Gründen der öffentlichen Sicherheit mit sofortiger Wirkung untersagt,

6.2.4 die Nutzung der für den Betrieb von GeoVeris relevanten Daten (insbesondere aufgrund von Nutzungsbeschränkungen durch Inhaber von Rechten an den für GeoVeris verwendeten Daten) nicht mehr erfolgen darf,

6.2.5 eine der beiden Parteien den Vertrag schwerwiegend verletzt und diese Vertragsverletzung nicht innerhalb einer angemessenen Frist nach Abmahnung durch die andere Partei behebt, wobei § 323 Abs. 2 BGB für die Entbehrlichkeit der Abmahnung entsprechend gilt;

6.2.6 sich die Vermögensverhältnisse einer Partei so verschlechtern, dass die Erreichung des Vertragszwecks gefährdet ist;

6.2.7 oder über das Vermögen einer Partei ein Insolvenzverfahren eröffnet oder ein Antrag auf Eröffnung eines solchen gestellt wird und die offenbare Unbegründetheit des Antrags nicht unverzüglich nachgewiesen wird.

6.3 Die Kündigung hat schriftlich oder in Textform zu erfolgen.

6.4 Die durch diesen Vertrag übertragenen Nutzungsrechte fallen nach Ende der Vertragslaufzeit ohne weitere Rechtshandlung an VdS zurück. Dies gilt auch im Hinblick auf etwaige Rechte an Sicherungskopien. Ein Recht zur weiteren Nutzung von GeoVeris besteht ab dem Ende der Vertragslaufzeit nicht mehr.

## 7. Haftung

7.1 VdS haftet für Schäden, außer im Fall der Verletzung wesentlicher Vertragspflichten, nur, wenn und soweit VdS, ihren gesetzlichen Vertreter, leitenden Angestellten oder sonstigen Erfüllungsgehilfen Vorsatz oder grobe Fahrlässigkeit zur Last fällt. Im Fall der Verletzung wesentlicher Vertragspflichten haftet VdS für jedes schuldhaftes Verhalten ihrer gesetzlichen Vertreter, leitender Angestellter oder sonstiger Erfüllungsgehilfen, wobei der Begriff der „wesentlichen Vertragspflichten“ solche Pflichten bezeichnet, deren Erfüllung die ordnungsgemäße Durchführung des Vertrags überhaupt erst ermöglicht, auf deren Einhaltung die Mitglieder regelmäßig vertrauen dürfen und deren Verletzung die Erreichung des Vertragszwecks gefährdet.

7.2 Außer bei Vorsatz oder grober Fahrlässigkeit gesetzlicher Vertreter, leitender Angestellter oder sonstiger Erfüllungsgehilfen, ist die Haftung von VdS der Höhe nach auf die bei Vertragsschluss typischerweise vorhersehbaren Schäden begrenzt.

7.3 Eine Haftung für den Ersatz mittelbarer Schäden, insbesondere für den entgangenen Gewinn, besteht nur bei Vorsatz oder grober Fahrlässigkeit gesetzlicher Vertreter, leitender Angestellter oder sonstiger Erfüllungsgehilfen von VdS.

7.4 Die vorgenannten Haftungsausschlüsse gelten nicht im Fall der Übernahme ausdrücklicher Garantien durch VdS und für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit sowie im Fall zwingender gesetzlicher Regelungen.

## 8. Datenschutz

8.1 Die Nutzung von GeoVeris (einschließlich der GeoVeris-Informationen) unterliegt datenschutzrechtlichen Beschränkungen. Die GeoVeris-Informationen werden nach Auffassung der Aufsichtsbehörden für den Datenschutz durch ihre Zuordnung zu einem bestimmten Objekt oder einem bestimmten Punkt zu personenbezogenen Daten im Sinne der DSGVO, spätestens, wenn sie darüber einer bestimmten Person zugeordnet werden können.

8.2 Vor diesem Hintergrund schließen die Parteien mit Abschluss des Nutzungsvertrages zugleich die dem Nutzungsvertrag als **Anlage 2** beigefügte Vereinbarung über Auftragsverarbeitung ab.

8.3 Der Kunde verpflichtet sich zudem, die datenschutzrechtlichen Bestimmungen bei seiner Nutzung von GeoVeris zu beachten. Danach dürfen nur die zur Wahrung

berechtigter Interessen (insbesondere zur Einschätzung und Kalkulation von objekt- oder ortsbezogenen Ereignissen und Risiken) erforderlichen Daten einem Objekt oder einer Fläche zugeordnet werden. Die GeoVeris-Informationen dürfen nicht zu anderen Zwecken genutzt werden, insbesondere nicht zur Erstellung georeferenzierter soziodemografischer Profile für den Rückschluss auf einzelne Personen. Der Kunde verpflichtet sich, die datenschutzrechtlichen Anforderungen in seinem Verantwortungsbereich insbesondere durch technische und organisatorische Maßnahmen sicherzustellen.

## **9. Schlussbestimmungen**

- 9.1 Der Nutzungsvertrag und diese Nutzungsbedingungen unterliegen jeweils dem Recht der Bundesrepublik Deutschland unter Ausschluss des Kollisionsrechts. Gerichtsstand ist, soweit rechtlich zulässig, Köln.
- 9.2 Änderungen oder Ergänzungen dieses Nutzungsvertrages und dieser Nutzungsbedingungen– inklusive dieser Textformklausel – bedürfen zu ihrer Wirksamkeit der Textform. Mitteilungen können, soweit nicht ausdrücklich Abweichendes vereinbart ist, per E-Mail an die von den Parteien zu diesem Zweck zu benennenden E-Mail-Adressen übermittelt werden. Mündliche und telefonische Übermittlung sind hingegen nicht ausreichend.
- 9.3 Die Nichtigkeit einzelner Bestimmungen des Nutzungsvertrages oder dieser Nutzungsbedingungen berührt die Wirksamkeit der anderen Bestimmungen nicht. Anstelle unwirksamer Bestimmungen treten in erster Linie solche, die den unwirksamen Bestimmungen in rechtswirksamer Weise wirtschaftlich am ehesten entsprechen. Gleiches gilt für eventuelle Regelungslücken.

## Anlage 2

### Vereinbarung über Auftragsverarbeitung GeoVeris

#### 1. **Gegenstand der Vereinbarung über Auftragsverarbeitung**

Da die Erbringung der Vertragsleistungen unter dem Nutzungsvertrag durch VdS (nachfolgend auch "**Auftragnehmer**") auch die Verarbeitung personenbezogener Daten im Auftrag und gemäß den Anweisungen des Kunden (nachfolgend auch "**Auftraggeber**") umfasst, schließen die Parteien ergänzend zum Nutzungsvertrag diese Vereinbarung zur Auftragsverarbeitung ("**AVV**"), um die Verpflichtungen beider Parteien zur Einhaltung des anwendbaren Datenschutzrechts (insbesondere der Anforderungen der EU Datenschutz-Grundverordnung („**DSGVO**“)) näher zu spezifizieren.

#### 2. **Pflichten des Auftragnehmers**

2.1 Weisungsbindung. Der Auftragnehmer darf die in **Anhang 1** zu dieser AVV aufgeführten und vom Auftraggeber zur Verfügung gestellten Kategorien personenbezogener Daten nur für die in Anhang 1 beschriebenen Zwecke und nur in Übereinstimmung mit den vom Auftraggeber erteilten Weisungen verarbeiten.

2.2 Verarbeitung aufgrund zwingender gesetzlicher Regelungen. Falls der Auftragnehmer verpflichtet ist, personenbezogene Daten nach dem Recht der Union oder des Mitgliedstaates, dem der Auftragnehmer unterliegt, zu verarbeiten, wird der Auftragnehmer den Auftraggeber hierüber vor der jeweiligen Verarbeitung schriftlich informieren, es sei denn, das Gesetz verbietet solche Informationen aus wichtigen Gründen des öffentlichen Interesses. Im letztgenannten Fall wird der Auftragnehmer den Auftraggeber unverzüglich informieren, sobald ihm dies rechtlich möglich ist.

2.3 Technische/organisatorische Maßnahmen. Unter Berücksichtigung des Stands der Technik, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen trifft der Auftragnehmer geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau für die im Auftrag des Auftraggeber durchgeführten Verarbeitungsvorgänge zu gewährleisten; einschließlich der als Mindeststandard in Anhang 2 näher beschriebenen Maßnahmen.

2.4 Laufende Bewertung und Verbesserung der technischen/organisatorischen Maßnahmen. Der Auftragnehmer prüft und bewertet die Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung im erforderlichen Umfang fortlaufend. Im Falle einer Verbesserung der

technischen und organisatorischen Maßnahmen wird der Auftragnehmer dem Auftraggeber auf Verlangen den Entwurf einer entsprechend aktualisierten Anlage 2 zur Verfügung zu stellen.

- 2.5 Compliance-Unterstützung. Der Auftragnehmer unterstützt auf dessen Anfrage den Auftraggeber in dem Umfang, der erforderlich ist, um die Einhaltung der datenschutzrechtlichen Verpflichtungen des Auftraggebers zu gewährleisten, indem er diejenigen Informationen zur Verfügung stellt und Unterstützungsleistungen erbringt, die der Auftraggeber zur Einhaltung datenschutzrechtlicher Vorschriften benötigt.
- 2.6 Informations-, Auskunfts- und Kontrollrechte. Der Auftragnehmer gewährt dem Auftraggeber und seinen Beauftragten während der Laufzeit dieser AVV auf Anfrage innerhalb einer angemessenen Frist die erforderlichen Informationen, um die Einhaltung der AVV und des anwendbaren Datenschutzrechts durch den Auftragnehmer zu überprüfen. Grundsätzlich erfolgen Kontrollmaßnahmen durch Abgabe von Eigenerklärungen des Auftragnehmers (oder der ggf. von ihm nach Maßgabe dieser AVV eingeschalteten Subunternehmer) oder durch Vorlage von Prüfungsergebnissen unabhängiger Dritter. Soweit es für den Auftraggeber zur Erfüllung seiner gesetzlichen Verpflichtungen erforderlich ist, kann sich der Auftraggeber nach rechtzeitiger vorheriger Anmeldung zu Prüfzwecken in den Betriebsstätten zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs von der Angemessenheit der Maßnahmen zur Einhaltung der technischen und organisatorischen Erfordernisse der für die Auftragsdatenverarbeitung einschlägigen Datenschutzgesetze überzeugen. Das Recht zur Durchführung der Kontrollmaßnahmen hat der Auftraggeber auch bereits vor Beginn der Datenverarbeitung. Die Kontrolle kann vom Datenschutzbeauftragten oder sonstigen Vertretern des Auftraggebers, welche zur Verschwiegenheit verpflichtet sind und gegen die der Auftragnehmer keine berechtigten Bedenken hat, durchgeführt werden. Umgehend im Anschluss an die Kontrolle der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen werden die Ergebnisse dieser Kontrolle vom Auftraggeber dokumentiert. Die Dokumentation ist dem Auftragnehmer im Anschluss zeitnah zur Verfügung zu stellen. Jede Partei trägt ihre im Zusammenhang mit den Kontrollmaßnahmen anfallenden Kosten.
- 2.7 Verletzung gesetzlicher / vertraglicher Bestimmungen durch Weisungen des Auftraggebers. Der Auftragnehmer wird den Auftraggeber benachrichtigen, wenn er der Ansicht ist, dass eine von ihm erhaltene Weisung gegen geltendes Datenschutzrecht und/oder gegen vertragliche Pflichten aus der AVV verstößt. Diese Hinweispflicht verpflichtet den Auftragnehmer nicht zu einer Prüfung etwaiger Weisungen. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung

solange auszusetzen, bis sie durch eine weisungsberechtigte Person des Auftraggebers bestätigt oder geändert wird.

- 2.8 Verletzung gesetzlicher / vertraglicher Bestimmungen durch den Auftragnehmer. Im Falle einer tatsächlichen oder vermuteten Verletzung des Schutzes personenbezogener Daten oder im Falle eines Verstoßes des Auftragnehmers, seiner Mitarbeiter oder sonstiger vom Auftragnehmer eingesetzter Dritter gegen datenschutzrechtlicher Vorschriften oder dieser AVV verpflichtet sich der Auftragnehmer
- 2.8.1 dem Auftraggeber unverzüglich (spätestens jedoch 36 Stunden nach Bekanntwerden des Ereignisses) über ein solches Ereignis beim Auftragnehmer oder einem Unterauftragnehmer zu informieren und dem Auftraggeber unverzüglich (wenn möglich, spätestens 36 Stunden nach Bekanntwerden des Ereignisses) angemessene Einzelheiten über das Ereignis mitzuteilen und
- 2.8.2 dem Auftraggeber auf Anfrage eine angemessene Zusammenarbeit und Unterstützung in Bezug auf alle Maßnahmen zu gewähren, die als Reaktion auf ein solches Ereignis im Rahmen der anwendbaren Datenschutzgesetze (v.a. nach Art. 33 (3), 34 (4) DSGVO) erforderlich sind.
- 2.9 Verzeichnis von Verarbeitungstätigkeiten. Der Auftragnehmer führt ein Verzeichnis über die im Auftrag des Auftraggebers durchgeführten Verarbeitungstätigkeit gemäß Art. 30 (2) GDPR und stellt dieses auf Anfrage dem Auftraggeber zur Verfügung.
- 2.10 Berichtigung, Löschung, Sperrung / Einschränkung der Verarbeitung. Aufzeichnungen, die vom Auftraggeber übermittelte personenbezogene Daten enthalten, dürfen nur gemäß den Anweisungen des Auftraggebers und der anwendbaren Datenschutzgesetze berichtigt, gelöscht und/oder gesperrt werden. Diese Verpflichtung bezieht sich nicht auf die vom Auftragnehmer zur Erbringung der Vertragsleistungen gespeicherten personenbezieharen Daten.
- 2.11 Aufsichtsbehörde. Der Auftragnehmer verpflichtet sich zur Zusammenarbeit und zur Einhaltung von Anweisungen, Richtlinien und Auflagen der zuständigen Aufsichtsbehörde.
- 2.12 Unterstützung bei Beschwerden oder Anfragen. Falls der Auftragnehmer Beschwerden, Anfragen oder Mitteilungen erhält, die sich auf die Verarbeitung personenbezogener Daten oder auf die Einhaltung der anwendbaren Datenschutzgesetze oder dieser AVV durch eine der Parteien beziehen, wird der Auftragnehmer den Auftraggeber unverzüglich benachrichtigen und dem Auftraggeber in Bezug auf solche Beschwerden, Anfragen oder Mitteilungen die erforderliche Mitwirkung, Informationen und Unterstützung (einschließlich der Berichtigung, Löschung und Sperrung personenbezogener Daten) gewähren.

2.13 Pflichten bei Beendigung der Auftragsverarbeitung. Bei Beendigung dieser AVV wird der Auftragnehmer auf Anweisung des Auftraggebers die vom Auftraggeber übermittelten personenbezogenen Daten entweder zurückgeben oder vernichten, wenn und soweit die weitere Speicherung dieser personenbezogenen Daten nicht zur Erfüllung von gesetzlichen Anforderungen erforderlich ist. Diese Verpflichtung bezieht sich nicht auf die vom Auftragnehmer zur Erbringung der Vertragsleistungen gespeicherten personenbeziehbaren Daten.

### **3. Datenverarbeitung außerhalb der EU/des EWR**

Der Auftragnehmer kann die Verarbeitung personenbezogener Daten im Rahmen dieser AVV auch außerhalb der EU/des EWR durchführen, wenn er die erforderlichen Garantien zur Gewährleistung eines angemessenen Datenschutzniveaus umsetzt.

### **4. Pflichten des Auftraggebers**

4.1 Verantwortlichkeit. Der Auftraggeber ist für die Rechtmäßigkeit der in Anlage 1 spezifizierten Verarbeitung personenbezogener Daten verantwortlich. Der Auftraggeber bleibt verantwortlich für alle Anforderungen des anwendbaren Datenschutzrechts in Bezug auf die betroffenen Personen, einschließlich, aber nicht beschränkt auf die Beantwortung von Auskunftersuchen der betroffenen Personen.

4.2 Weisungen. Der Auftraggeber ist nach näherer Maßgabe von Anlage 1 berechtigt, Weisungen über den Umfang und die Art und Weise der Verarbeitung personenbezogener Daten zu erteilen. Weisungsberechtigt sind nur Personen, die befugt sind, den Auftraggeber im Geschäftsverkehr umfassend zu vertreten.

### **5. Personal**

5.1 Der Auftragnehmer wird bei der Verarbeitung personenbezogener Daten im Auftrag des Auftraggebers das Datengeheimnis beachten und die mit der Datenverarbeitung betrauten Personen zur Vertraulichkeit verpflichten. Auf Verlangen des Auftraggebers wird der Auftragnehmer die Verpflichtungen aller Personen, die an der Verarbeitung personenbezogener Daten im Auftrag des Auftraggebers beteiligt sind, nachweisen.

5.2 Der Auftragnehmer wird dafür sorgen, dass alle an der Datenverarbeitung beteiligten Personen mit den einschlägigen Datenschutzbestimmungen vertraut gemacht werden. Der Auftragnehmer wird die Einhaltung dieser Datenschutzbestimmungen und dieser AVV durch diese Personen überwachen.

### **6. Unterauftragnehmer**

6.1 Der Auftragnehmer ist berechtigt, die in diesem Vertrag geregelte Auftragsverarbeitung ganz oder teilweise durch andere Dritte erfüllen zu lassen. Dies gilt auch für Tätigkeiten, die mit der in diesem Vertrag geregelten Auftragsverarbeitung im

Zusammenhang stehen und bei denen nicht ausgeschlossen werden kann, dass Dritte auf die personenbezogenen Daten des Auftraggebers zugreifen kann. Der Auftragnehmer wird den Auftraggeber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Unterauftragnehmern informieren.

- 6.2 Der Auftragnehmer ist verpflichtet, mit seinen Unterauftragnehmern, die er mit der Verarbeitung personenbezogener Objektdaten des Auftraggebers beauftragt, eine schriftliche Vereinbarung abzuschließen. Diese darf in Bezug auf die Interessen des Auftraggebers kein geringeres Schutzniveau als diese AVV aufweisen.

## **7. Freistellung**

- 7.1 Wenn gegen eine Partei aufgrund einer Verletzung der Verpflichtungen der anderen Partei nach dem anwendbaren Datenschutzgesetz und/oder dieser AVV von Dritten Ansprüche geltend gemacht werden, wird die andere Partei die in Anspruch genommene Partei von allen durch die Verletzung entstandenen Kosten, Gebühren, Schäden, Aufwendungen oder Verluste freistellen.

- 7.2 Die Freistellung setzt voraus, dass

- 7.2.1 die in Anspruch genommene Partei die andere Partei unverzüglich über den geltend gemachten Anspruch informiert; und

- 7.2.2 der anderen Partei die Möglichkeit gegeben wird, gemeinsam mit der in Anspruch genommenen Partei den geltend gemachten Anspruch abzuwehren oder zu vergleichen.

## **8. Vertragsdauer und Kündigung**

- 8.1 Diese AVV tritt mit Unterzeichnung durch beide Parteien in Kraft und ist auf unbestimmte Zeit abgeschlossen. Diese AVV kann von jeder Partei gegenüber der jeweils anderen Partei gekündigt werden, sobald der letzte Auftrag des Auftraggebers, der die Verarbeitung personenbezogener Daten umfasst, vollständig abgewickelt wurde.

- 8.2 Unbeschadet der vorstehenden Ziffer 8.1 kann jede Partei die AVV jederzeit aus wichtigem Grund gemäß § 314 BGB kündigen.

- 8.3 Kündigungen bedürfen der Schriftform.

## **9. Schlussbestimmungen**

- 9.1 Diese AVV unterliegt dem Recht der Bundesrepublik Deutschland unter Ausschluss des Kollisionsrechts.

- 9.2 Diese AVV enthält zusammen mit dem Nutzungsvertrag die gesamte Vereinbarung der Parteien über den Gegenstand (Auftragsverarbeitung personenbezogener Daten). Im Falle von Widersprüchen zwischen dem Nutzungsvertrag und dieser AVV gehen die Regelungen der AVV vor. Änderungen und Ergänzungen dieser AVV

bedürfen zu ihrer Gültigkeit der Schriftform und der Unterschrift von bevollmächtigten Vertretern der Parteien. Dies gilt auch für eine Änderung dieses Schriftformerfordernisses.

- 9.3 Für den Fall, dass eine Klausel dieser AVV unwirksam sein sollte, oder die AVV in Bezug auf einen bestimmten Gegenstand eine Lücke aufweist, bleibt die Wirksamkeit der übrigen Klauseln hiervon unberührt. In diesem Fall haben die Parteien eine Vereinbarung zu treffen, die dem Zweck der unwirksamen Klausel, oder im Falle einer Lücke, der Systematik und dem Schutzzweck der gesamten AVV, am ehesten entspricht.

## **Anhang 1**

### **Einzelheiten der Auftragsverarbeitung**

#### **1. Gegenstand und Dauer des Auftrags**

##### 1.1 Gegenstand des Auftrags

1.1.1 Der Auftragnehmer stellt dem Auftraggeber nach Maßgabe des Nutzungsvertrages einen Online-Zugriff auf GeoVeris zur Verfügung. Zur Nutzung von GeoVeris ist es erforderlich, dass der Auftraggeber dem Auftragnehmer Geo-Punkt-daten übermittelt, damit Geoinformationen zu den vom Auftraggeber durch Geo-Punkt-daten bezeichneten Objekten zugeordnet werden können. Eine weitere Verarbeitung oder Nutzung der Geo-Punkt-daten durch den Auftraggeber findet nicht statt.

1.1.2 Der Auftraggeber wird nur Daten (insbesondere Geo-Punkt-daten) an den Auftragnehmer übermitteln, bezüglich derer er selbst ausschließlich Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO ist und die er unter Beachtung der datenschutzrechtlichen Bestimmungen erhoben hat.

##### 1.2 Dauer des Auftrags

Die Dauer des Auftrags entspricht der Laufzeit des Nutzungsvertrages.

#### **2. Konkretisierung des Auftragsinhalts**

##### 2.1 Art der Auftragsverarbeitung von personenbeziehbaren Daten

2.1.1 Der Auftragnehmer verarbeitet bei Nutzung von GeoVeris durch den Auftraggeber Geo-Punkt-daten, die nach Auffassung der Aufsichtsbehörden für den Datenschutz personenbezogene Daten im Sinne von Art. 4 Nr. 1 DSGVO sind.

2.1.2 Beim Auftragnehmer werden die vom Auftraggeber ausschließlich online übermittelten Geo-Punkt-daten durch GeoVeris automatisch verarbeitet. Dabei können vom Auftraggeber zum Zweck der Abfragevorbereitung Klartext-Adressen der abzufragenden Orte an den Auftragnehmer übermittelt werden. Dort werden diese automatisch in Punktkoordinaten des Objekts (Objektkoordinaten) umgerechnet und diese Punktkoordinaten werden dem Auftraggeber online zurück übermittelt (Geocoder-Funktion). Bei einer sofort oder später erfolgenden Abfrage der Geoinformationen zu dem Objekt (den Objekten) aus GeoVeris werden diese Geoinformationen dann den Objektkoordinaten zugeordnet und mit diesen online an den Auftraggeber übermittelt. Dabei werden die vom Auftraggeber übermittelten Adressdaten und Geokoordinaten beim Auftragnehmer in automatisierten Dateien gespeichert. Diese Dateien werden vorbehaltlich abweichender

Vereinbarungen mit dem Auftraggeber im Einzelfall unter Beachtung der gesetzlichen Vorschriften (einschließlich der anwendbaren handels- und steuerrechtlichen Aufbewahrungspflichten) gespeichert.

- 2.2 Der Datenverarbeitungsvorgang gliedert sich in folgende Verarbeitungsschritte:
  - 2.2.1 Ein Berechtigter Nutzer des Auftraggebers loggt sich mit Benutzernamen und Passwort auf der GeoVeris-Plattform ein.
  - 2.2.2 Anschließend übermittelt er durch Eingabe in eine vorgegebene Maske an den Auftragnehmer Adressdaten oder Geokoordinaten (bei Ereignis-Abfragen zudem obligatorisch die Schadennummer und optional die Versicherungsscheinnummer; bei Risikoabfragen optional eine Projektnummer) und wählt die gewünschten Produkte aus.
  - 2.2.3 Soweit Adressdaten übermittelt werden, rechnet der Auftragnehmer diese in Geokoordinaten um.
  - 2.2.4 Die Geokoordinaten werden mit den beim Auftragnehmer verfügbaren Geoinformationen angereichert.
  - 2.2.5 Die angereicherten Datensätze werden an den Auftraggeber zurückübermittelt.
  - 2.2.6 Der Abschluss der Abfrage-Sitzung erfolgt durch ein Logout des Nutzers oder nach Timeout.
- 2.3 Zweck der Auftragsverarbeitung personenbezogener Daten

Dem Auftraggeber soll es ermöglicht werden, einzelnen Adressen Geoinformationen zuzuordnen. Dies erfolgt nur im Zusammenhang mit der im Nutzungsvertrag vereinbarten zulässigen Nutzung von GeoVeris zur Beurteilung, Bearbeitung und Regulierung von Schadensfällen.
- 2.4 Arten personenbezogener Daten

In GeoVeris werden neben den personenbeziehbaren Adressdaten oder Geokoordinaten ohne Namensangaben ausschließlich die in der jeweils geltenden Leistungsbeschreibung zum Nutzungsvertrag genannten Geoinformationen zur Verfügung gestellt.
- 2.5 Kategorien betroffener Personen

Die übermittelten Adressdaten oder Geokoordinaten können zu Objekten gehören, die bereits Gegenstand von Verträgen zwischen dem Auftraggeber und Dritten sind oder die im Rahmen der Bearbeitung von Geschäftsvorfällen mit Bezug zu bestimmten Risiken gegenüber dem Auftraggeber genannt wurden und für diese Bearbeitung erforderlich sind. Betroffene sind daher regelmäßig solche Personen, die mit dem Auftragnehmer in einer vertraglichen oder sonstigen geschäftlichen Beziehung stehen sowie Personen, die zu dem durch die Adresse oder Geokoordinate

bezeichneten Objekt in einer rechtlichen Beziehung stehen (wie Eigentümer und Inhaber sonstiger Rechte laut Grundbuch, Mieter, Pächter, Bewohner oder sonstige Personen, die das Objekt nicht nur vorübergehend nutzen, ebenso wie dort polizeilich gemeldete Personen).

### **3. Weisungen des Auftraggebers**

- 3.1 Die Verarbeitung der personenbeziehbaren Daten erfolgt im Rahmen von GeoVeris überwiegend automatisiert nach den Eingaben des Auftraggebers im Rahmen der vom Auftragnehmer definierten Funktionalitäten und Einsatzbedingungen von GeoVeris. Eine manuelle Steuerung oder Eingriffsmöglichkeit des Auftragnehmers in einen laufenden Datenverarbeitungsprozess ist nicht vorgesehen. Auf die automatisierte Datenverarbeitung kann durch Weisungen des Auftraggebers an den Auftragnehmer in der Regel kein sofortiger Einfluss genommen werden. Vor diesem Hintergrund gelten vom Auftragnehmer definierte Maßgaben und die vom Auftraggeber an den Auftragnehmer erteilten Aufträge zugleich auch als Weisungen des Auftraggebers an den Auftragnehmer im Hinblick auf Art und Umfang der Verarbeitung und Nutzung personenbezogener Daten.
- 3.2 Soweit im Rahmen von GeoVeris (z.B. bei der manuellen Zusammenstellung von Geo-Daten durch den Auftragnehmer oder einen vom Auftragnehmer beauftragten Dritten) Aufträge erteilt werden können, gelten die vom Auftraggeber an den Auftragnehmer erteilten Aufträge zugleich auch als Weisungen des Auftraggebers an den Auftragnehmer im Hinblick auf Art und Umfang der Verarbeitung und Nutzung personenbezogener Daten
- 3.3 Soweit dies möglich ist, ist der Auftragnehmer verpflichtet, Weisungen des Auftraggebers im Hinblick auf seine Daten Folge zu leisten, z. B. durch veränderte Programmierungen der zukünftigen Verarbeitungen seiner Objektdaten. Etwaige hierdurch verursachte Kosten sind vom Auftraggeber zu tragen. Die Weisungen sind schriftlich zu erteilen; mündliche Weisungen sind unwirksam.
- 3.4 Der Auftragnehmer wird den Auftraggeber darauf hinweisen, wenn er der Ansicht ist, dass eine Weisung gegen Datenschutzvorschriften verstößt. Diese Hinweispflicht verpflichtet den Auftragnehmer nicht zu einer Prüfung etwaiger Weisungen. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch eine weisungsberechtigte Person des Auftraggebers bestätigt oder geändert wird.

## **Anhang 2**

### **Technische und organisatorische Maßnahmen**

GeoVeris wird im Auftrag des Auftragnehmers durch die BTC Business Technology Consulting AG, Escherweg 5, 26121 Oldenburg (BTC AG) unter Einbindung ausgewählter Unterauftragnehmer betrieben. Die hierbei von der BTC AG bzw. den Unterauftragnehmern getroffenen technischen und organisatorischen Maßnahmen sind in den im Folgenden beigefügten und von der BTC AG zur Verfügung gestellten Dokumenten ("Informationssicherheit BTC" sowie "Managed Cloud Services") beschrieben und dokumentiert.

## Informationssicherheit BTC

Konzeption und Übersicht der technischen und organisatorischen Maßnahmen gem. Artikel 32 DSGVO

Zur internen Verwendung



Ihre **Vision**  
ist unser **Fokus!**

Verwirklichen wir sie gemeinsam.

## Inhaltsverzeichnis

<b>1</b>	<b>Konzeption der Datenschutzrechtlichen Maßnahmen .....</b>	<b>3</b>
1.1	Geltungsbereich .....	3
1.2	Meldepflichten .....	4
1.3	Cloudprovider korrespondierende Maßnahmen .....	4
1.4	Kundenkorrespondierende Maßnahmen .....	5
1.5	Standarddatenschutzmodell (SDM) .....	7
1.6	Ziele der DSGVO zur technischen und organisatorischen Sicherheit .....	8
<b>2</b>	<b>Relevante Zertifizierungen und Testate.....</b>	<b>9</b>
<b>3</b>	<b>Zutrittskontrolle .....</b>	<b>10</b>
<b>4</b>	<b>Zugangskontrolle .....</b>	<b>12</b>
<b>5</b>	<b>Zugriffskontrolle .....</b>	<b>15</b>
<b>6</b>	<b>Weitergabekontrolle .....</b>	<b>17</b>
<b>7</b>	<b>Eingabekontrolle .....</b>	<b>19</b>
<b>8</b>	<b>Auftragskontrolle .....</b>	<b>19</b>
<b>9</b>	<b>Verfügbarkeitskontrolle .....</b>	<b>20</b>
<b>10</b>	<b>Trennungsgebot .....</b>	<b>22</b>
<b>11</b>	<b>Organisation .....</b>	<b>22</b>
<b>12</b>	<b>TOM-Liste nach Stichworten .....</b>	<b>23</b>
<b>13</b>	<b>Dokumentenlenkung.....</b>	<b>27</b>

# 1 Konzeption der Datenschutzrechtlichen Maßnahmen

## 1.1 Geltungsbereich

Grundsätzlich gelten für die eingesetzten Systeme bei der BTC die gleichen datenschutzrechtlichen Anforderungen wie für den Betrieb von Kundensystemen, auf denen personenbezogene Daten verarbeitet werden (Outsourcing).

Dieses Dokument dient der erläuternden Darstellung der gesetzlichen Anforderungen in Bezug auf den Datenschutz gemäß Art. 32 DSGVO (Datenschutzgrundverordnung) insbesondere unter den folgenden Bedingungen:

- ✓ Der IT-Betrieb Informationssysteme mit personenbezogenen Daten im Sinne der DSGVO wird durch die BTC IT-Services verantwortet
- ✓ Die Informationssysteme mit personenbezogenen Daten im Sinne der DSGVO werden von der BTC IT-Services betrieben (Rechenzentren in Oldenburg, Integration in Web-Services / private Cloud Kundenumgebungen innerhalb der EU, Microsoft Online Services / Azure innerhalb der EU)
- ✓ Die BTC Office-IT wird für die Leistungserbringung eingesetzt

Für die eingesetzte IT-Infrastruktur Office-IT und Produktions-IT der BTC treffen diese Bedingungen zu. Im Zuge der Leistungserbringung bei einem Kunden vor Ort werden die internen Systeme eingesetzt, um beispielsweise auf die Fernwartungsplattform zuzugreifen, Projektdokumentation nachzuhalten, Kommunikationsdienste zu nutzen und die erbrachten Leistungen abzurechnen.

Die Rechte und Pflichten der Parteien ergeben sich allein aus den vertraglichen Vereinbarungen, internen Regelungen und den gesetzlichen Bestimmungen zum Datenschutz. Insofern können aus dieser Dokumentation keine Ansprüche abgeleitet werden. Die aufgeführten Maßnahmen können im Einzelnen gemäß der vertraglichen Vereinbarung sowie aufgrund der kontinuierlichen Fortentwicklung der Kundenanforderungen variieren und ein höheres Sicherheitsniveau erwirken.

Im Zuge zahlreicher Audits wird die Schutzwirkung einzelner Maßnahmen regelmäßig überwacht und durch interne Kontrollmaßnahmen bestätigt.

Verantwortlich für die technischen und organisatorischen Maßnahmen im Zuge der Leistungserbringung sind:

- ✓ BTC
  - IT-Strategie und Steuerung der Office-IT und Produktions-IT BTC
  - Cloud Integration
  - Qualitätsmanagement QM
  - IT-Betriebsprozesse und -mittel
  - Netzwerk LAN/Backbone
  - Informationssicherheitsmanagement ISMS (Integriertes IMS)
  - Business Continuity Management BCMS (Integriertes IMS)
  - Service Integration (Cloudservices, On-Premise, etc.)

- ✓ EWE TEL GmbH
  - Rechenzentrums-Betrieb
  - WAN-Anbindung inkl. DDoS Schutz
- ✓ Microsoft Online Services
  - Microsoft 365
- ✓ Azure (kundenspezifisch im Rahmen der Cloud-Integration /Service Integration)
- ✓ Amazon Webservices (kundenspezifisch im Rahmen der Cloud-Integration /Service Integration)

## 1.2 Meldepflichten

Grundsätzlich erhebt die BTC auch Daten von ihren Mitarbeitern und setzt eigene Webservices zur Außendarstellung ein und ist dafür die verantwortliche Stelle im datenschutzrechtlichen Sinne. Diesbezüglich werden gemäß der DSGVO die gesetzlichen Informations- und Meldepflichten gegenüber den Betroffenen und der Datenschutz-Aufsichtsbehörde eingehalten.

Im Rahmen unserer beauftragten Leistungserbringung sind unsere Kunden und Partner jeweils die verantwortliche Stelle im Rahmen der Auftragsverarbeitung. Berechtigte Anfragen von Betroffenen und der anfragenden Aufsichtsbehörde werden unverzüglich an die von Ihnen mitgeteilten Ansprechpartner und Meldestellen weitergeleitet, um das weitere Vorgehen und mögliche Unterstützungsleistungen abzustimmen und zu priorisieren.

Zudem stimmen wir die darüberhinausgehenden Meldepflichten im Rahmen der Vereinbarung zum Datenschutz (Art. 28 DSGVO) sowie der gesetzlichen Anforderungen (Art. 33-36 DSGVO) mit Ihnen ab und kommen diesen nach.

## 1.3 Cloudprovider korrespondierende Maßnahmen

Im Kontext von Cloudservices hat die Steuerung des Cloudproviders eine besonders hohe Relevanz. Maßgebliche Entscheidungen sind zu treffen bezüglich des Einsatzes in kritischen Geschäftsbereichen (Schutzbedarfe, Business Impact, KRITIS, etc.) sowie in Bezug auf Drittstaatentransfer (außerhalb der EU). Die enge Abstimmung und Einhaltung der gesetzlichen Pflichten zur Transparenz und Rechenschaft erfolgt in der Phase der Auftragsanbahnung, der Transition sowie im weiteren Verlauf in der Betriebsphase durch die Serviceorganisation (Änderungen in der Funktionalität / Anbieter / Zweckänderungen etc.).

Die Ansprechpartner, Supportkanäle und der Grad der geteilten Verantwortung (Prinzip der Cloudprovider) bzw. Abgrenzung der Betriebsverantwortung sind festgelegt und in den cloudspezifischen Betriebsprozessen implementiert.

Der Einsatz von Cloudservices erfolgt ausschließlich in Kenntnis unserer Kunden. Auch die Gegebenheiten werden transparent dargelegt.

Das Betriebskonzept für Cloudservices kann kundenspezifisch ausgeprägt sein und kann IaaS, PaaS, SaaS beinhalten.

Cloud-Provider und weitere Leistungserbringer innerhalb der Cloudservices werden sorgfältig ausgewählt und transparent in der Serviceorganisation dargelegt.

Veränderungen der Funktionsweise von Cloudservices sind aufgrund der geringen Innovationszyklen zu erwarten – die Möglichkeiten der Einflussnahme zur Konfiguration ist abhängig davon, welche Optionen der Cloudprovider dafür zur Verfügung stellt.

## 1.4 Kundenkorrespondierende Maßnahmen

Die Leistungserbringer werden in ihrem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht werden. Sie werden technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Kunden treffen, die den Anforderungen der gemäß Art. 32 DSGVO genügen.

Es sind dabei technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen.

Unseren Kunden werden die technischen und organisatorischen Maßnahmen kategorisch in diesem Dokument sowie auftragsspezifisch in angemessener Weise zur Kenntnis gebracht. Die Eignung dieser Maßnahmen kann in die kundeneigenen Risikobewertungen einfließen. Ein angemessenes Schutzniveau ist zu erreichen.

Bei besonderen Kategorien von personenbezogenen Daten oder bei hohen Risiken für die Betroffenenrechte ist es die Aufgabe unserer Kunden und Partner, eine Datenschutzfolgeabschätzung durchzuführen (Art. 35 DSGVO) und in Abstimmung der Ansprechpartner für die im Rahmen des Vertrages anfallenden Datenschutzfragen ggf. spezielle technische Maßnahmen anzuweisen.

Im IT-Betrieb sowie beim Einsatz der Office-IT wird insbesondere die Aufrechterhaltung der Zertifizierung des Managementsystems für Informationssicherheit nach der international anerkannten Norm ISO/IEC 27001 als ein geeigneter Nachweis für die Wirksamkeit der technischen und organisatorischen Maßnahmen anerkannt und dient als Basis für die datenschutzrechtlichen Kontrollmaßnahmen.

Die technischen und organisatorischen Maßnahmen im IT-Betrieb im Marktangebot „Managed Service Provider IT-Outsourcing“ sind grundsätzlich Bestandteil des integrierten Managementsystems für Informationssicherheit, Business Continuity (Notfall- und Krisenmanagement) sowie der ITIL-orientierten Betriebsprozesse.

Kundenspezifische Ausprägungen der vereinbarten Maßnahmen münden in der kundenspezifischen Konzeption der IT-Architektur und in die vereinbarten Freigabeprozesse bei der Einführung eines IT-Services sowie im Transition- und Change-Management (ITIL).

Das integrierte Managementsystem beinhaltet ein Risikomanagement, welches insbesondere die Eignung der getroffenen Risikobehandlungsmaßnahmen prozessual bewertet. Darüber hinaus werden operative Risiken zum Beispiel bei Bekanntwerden kritischer Schwachstellen im IT-Betrieb ad hoc bewertet und erforderliche Maßnahmen abgeleitet. Diese werden mit den jeweiligen Ansprechpartnern für die Freigabe von Maßnahmen im Changemanagement abgestimmt. Bei Gefahr im Verzug werden in Einvernehmen die Freigabeprozesse ausgesetzt und im Nachgang die erforderlichen Maßnahmen zur Gefahrenabwehr mitgeteilt und freigegeben.

Sämtliche IT-Services und Applikationen sind in einer strukturierten und kundenspezifischen IT-Inventarisierung geführt. Diese Informationen können Ihnen ggf. bei der Erarbeitung Ihres Verzeichnisses der Verarbeitungstätigkeiten (Verfahrensverzeichnis) behilflich sein.

Die getroffenen Sicherheitsmaßnahmen werden im IT-Betrieb standardmäßig im Systemkonzept und im Betriebsführungshandbuch (Architekturkonzept, Service Level, etc.) bzw. im Servicekonzept dokumentiert.

Fachspezifische Informationen zum Datenfluss, zum Datenexport / Schnittstellen sowie die zulässigen Speicherorte und Berechtigungskonzepte liegen dem IT-Betrieb / dem Fachsupport in der Regel nicht in dokumentierter Form vor. Sofern dies zur datenschutzrechtlichen Bewertung aus Kundensicht erforderlich ist, kann mit Unterstützung des IT-Betriebes eine entsprechende Dokumentation mittels einer beauftragten Leistungserbringung erfolgen.

Zur Erfüllung Ihrer datenschutzrechtlichen Pflichten unterstützen unsere Fach- und Kundenansprechpartner mit technischen Lösungen für die in ihrem Datenschutzmanagement identifizierten Handlungsbedarfe.

Zur Umsetzung der datenschutzrechtlich erforderlichen Maßnahmen ist aus unserer Sicht zusammengefasst eine enge Zusammenarbeit in folgenden Aufgabenfeldern erforderlich:

- **Verarbeitungsverzeichnis**

- ✓ Wir benötigen von Ihnen eine Übersicht der Kategorien Ihrer Daten, auf die sich unsere Tätigkeiten gemäß Leistungsvertrag beziehen und aus der die Risiken für die Betroffenenrechte (Schutzbedürftigkeit) sowie die Verarbeitung besonderer Kategorien (Art. 9 DSGVO) hervorgeht.
- ✓ Wir halten alle technischen Informationssysteme / IT-Systeme in einem kundenspezifisch geführten, elektronischen Inventar vor (Configuration Items, Architekturgraph).
- ✓ Die Beschreibung der allgemein anwendbaren Maßnahmen sind in diesem Dokument aufgeführt. Fachspezifische Maßnahmen sind den vereinbarten Dokumentationen zu entnehmen (Fachkonzepte, Systemkonzepte, Servicekonzepte, etc.).

- **Unterstützung bei der Datenschutzfolgeabschätzung, um**

- die Eignung der getroffenen Maßnahmen gemeinsam zu bewerten und
- Empfehlungen für die Erweiterung der bisherigen technischen Maßnahmen zu erarbeiten sowie
- ggf. durch Erweiterung der Leistungsvereinbarung umzusetzen.

- **Anfragen durch Aufsichtsbehörden**

- ✓ Unserer Pflicht zur Zusammenarbeit kommen wir vollumfänglich nach. Wir werden alle relevanten und festgelegten Ansprechpartner unverzüglich über Anfragen der Aufsichtsbehörden informieren und das weitere Vorgehen mit Ihnen abstimmen.
- ✓ Sollten Sie durch eine Aufsichtsbehörde kontaktiert werden, unterstützen unsere Fachkräfte Sie mit höchster Priorität in allen Belangen, die in unserer Verantwortlichkeit liegen und darüber hinaus stehen wir Ihnen soweit erforderlich mit Rat und Tat zur Seite.
- ✓ Beachten Sie bitte, dass zahlreiche gesetzliche Forderungen aus der DSGVO und dem BDSG der verantwortlichen Stelle zugeordnet sind und diese nicht delegiert werden können.

- **Stand der Technik**

- ✓ Das allgemeine technische Sicherheitsniveau wird unter Berücksichtigung wirtschaftlicher Aspekte angemessen aufrechterhalten und entspricht grundsätzlich dem Stand der Technik.
- ✓ Die beauftragten Services und Dienstleistungen werden mit Ihnen gemeinsam innerhalb der Auftragsanbahnung bis zur Auftragsabwicklung abgestimmt und zur Kenntnis gebracht. Nach wirtschaftlichen und risikoorientierten Bewertungsgrundlagen kann der Einsatz zusätzlicher spezieller Sicherheitstechnologien zur Angriffserkennung und regelmäßiger Einsatz von Prüfwerkzeugen zur Schwachstellenermittlung erfolgen.
- ✓ Insbesondere Anforderungen an die Verschlüsselung, Pseudonymisierung und Anonymisierung und die Handhabung in der täglichen Praxis bedürfen einer engen fachlichen Abstimmung (Testdaten, Webservices, etc.).
- ✓ Hohe Risiken sowie besondere Kategorien von personenbezogenen Daten (DSGVO) können ggf. zusätzliche Sicherheitstechnologien erfordern, die wir gemäß Ihrer Bewertung und vereinbartem Leistungsvertrag implementieren können. Dabei gilt es, den aktuellen Stand der Technik zu Grunde zu legen.

- **Datenschutz durch Technik und Voreinstellungen**
  - ✓ Bei der Konzeption der Services haben Sie direkten Einfluss auf die technische Gestaltung und die Voreinstellungen zur etwaigen Erhebung von Daten, die Einfluss auf die Betroffenenrechte nehmen.
- **Meldung von Datenschutzverstößen**
  - ✓ Verletzungen des Schutzes von personenbezogenen Daten werden wir Ihnen unverzüglich mitteilen, so dass Sie Ihrer Meldepflicht an die zuständige Datenschutzaufsichtsbehörde bei hohen Risiken für die Betroffenenrechte unverzüglich nachkommen können.
  - ✓ Von unserer Seite als unzulässig oder zweifelhaft identifizierte Anfragen zur Datenverarbeitung werden umgehend an die von Ihnen genannten Ansprechpartner für Datenschutzfragen (Datenschutzbeauftragte/r, Fachabteilung, etc.) mitgeteilt.
- **Bewertung operativer Risiken**
  - ✓ Je nach vertraglicher Vereinbarung können technische Schwachstellen ggf. automatisiert ermittelt und im Rahmen der vereinbarten Wartungsfenster behoben werden.
  - ✓ Bei Bekanntwerden von Schwachstellen mit besonders hohen Risiken, ist eine enge Abstimmung und eine kundenseitige Priorisierung der einzuleitenden Maßnahmen erforderlich.
  - ✓ Bei Datenverarbeitungen von Daten mit besonderen Risiken oder besonderen Kategorien von personenbezogenen Daten (sofern zutreffend) sind die Verfahren entsprechend anzupassen. Eine rechtzeitige Beseitigung durch Optimierung oder Einführung von technischen und organisatorischen Maßnahmen ist zu erwirken.

## 1.5 Standarddatenschutzmodell (SDM)

Folgende Grundwerte werden standardmäßig im IT-Betrieb in den Managementsystemen berücksichtigt:

<b>Vertraulichkeit</b>	Die Fähigkeit zum Schutz vor unbefugtem Zugriff
<b>Integrität</b>	Die Korrektheit der personenbezogenen Daten
<b>Verfügbarkeit</b>	Die zeitgerechte Bereitstellung der Daten
<b>Belastbarkeit</b>	Die Fähigkeit, die Systeme fehlerresistent betreiben zu können

Insbesondere die Anforderungen an die Verfügbarkeit und die Belastbarkeit sind standardmäßig vertraglich durch entsprechende Leistungsangaben (Service Level Agreements, Leistungsscheine etc.) festgelegt. In der Transitionsphase sowie bei Änderungen der IT-Services werden mit Unterstützung der IT-Architekten Schutzbedarfsanalysen erstellt. Daraus resultiert eine entsprechende IT-Architektur wie z. B. eine redundante Datenhaltung, Lastverteilung, die schnelle Wiederherstellung der Daten sowie eine performante Anbindung an das Netzwerk / VPN / Internet und Perimeterschutz (Firewall, Routing etc.).

Die IT-Betriebsprozesse im Marktangebot IT-Outsourcing werden nach der ISO/IEC 27001 (Managementsystem für Informationssicherheit) und der ISO 22301 (Managementsystem für Business Continuity) in regelmäßigen Audits auf Wirksamkeit geprüft. Weitergehend gilt dies im Rahmen der jährlichen Prüfung nach den Wirtschaftsprüfungsstandards ISAE 3402 und IDW PS 951.

Als Voraussetzung zur Erreichung der vorgenannten Zertifizierungen sowie der gesetzlichen Vorgaben finden jährlich interne Audits und datenschutzrechtliche Kontrollen statt. Darüber hinaus ist bei jedem externen Zertifizierungsaudit sowie ausgewählten Lieferantenaudits im IT-Betrieb der Datenschutzbeauftragte involviert.

Nach unserem Kenntnisstand sind die vorgenannten Ausführungen hinreichende Garantien für die Eignung der getroffenen Maßnahmen zum Schutz personenbezogener Daten und die damit verbundenen datenschutzrechtlichen Betroffenenrechte (Art. 28 DSGVO).

Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung bzw. unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden. Dieses gilt insbesondere, wenn dies zu einem physischen, materiellen oder immateriellen Schaden der Betroffenen führen würde (Art. 32 DSGVO).

## 1.6 Ziele der DSGVO zur technischen und organisatorischen Sicherheit

<b>Zutrittskontrolle</b>	Die BTC sichert zu, den Zugang zu den Geschäftsräumen und Datenverarbeitungsanlagen durch geeignete Verfahren abzusichern.
<b>Zugangskontrolle</b>	Die BTC sichert zu, dass nur autorisierte Mitarbeiter Zugang zu den Datenverarbeitungsanlagen haben.
<b>Zugriffskontrolle</b>	Die BTC sichert im Rahmen der Beauftragung zu, dass nur autorisierte Mitarbeiter Zugriff auf die Informationssysteme und zu den zu verarbeitenden personenbezogenen Daten haben.
<b>Weitergabekontrolle</b>	Die BTC gewährleistet im Rahmen der Beauftragung, dass bei elektronischer Übertragung von personenbezogenen Daten diese nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.
<b>Eingabekontrolle</b>	Die BTC sichert im Rahmen der Beauftragung zu, dass die Verarbeitung der personenbezogenen Daten durch ausreichende Verfahren angemessen protokolliert wird. Dies gilt auch für die ggf. beauftragte Vernichtung von Daten.
<b>Auftragskontrolle</b>	Die BTC gewährleistet die weisungsgemäße Auftragsverarbeitung sowie auch bei einem Einsatz von genehmigten Subunternehmern die datenschutzrechtlichen Pflichten dem Subunternehmer zu übertragen. Erfüllungsgehilfen sind dabei gesondert zu betrachten.
<b>Verfügbarkeitskontrolle</b>	Die BTC gewährleistet im Rahmen der Beauftragung, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.
<b>Trennungsgebot</b>	Die BTC gewährleistet im Rahmen der Beauftragung, dass zu unterschiedlichen Zwecken erhobene Daten getrennt voneinander gespeichert und verarbeitet werden können.

---

### Sonstiges

Für die auftragsspezifische Ausgestaltung und Bewertung der technischen und organisatorischen Maßnahmen stehen Ihnen ihre Ansprechpartner (Accountmanager, Servicemanager) zur Verfügung. Insbesondere im Rahmen der Auftragsanbahnung, der ersten Projektstartphase oder der Transitionsphase ist eine gemeinsame Bewertung des erreichten angemessenen Schutzniveaus vorgesehen.

Eine Pseudonymisierung oder eine Anonymisierung von Daten erfolgt nach Erfordernis und Vorgaben aus der Risikobewertung seitens der verantwortlichen Stelle. Insbesondere sind diese Maßnahmen in Testumgebungen zu empfehlen, bei denen von den typischen Sicherheitsmaßnahmen möglicherweise abgewichen werden soll. Eine Mengenbeschränkung kann ggf. zusätzlich als risikomindernde Maßnahme erfolgen.

---

## 2 Relevante Zertifizierungen und Testate

Neben herstellerspezifischen zertifizierten Partnerschaften (SAP, Microsoft, Oracle, Citrix etc.) sind folgende akkreditierte Zertifizierungen aus datenschutzrechtlicher Betrachtung relevant:

Unternehmen	Zertifizierung
<b>BTC IT Services</b>	
IT-Betrieb	TÜV Rheinland Cert: ISO/IEC 27001 TÜV Rheinland Cert: ISO 22301 Ebner Stolz: ISAE 3402 Typ I + II, PS 951 Typ 1 + 2 Unterstützungsprozesse, Auftragsanbahnung, Auftragseinstellung unterliegen der Zertifizierung der BTC zur ISO/IEC 9001 Microsoft 365/Azure Services unterliegen der Zertifizierung von Microsoft durch bsi ISO/IEC 27001, ISO/IEC 27018 etc.
<b>BTC</b>	
Dienstleistungen	DeuCert: ISO / IEC 9001
Application Management	DeuCert: ISO/IEC 27001
Office IT	Die IT-Betriebsprozesse der Office IT unterliegen der Zertifizierung durch die BTC IT Services TÜV Rheinland Cert: ISO/IEC 27001  Microsoft 365/Azure Services unterliegen der Zertifizierung von Microsoft durch bsi ISO/IEC 27001, ISO/IEC 27018 etc.
<b>BTC / BITS</b>	
Smart Metering	TÜV Rheinland Cert: TR 3109-6
<b>EWE TEL</b>	
Rechenzentrum	TÜV IT: Trusted Site Infrastructure Level 2 / 3 (erweitert) DQS: ISO/IEC 27001 DQS: ISO/IEC 9001 Treuhand Weser Ems: PS 951

---



<b>3.7</b>	Durch welche weiteren organisatorische / technische Maßnahmen wird die Zutrittskontrolle unterstützt?	<p>Alarmanlage</p> <p>Gebäudebewachung</p> <p>RZ: Handvenenscanner</p> <p>RZ: Videoüberwachung (aktiv)</p>	<p>Wachdienst führt Begehung bei Alarmierung durch sowie unregelmäßige Rundgänge</p>
<b>3.8</b>	Sind die Eingangstüren und Nebentüren gesichert, so dass ein Schutz vor unbemerktem Betreten besteht?	<p>RZ: Vereinzelungsschleusen</p> <p>Elektronische Schließung</p> <p>Tür-offen-Überwachung</p> <p>Mitarbeiterausweise</p> <p>Mitarbeitersensibilisierung</p>	<p>Alarmmeldungen an den Wachdienst</p>
<b>3.9</b>	Werden Fremddienstleister in den Gebäuden beaufsichtigt?	<p>RZ: Ja, in ständiger Begleitung</p> <p>Risikobasierte Entscheidungen der betroffenen Fachabteilung</p>	<p>Eine vollständige Begleitung kann unter Umständen nicht gewährleistet werden und ist abhängig von den Umständen</p>
<b>3.10</b>	Werden Besucher vom Besuchten begleitet bzw. von ihm abgeholt?	<p>Grundsatz: Ja, in ständiger Begleitung bis zur Verabschiedung</p>	
<b>3.11</b>	Werden Fenster verschlossen, wenn die Räume, in denen der Auftragnehmer Daten des Auftraggebers verarbeitet, nicht besetzt sind?	<p>RZ: Keine Fenster vorhanden</p> <p>IT-Betrieb: Organisatorische Regelung und Awareness Maßnahmen</p> <p>Rundgänge Wachdienst</p>	<p>RZ-Zertifizierung physische Sicherheit</p>
<b>3.12</b>	Sind einstiegsgefährdete Fenster und Türen in Gebäuden, in denen der Auftragnehmer Daten des Auftraggebers verarbeitet, gegen Einbruch abgesichert?	<p>RZ: Keine einstiegsgefährdeten Fenster / Türen</p> <p>IT-Betrieb: Alarmsicherung</p>	<p>RZ-Zertifizierung physische Sicherheit</p>
<b>3.13</b>	Welche Personen dürfen eigenständig das Rechenzentrum betreten?	<p>RZ-Verantwortliche</p> <p>Haustechniker</p> <p>Infrastrukturteam</p> <p>IT-Systemtechniker</p>	<p>Dedizierte Wartungsbereiche</p>
<b>3.14</b>	Sind die Technikräume bzw. das Rechenzentrum vor dem Zutritt unberechtigter Personen – insbesondere auch außerhalb der Geschäftszeiten – geschützt?	<p>RZ: Bewegungsmelder / Aktive Videoüberwachung</p> <p>Wachdienst</p> <p>Objektschutz</p> <p>Alarmierung</p> <p>Videoaufzeichnungen</p>	<p>Dedizierte Zutrittsrechte auch im Bürogebäude</p>

<b>3.15</b>	Durch welche Maßnahmen wird der Zutritt zu DV-, TK-Systemen für Unbefugte verwehrt?	Einteilung in Sicherheitszonen Automatische Zutrittskontrolle Berechtigungsausweis RZ Biometrische Zutrittskontrolle	RZ-Zertifizierung physische Sicherheit
-------------	---	---	--

## 4 Zugangskontrolle

Folgende Fragestellungen gelten für das Outsourcing „On-Premises“ mit RZ-Betrieb in Oldenburg. Bei der Einbindung von Cloud-Service Providern wird auf die Zertifizierung der Cloudprovider referenziert. Varianten die cloudspezifisch sind, werden hier allgemein aufgeführt und können im Detail variieren:

Nr.	Frage	Antwort	Anmerkungen
<b>4.1</b>	Welche Maßnahmen schützen IT-Services vor unbefugter Nutzung?	Kundenspezifische IT-Sicherheitsarchitektur gemäß Beauftragung Komplexe Passwörter Multifaktorauthentifizierung in der Administrations-umgebung sowie der Office-IT / Citrix / VPN Protokollierung der Anmeldevorgänge KAMU (Adminnetz) und Office-IT: SIEM/SOC Personalisierte Zugänge mit regelmäßiger Passwortänderung Passwort-Safe Verfahren Logische Netztrennung Anweisung zum Umgang mit administrativen Kennungen Zonentrennung mit dediziertem Adminnetz (KAMU)	Regelmäßige Awareness Maßnahmen
<b>4.2</b>	Existieren für Mitarbeiter des Auftragnehmers, die Daten des Auftraggebers verarbeiten und/ oder speichern bzw. Systeme betreuen, Hinweise über den Umgang mit administrativen Passwörtern?	Passwort-Safe Verfahren Awareness Maßnahmen Anweisung zum Umgang mit administrativen Kennungen	Zusätzlich Fachkunde und Berufserfahrung Trainingseinheiten (eLearning) zur Informationssicherheit und Datenschutz sowie Compliance und Systemmanagement

4.3	Verfügt jeder Berechtigte über ein eigenes, nur ihm bekanntes Passwort?	Personalisierte Konten im Office- und Adminnetz	Officenet, Adminnetz und Kundennetze sind logisch getrennt
4.4	Gibt es Gruppenpasswörter, die von mehreren Nutzern eingesetzt werden?	Ja, sofern technisch erforderlich (Monitoring, Backup, privilegierte Systemkennungen etc.)  Steuerung über Passwort Safe Verfahren (Berechtigungskonzept)	Anweisung zum Umgang mit administrativen Kennungen  Nachvollziehbarkeit der Nutzung auf Personen
4.5	Wird dokumentiert, wenn ein Mitarbeiter ein Gruppenpasswort benutzt hat?	Passwort Safe Verfahren (Protokollierung)  Personalisierte Administratorkennungen im Adminnetz  C-Ports-Reporter (Netzüberwachung)  System-Eventlogs der Systeme  SIEM im Adminnetz (auch im Officenet)	Bestandteil von Zertifizierungsaudits  Prozess Accessmanagement
4.6	Gibt es eine Passwortrichtlinie, die die Struktur eines Passwortes, sowie die Änderungsintervalle und Nutzung beschreibt?	Active Directory Richtlinien für Office IT und Adminnetz (KAMU)  Passwort-Richtlinie	
4.7	Wird der Zugang zu Fernwartungsplattformen abgesichert?	BITS-Fernwartungsplattform als virtuelles Adminnetz  Die Zugänge sind gemäß den Sicherheitsanforderungen unserer Kunden abgesichert	Der Betrieb der Fernwartungsplattform entspricht den Anforderungen der ISO 27001
4.8	Wird der Passwortwechsel systemseitig angefordert?	Office IT und Adminnetz IT-Betrieb (KAMU) in regelmäßigen Abständen  Multifaktorauthentifizierung (Office + KAMU)	Kundenabstimmung  Anbindung an Kunden-Infrastruktur (Accessmanagement)
4.9	Welche Mindestlänge haben Passwörter?	Office IT: min. 8 Zeichen + Komplexität + MFA  Adminnetz: min. 12 Zeichen + Komplexität + MFA	Kundenanforderungen werden entsprechend umgesetzt

<b>4.10</b>	Werden Passwörter für Services / Nutzer nur verschlüsselt abgespeichert und übertragen?	Windows-Anmeldeprozeduren (Kerberos) Secure Shell (Administration) Zertifikatsbasierte Verschlüsselung (Web)	Zusätzlich VPN (Kundenetze)
<b>4.11</b>	Gibt es für IT-Services / Nutzer eine Passwort-Historie, um zu vermeiden, dass alte Passwörter wiederverwendet werden?	Active Directory Richtlinie für Office IT und Adminnetz	
<b>4.12</b>	Werden Administrationspasswörter für IT-Services gesichert aufbewahrt?	Passwort Safe Verfahren	Personalisierter Passwort Safe steht zudem jedem Mitarbeiter zur Verfügung
<b>4.13</b>	Werden Schlüssel für Kryptographie-Verfahren gesichert aufbewahrt?	Passwort Safe Verfahren Administrationsprozesse	PIN (Import der Zertifikate)
<b>4.14</b>	Wird ein Benutzer automatisch gesperrt, wenn die Anmeldung an IT-Services fehlschlägt (Brute Force)?	Bei der Anmeldung an Systemen der Office IT und Adminnetz wird der Zugang nach fehlerhaften Anmeldeversuchen gesperrt. Zugang zum Office Netz ist Voraussetzung für den Zugang zur Administrationsplattform	
<b>4.15</b>	Wie erfolgt im Falle der Sperrung eines Administrationszugangs die Entspernung im IT-Betrieb?	Dokumentierter Service Request / Servicedesk	Bei Auffälligkeiten als Sicherheitsereignis deklariert
<b>4.16</b>	Werden über Aktivitäten auf IT-Services automatisch Protokolle erstellt?	System- und applikationsseitiges Eventlog (BS, DB, SAP, Webserver, Netzwerk etc.)  SIEM in Office- + Adminnetz	
<b>4.17</b>	Werden Protokolle und Systemzustände hinsichtlich etwaiger Unregelmäßigkeiten ausgewertet?	Operatives Team IT-Security (SIEM+SOC)  Prozess Eventmanagement (Alarmierung, Schnittstellen)  Verfügbarkeitsüberwachung von Services / Applikation / Systeme  Service Level Management  Tagesdienst im IT-Betrieb  Anlassbezogene Prüfungen (Incidents, Datenschutzvorfälle)	Zusätzlich ggf. bei Auffälligkeiten und Sicherheitsvorfällen

4.18	Wer genehmigt die Zugangsberechtigungen bei IT-Services?	Prozessverantwortliche Einheit Verantwortlicher des Auftraggebers (Weisung)	Bestellsystem IT-Buy
4.19	Von wem werden die Einstellungen im BIOS-Setup vorgenommen?	Zuständige Administratoren im IT-Betrieb	
4.20	Wird bei Arbeitsunterbrechungen eine Bildschirmsperre aktiviert?	Automatisiert nach Active Directory Richtlinie Manuelles Sperren (Awareness)	Arbeitsplatz Admin / Nutzer

## 5 Zugriffskontrolle

Nr.	Frage	Antwort	Anmerkungen
5.1	Wie werden Datenträger vor unbefugtem Lesen, Kopieren, Verändern oder Entfernen geschützt?	Verschlüsselung der Datenträger (Clients) Datenschutzcontainer Zertifizierte Entsorger (Datenträger, Papier) Zertifizierte Rückgabeprozesse (IT-Betrieb) RZ: Kameraüberwachung (reaktiv)	Serverseitige Verschlüsselungsmaßnahmen sind deziert zu beauftragen
5.2	Wo werden Backupmedien aufbewahrt?	Standortredundantes Backupkonzept Bandloses Verfahren Datenspeicherung in den RZ	Keine Verwendung von Backup Bändern mehr im IT-Betrieb Sonderlösungen sind möglich in Kundenabstimmung
5.3	Wie wird die Verwaltung von mobilen Datenträgern durchgeführt?	Liste der persönlichen Ausrüstung (z.B. IT-Buy)	Awareness der Mitarbeiter zur Handhabung mobiler Datenträger und privater Gerätschaften
5.4	Wird durch eine Zugriffskontrolle sichergestellt, dass Mitarbeiter nur auf Programme und Daten zugreifen können, die sie zur Aufgabenerfüllung benötigen (Need-to-know-Prinzip)?	IT-Betrieb: Zugriff auf Team Ebene (24/7 Betrieb) Berechtigungsvergabe: Zentrale Verwaltung mit Genehmigung (Bestellsystem) IS-Strategie Ticketsystem (fulfillment)	Need to know Prinzip auf Mitarbeiterebene ist aufgrund der Komplexität im IT-Betrieb auf Gruppenebene umgesetzt. Erfordernis durch 3 Schichten IT-Betrieb sowie Bereitschaftsdienste

5.5	Durch welche Maßnahmen wird ein Zugriff dokumentiert?	<p>Protokollierung der Systemnutzung (Sharepoint, Solution Manager, Passwort Safe etc.)</p> <p>Datenbank-Auditfunktionen</p> <p>Applikationsprotokollierung</p> <p>Logmanagement (SIEM) KAMU</p>	
5.6	Sind die Daten auf mobilen IT-Services verschlüsselt?	<p>Notebooks und Smart-Devices werden standardmäßig verschlüsselt</p> <p>Mobile Datenträger werden verschlüsselt</p>	Standardisierte Clients
5.7	Können Nutzer nur auf getestete und freigegebene Anwendungssoftware zugreifen?	<p>IT-Betrieb: Changemanagement Prozess</p> <p>Arbeitsplatz: Softwareverteilung / -portfolio und Inventarisierung, standardisierte Clients</p>	Im Einzelfall werden Administrationswerkzeuge im Fachteam vorgegeben
5.8	Werden Zugriffsrechte für IT-Services genehmigt?	<p>Disziplinarische Vorgesetzte</p> <p>Weisungsberechtigte (kundenseitig)</p>	Genehmigungs-Workflow im Bestellsystem
5.9	Werden Zugriffsrechte dokumentiert?	<p>Genehmigte Zugriffsrechte sind im Bestellsystem dokumentiert</p> <p>Die Einrichtung von Rechten wird im Ticketsystem dokumentiert</p>	
5.10	Wird sichergestellt, dass Zugriffsrechte rechtzeitig beim Ausscheiden entzogen werden?	<p>Automatisierte Sperrung der Nutzer zum Austrittsdatum sowie anlassbezogen kurzfristige Sperrung auf Anweisung</p>	Sekundär: Zeitgerechte Kündigung der Ausrüstung im Bestellsystem durch Führungskräfte
5.11	Gibt es ein Änderungsmanagement bei wesentlicher Veränderung der Systemlandschaft?	<p>Konzeption / Architektur</p> <p>IT-Betrieb: Prozess Changemanagement</p> <p>Kundenabstimmung</p>	Insbesondere bei Einführung neuer Technologien / Cloudstrategie
5.12	Wer darf die Änderungen der Systemlandschaften veranlassen?	<p>Auftraggeber: Gemäß Weisungsbefugnis / Beauftragung</p> <p>IT-Betrieb: Change Advisory Board mit Kundenabstimmung</p> <p>Office IT: CIO</p>	

## 6 Weitergabekontrolle

Nr.	Frage	Antwort	Anmerkungen
6.1	Wird der Versand von Datenträgern durch Registrierung, Begleitzettel und/ oder Lieferscheine kontrolliert?	IT-Betrieb: Im Einzelfall durch persönliche Übergabe sowie durch abgestimmte Verfahren gemäß Kundenvorgaben	Ein Versand von Datenträgern ist in der Regel nicht vorgesehen und wird nur gemäß einem abgestimmten Vorgehen zu festgelegten Zwecken autorisiert
6.2	Werden stichprobenartige Kontrollen der Mitarbeiter (Taschenkontrolle o. ä.) durchgeführt?	RZ Betrieb: Videoüberwachung Awareness der Mitarbeiter Begleitete Wartungsarbeiten (4 Augen Prinzip)	Taschenkontrollen sind im Verdachtsfall unter Einbeziehung des Betriebsrates möglich
6.3	Wie werden mobile Datenträger vernichtet?	Magnetische Datenträger: Sichere Lösungsverfahren: Zertifizierte Entsorgung  Optische Datenträger und defekte Festplatten: Zertifizierte Entsorgung  Papier: Zertifizierte Entsorgung	Verschlüsselte Datenträger
6.4	Wie werden Daten bei Übertragungen über das Internet gegen das unbefugte Lesen, Kopieren, Verändern oder Entfernen geschützt?	Logische Netzwerktrennung  Datenverschlüsselung im VPN  Verschlüsselung durch sichere Protokolle (https etc.)	
6.5	Welche Sicherheitsmaßnahmen werden bei der Übermittlung über das Internet eingesetzt?	Firewall  Intrusion Prevention System (IPS)  Virtual Private Network (VPN)  Proxyserver  Systeme zum Schadsoftwareschutz	IT-Architektur der Kundenanbindung ist abhängig von der Beauftragung unter Einbeziehung einer Schutzbedarfsanalyse
6.6	Durch welche Maßnahmen kann überprüft und festgestellt werden, ob eine unautorisierte Datenübermittlung stattgefunden hat?	Anwendungen: Abhängig vom Berechtigungskonzept und in Verantwortung der Kundenfachabteilungen  IT-Betrieb: forensische Analyse der Protokolldateien sowie SIEM in der Administrationsumgebung KAMU	Weisungen per Ticketsystem dokumentiert

6.7	Werden zur Übermittlung eingesetzte IT-Services in zertifizierten Rechenzentren betrieben?	RZ-Betrieb: Physische Sicherheit sowie RZ-Betriebsprozesse zertifiziert (TÜV Trusted Site Infrastruktur, ISO/IEC 27001)	
6.8	Sind die Server-Konsolen bei Nichtnutzung gesperrt?	RZ-Betrieb: Standard  IT-Betrieb: Admin- Arbeitsplätze automatisch Manuelle Sperrung (Win+L) Awareness der Mitarbeiter  Office IT: Automatische Sperrung bei Inaktivität	
6.9	Welche Maßnahmen werden realisiert, wenn Daten in großer Menge an Kunden übermittelt werden müssen?	Grundsatz: Nur nach legitimer Weisung und per Ticket dokumentiert  IT-Systeme: Übergabe nach 4 Augenprinzip vor Ort  Datenträger: In Abstimmung mit dem Kunden (Kurier, Einschreiben) mit vorgegebenem Verschlüsselungsverfahren	Legitimation und Verfahren sind kundenseitig abzustimmen (Einzelfälle)
6.10	Werden externe Dienstleister zur Wartung / Reparatur auf den Datenschutz verpflichtet?	Grundsätzlich werden alle Fremddienstleister auf Vertraulichkeit, Datenschutz und Regelungen zum Remotezugriff verpflichtet	
6.11	Werden die Zugänge zwecks Fernwartung nur fallbezogen freigegeben?	Verbindungsaufbau wird durch IT-Betrieb initiiert  Keine eigenmächtige Administration	

## 7 Eingabekontrolle

Nr.	Frage	Antwort	Anmerkungen
7.1	Durch welche Maßnahmen kann nachträglich überprüft und festgestellt werden, ob und von wem Daten in IT-Services eingegeben, verändert oder entfernt worden sind?	Forensische Analyse der Protokollierung im Verdachtsfall	Ohne Weisung durch den Auftraggeber werden Daten nicht eingesehen/verändert
7.2	Gibt es ein mehrstufiges Schadsoftwarekonzept?	Mehrstufiges Konzept zum Schutz vor Schadsoftware (Mail, Internet, Server, Client)	Integrität der Datenbestände wird durch Schadsoftwareschutz abgesichert (Angriffe)
7.3	Werden sicherheitsrelevante Updates und Patches für Betriebssysteme und Anwendungsprogramme regelmäßig und zeitnah eingespielt?	IT-Betrieb: Gemäß Freigabe durch Auftraggeber  Clients: Automatisierte Verteilung der Sicherheitsupdates	
7.4	Wird die Integrität und Installation von Softwarequellen überprüft?	Checksummen Dedizierte Herstellerseiten	Einschleusen von Schadsoftware wird verhindert
7.5	Wird vor umfangreichen Wartungs-, Fernwartungs- oder Reparaturarbeiten eine komplette Sicherung der betroffenen Systeme erstellt?	IT-Betrieb: Prozess Change-Management  Backupprozess	

## 8 Auftragskontrolle

Nr.	Frage	Antwort	Anmerkungen
8.1	Durch welche Maßnahmen kann nachträglich überprüft und festgestellt werden, ob eine Weisung durch den Auftraggeber erfolgte?	IT-Betrieb: Prozess Changemanagement  Dokumentation der Changes mit Freigabe durch den Kunden in den Tickets  Servicerequests sind im Ticketsystem nachvollziehbar	Mündliche Weisungen werden schriftlich fixiert. Im ausgerufenen Notfall ggf. nachträglich im Ticketsystem im vereinbarten Verfahren.
8.2	Durch welche Maßnahmen wird erreicht, dass die Verarbeitung personenbezogener Daten im Auftrag nur entsprechend den Weisungen des Auftraggebers erfolgt?	Vertraglich festgelegte Verantwortlichkeiten und dedizierte Ansprechpartner Awareness der Mitarbeiter zu rechtlichen Folgen  Forensische Untersuchungen im Verdachtsfall	Regelmäßige Rechtfertigung der Maßnahmen durch die Fachverantwortlichen bei internen Audits, Zertifizierungsaudits, Kontrollen etc.

8.3	Wer ist beim Auftragnehmer berechtigt, Weisungen vom Auftraggeber entgegenzunehmen?	Grundsatz im IT-Betrieb: Vertraglich sowie nachträglich vom Kunden legitimierte Ansprechpartner  Servicemanager  Service Desk (Rücksicherung von Dateien etc.)	Störungen und Serviceanfragen werden nicht als Weisung verstanden und vom Service Desk bzw. Fachteam bearbeitet
8.4	Wird der Auftraggeber über Service-Unterbrechungen aktiv informiert?	IT-Betrieb: Incidentmanagement Eskalationsmanagement Notfallmanagement Servicemanagement	Prozessuale Einbindung der Kundenansprechpartner gemäß betrieblicher Abstimmung (Serviceorganisation)

## 9 Verfügbarkeitskontrolle

Nr.	Frage	Antwort	Anmerkungen
9.1	Wie wird gewährleistet, dass Daten gegen zufällige Zerstörung oder Verlust geschützt sind?	Storage Area Network (SAN)  Standortübergreifendes Backupkonzept  Redundante Systemauslegung  RZ-Betrieb: Unterbrechungsfreie Stromversorgung (USV)  ÜberspannungsfILTER	Gemäß Service Level Agreement
9.2	Gibt es Notfall- und Krisenmanagement?	IT-Betrieb: Prozess Business Continuity	ISO/IEC 22301 zertifiziertes Business Continuity Management BCM
9.3	Ist das Rechenzentrum redundant ausgelegt?	IT-Betrieb: Redundantes Rechenzentrum OL1B ↔ OL2	Gemäß Kundenvertrag
9.4	Ist die zeitgerechte Wiederherstellung von Daten gewährleistet?	Mehrgenerationenkonzept Backup  Systemkonzept (Verfügbarkeiten, Wiederherstellungszeiten etc.)  Aktuelle Technologien  Notfallmanagement-Prozesse	Wiederherstellung gemäß Beauftragung

<b>9.5</b>	In welchen Intervallen wird standardmäßig eine Datensicherung durchgeführt?	Täglich: Incremental Wöchentlich: Full Gemäß Vereinbarung in der Transitionsphase / Vertrag	
<b>9.6</b>	Wird das allgemeine Backup-Verfahren regelmäßig kontrolliert?	Backup-Prozess ist u.a. Bestandteil der ISO / IEC 27001 Zertifizierung	
<b>9.7</b>	Werden Sicherungsprotokolle erstellt und geprüft?	Tägliche Sichtprüfung der Wirksamkeit durch Backup-Team	
<b>9.8</b>	Wo werden Backup-Medien aufbewahrt?	Mehrstandortkonzept Verschiedene Brandabschnitte	
<b>9.9</b>	Werden gesetzliche Aufbewahrungsfristen beachtet?	Aufbewahrungsfristen gemäß vertraglicher Vereinbarung	
<b>9.10</b>	Sind in den Rechenzentren Feuchtigkeits-, Rauch-, Wärmesensoren installiert?	Feuchtigkeitssensoren Rauchmelder Wärmesensoren Rauchererkennung	TÜV-Zertifizierung
<b>9.11</b>	Sind in den Rechenzentren entsprechend zugelassene Feuerlöscher/ Löschanlage zur Verfügung?	Regelmäßige Wartung der Feuerlöscher / Löschanlage	TÜV-Zertifizierung
<b>9.12</b>	Wird ein zuständiger Mitarbeiter bei einem Alarmsignal eines Sensors über den kritischen Zustand in den Serverräumen informiert?	Überwachung und Alarmierung	Zentrale Aufschaltung und Auswertung der Alarmierung
<b>9.13</b>	Ist die Erreichbarkeit eines zuständigen Mitarbeiters im Katastrophenfall jederzeit gewährleistet?	RZ-Betrieb: ÜBD IT-Betrieb: Dutymanager Fachlich: CIO	Bestandteil regelmäßiger Audits
<b>9.14</b>	Gibt es Eskalationsverfahren (Krisenfall)?	Notfallprozesse mit Eskalationsverfahren zur Krise	
<b>9.15</b>	Sind die Rechenzentren vor Einbruch ausreichend geschützt?	Physische Sicherheit regelmäßig zertifiziert	Siehe TSI-Zertifizierung
<b>9.16</b>	Sind die Rechenzentren entsprechend der technischen Spezifikation ausreichend klimatisiert?	Physische Sicherheit regelmäßig zertifiziert	Siehe TSI-Zertifizierung
<b>9.17</b>	Wer ist für die Einhaltung von Wartungsintervallen, der Auswahl und Beauftragung von Wartungsunternehmen verantwortlich?	RZ-Betrieb: Gebäudemanagement	TSI-Zertifizierung (RZ)

## 10 Trennungsgebot

Nr.	Frage	Antwort	Anmerkungen
10.1	Wie wird gewährleistet, dass die zu unterschiedlichen Zwecken erhobenen Daten getrennt verarbeitet werden?	<p>Softwareseitiger Ausschluss (Mandantentrennung)</p> <p>Datenbankfunktionen (Zugriffsrechte und Architektur)</p> <p>Trennung von Test- und Produktionsumgebung</p> <p>Kundenseitige Abstimmung und Festlegung im Umgang mit Testdaten</p> <p>Dedizierte IT-Systeme</p> <p>Logische Netztrennung</p>	<p>Verarbeitung gemäß Weisung. Datenschutzrechtliche Verstöße werden dem Kunden mitgeteilt – ggf. unter Einbindung der Datenschutzbeauftragten</p>

## 11 Organisation

Nr.	Frage	Antwort	Anmerkungen
11.1	Durch welche allgemeinen organisatorischen Maßnahmen werden die Anforderungen des Datenschutzes gestützt?	<p>Mitarbeiterschulungen sowie Awarenessmaßnahmen</p> <p>Datenschutzbeauftragter ist ordentlich bestellt gemäß BDSG</p> <p>Ansprechpartner für Datenschutzrechtliche Fragen durch Datenschutzbeauftragten gewährleistet</p> <p>Audit- und Kontrollverfahren sind eingerichtet</p>	<p>TOM regelmäßig Bestandteil interner und externer Audits</p>
		<p>Festgelegte Verantwortlichkeiten und Mitwirkung durch alle Führungskräfte und Mitarbeiter</p>	<p>IMS-Richtlinie</p> <p>Anforderung an die Fachkunde</p> <p>Schutzbedarfsanalyse</p>

## 12 TOM-Liste nach Stichworten

### Zutrittskontrolle

- ✓ Alarmanlage (EMA)
- ✓ Absicherung von Gebäudeschächten
- ✓ Automatisches Zutrittskontrollsystem (alle Eingänge)
- ✓ Chipkarten-Schließsystem (Einzelschließungen)
- ✓ Biometrische Zugangssperren (RZ)
- ✓ Videoüberwachung der Zugänge (RZ)
- ✓ Lichtschranken / Bewegungsmelder (RZ, Office)
- ✓ Sicherheitsschlösser
- ✓ Schlüsselregelung (Schlüsselausgabe etc.)
- ✓ Personenkontrolle beim Empfang (Plausibilität)
- ✓ Protokollierung der Besucher
- ✓ Sorgfältige Auswahl von Reinigungspersonal
- ✓ Sorgfältige Auswahl von Wachpersonal
- ✓ Tragepflicht von Mitarbeiterausweisen
- ✓ Schlüsselregelung (Schlüsselausgabe etc.)
- ✓ Tragepflicht von Berechtigungsausweisen

### Zugangskontrolle

- ✓ Zuordnung von Benutzerrechten / Adminrechten
- ✓ Sichere Passwortvergabe
- ✓ Authentifikation mit Benutzername / Passwort / Multifaktor MFA
- ✓ Einsatz von VPN-Technologie
- ✓ Sicherheitsschlösser (Kensington) beim Einsatz mobiler Endgeräte
- ✓ Sorgfältige Auswahl von Reinigungspersonal
- ✓ Sorgfältige Auswahl von Wachpersonal
- ✓ Einsatz von Intrusion-Detection-Systemen
- ✓ Verschlüsselung von mobilen Datenträgern
- ✓ Verschlüsselung von Smartphone-Inhalten
- ✓ Verschlüsselung von Datenträgern in Notebooks
- ✓ Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten / Mobile Device Management)
- ✓ Einsatz von Anti-Viren-Lösungen

- ✓ Einsatz Perimeter-Firewall
- ✓ Einsatz hostbasierte-Firewall
- ✓ Automatische Bildschirmsperre
- ✓ Clean Desk Grundsatz
- ✓ Praxisleitfaden Informationssicherheit und Datenschutz

### **Zugriffskontrolle**

- ✓ Berechtigungskonzepte
- ✓ Rechteverwaltung durch zuständige Systemadministratoren
- ✓ Anforderungsbasierte Trennung der Zugriffsrechte
- ✓ Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel, Komplexität
- ✓ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- ✓ Löschung von Datenträgern vor Wiederverwendung
- ✓ Ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
- ✓ Einsatz von Aktenvernichtern bzw. Dienstleister mit Datenschutz-Gütesiegel
- ✓ Verschlüsselung von Datenträgern

### **Weitergabekontrolle**

- ✓ Einrichtungen von Standleitungen bzw. VPN-Tunneln
- ✓ Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- ✓ E-Mail-Verschlüsselung (Standard: Transportverschlüsselung)
- ✓ Beim physischen Transport sichere Transportbehälter/-verpackungen und sorgfältige Auswahl von Transportpersonal und -fahrzeugen
- ✓ Behandlung gemäß der Klassifizierung vertraulich / geheim

### **Eingabekontrolle**

- ✓ Einsatz geprüfter Software
- ✓ Updates
- ✓ Schadsoftwareschutz

**Auftragskontrolle**

- ✓ Auswahl vertrauenswürdiger Auftragnehmer mit geeigneten Sicherheitsmaßnahmen
- ✓ schriftliche Weisungen (Ticketsystem)
- ✓ Verpflichtung der Mitarbeiter zur Informationssicherheit / Vertraulichkeit
- ✓ Ordentliche Bestellung des Datenschutzbeauftragten
- ✓ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- ✓ Kontrollrechte des Auftraggebers
- ✓ laufende Überprüfung der Sicherheitsmaßnahmen

**Verfügbarkeitskontrolle**

- ✓ Redundante IT-Architektur gemäß SLA
- ✓ Notfall- und Krisenmanagement / Business Continuity Management (ISO 22301)
- ✓ Zertifizierte Rechenzentren
- ✓ Unterbrechungsfreie Stromversorgung (USV)
- ✓ Klimaanlage in Serverräumen
- ✓ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- ✓ Feuer- und Rauchmeldeanlagen
- ✓ Feuerlöschanlage in Serverräumen
- ✓ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- ✓ Erstellen eines Backup- & Recoverykonzepts
- ✓ Testen von Datenwiederherstellung
- ✓ Erstellen eines Notfallplans
- ✓ Redundante Datensicherung in verschiedenen RZ
- ✓ Hochwasser: RZ über der max. Wassergrenze

**Trennungsgebot**

- ✓ Logische Mandantentrennung (softwareseitig)
- ✓ Nach Kundenanforderung: Umsetzung physikalische Mandantentrennung
- ✓ Berechtigungskonzept
- ✓ Festlegung von Datenbankrechten
- ✓ Trennung von Produktiv-, Entwicklungs- und Testsystem

**Pseudonymisierung / Anonymisierung**

- ✓ Kundenabstimmung / Weisung
- ✓ Sorgfältiger Umgang mit Testdaten / zwecks Fehleranalyse
- ✓ Grundsatz der Anonymisierung in Abstimmung mit Kunden

**Datenschutzmanagement**

- ✓ Integriertes Managementsystem für QM, ISMS, DSMS, Compliance, Arbeitsschutz, BCM
- ✓ Verantwortlichkeiten
- ✓ Mitarbeiterawareness
- ✓ Trainingseinheiten

## 13 Dokumentenlenkung

Die Weiterentwicklung dieses Dokumentes obliegt dem betrieblichen Datenschutzbeauftragten der BTC und erfolgt mit den zuständigen Fachansprechpartnern der aufgeführten Unternehmen.

Die Weitergabe dieses Dokumentes ist ausschließlich an Vertragskunden der BTC sowie in der Phase einer konkreten Vertragsanbahnung zulässig.

Die weitere Nutzung des Dokumentes oder Teile daraus zu eigenen internen Zwecken durch Vertragskunden ist zulässig.

### Verantwortlich für den Inhalt:

- Maik Evers, betrieblicher Datenschutzbeauftragter, BTC und BTC IT-Services
- Matthias Dierkes, Informationssicherheitsbeauftragter BTC IT-Services
- Walter Schultz, IT-Sicherheitsbeauftragter BTC IT-Services

### Freigabe:

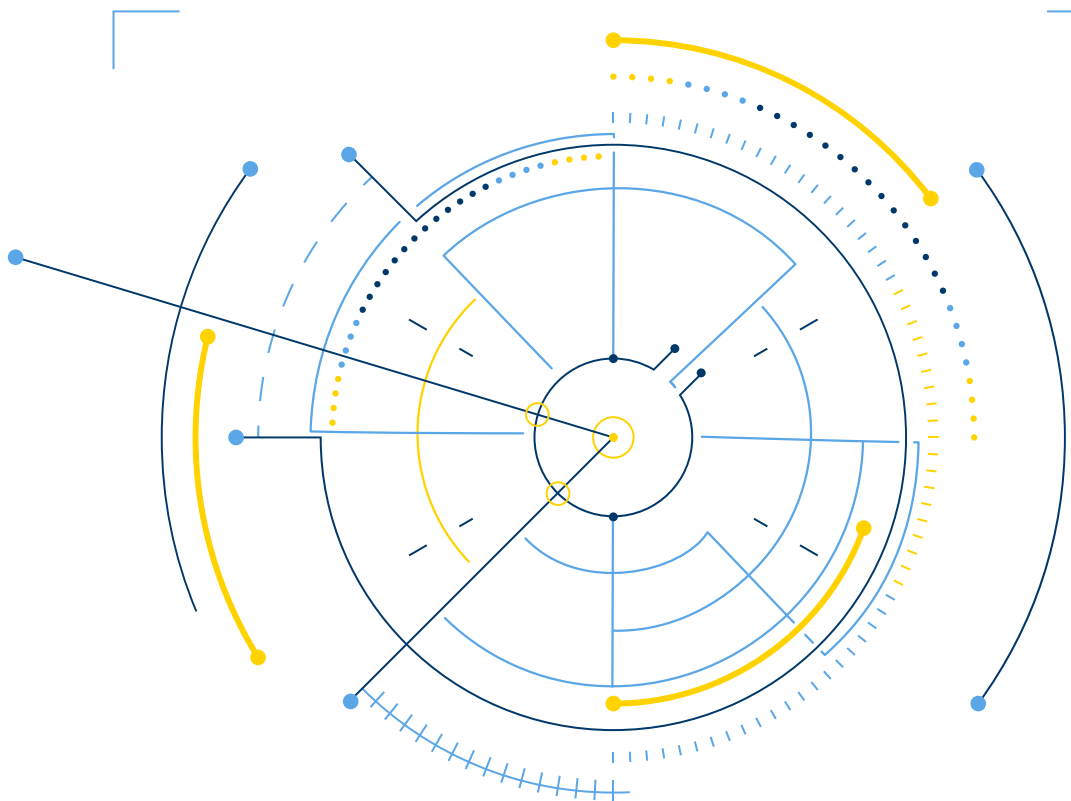
Informationssicherheitsbeauftragter und betrieblicher Datenschutzbeauftragter BTC AG

Version	Kapitel	Gegenstand der Änderung	Autor	Datum
1.0	Alle	Überprüfung / Ergänzung / Korrektur / bisheriger TOM-Listen nach Maßgabe der DSGVO	Maik Evers	13.03.2018
1.1	Alle	Überprüfung und Corporate Design	Maik Evers	22.02.2018
1.2	2,12	Überprüfung und Korrektur Kapitelnummerierung	Maik Evers	29.04.2019
1.3	Alle	Ergänzung	Maik Evers	28.06.2019
1.4	3-7	Prüfung und Aktualisierung	Maik Evers	16.06.2020
1.5	Alle	Prüfung und redaktionelle Anpassung	Maik Evers	03.03.2021
1.6	Alle	Redaktionelle Überarbeitung / Korrektur / Ergänzung	Maik Evers Walter Schultz	19.07.2022
		Redaktionelle Überarbeitung / Korrektur / Ergänzung	Walter Schultz Matthias Dierkes	04.07.2023

## Managed Cloud Services

Konzeption und Übersicht der technischen und organisatorischen Maßnahmen gem. Artikel 32 DSGVO

Spezifische Darstellung zum Betrieb von Cloudservices



Ihre **Vision**  
ist unser **Fokus!**

Verwirklichen wir sie gemeinsam.

## Inhaltsverzeichnis

<b>1</b>	<b>Konzeption der Datenschutzrechtlichen Maßnahmen .....</b>	<b>3</b>
1.1	Geltungsbereich .....	3
1.2	Meldepflichten .....	3
1.3	Kundenkorrespondierende Maßnahmen .....	4
1.4	Grundwerte zum Datenschutz / Informationssicherheit .....	6
1.5	Standarddatenschutzmodell (SDM) .....	7
1.6	Systematisierung der rechtlichen Anforderungen mit Hilfe der Gewährleistungsziele .....	8
1.7	Gewährleistungsziele .....	9
<b>2</b>	<b>Zertifizierungen und Testate .....</b>	<b>11</b>
2.1	BTC Managed Cloud Services.....	11
2.2	AWS .....	11
2.3	Microsoft.....	12
<b>3</b>	<b>Maßnahmen zur Erreichung der Gewährleistungsziele .....</b>	<b>12</b>
3.1	Vertraulichkeit .....	12
3.2	Verfügbarkeit.....	15
3.3	Integrität .....	16
3.4	Nichtverkettung .....	17
3.5	Transparenz .....	18
3.6	Intervenierbarkeit .....	20
3.7	Datenminimierung .....	21
<b>4</b>	<b>Dokumentenlenkung.....</b>	<b>23</b>
4.1	Abkürzungen .....	23
4.2	Quellen .....	23

# 1 Konzeption der Datenschutzrechtlichen Maßnahmen

## 1.1 Geltungsbereich

Grundsätzlich gelten für die von der BTC selbst eingesetzten Systeme die gleichen datenschutzrechtlichen Anforderungen wie für den Betrieb von Kundensystemen, auf denen personenbezogene Daten verarbeitet werden (Outsourcing).

Der IT-Betrieb der Betriebsmittel, die zur Leistungserbringung z. B. für die interne Organisation, Dokumentation, Kommunikation und Abrechnung erforderlich ist (Office IT), wird in diesem Dokument nicht dargelegt. Stattdessen wird auf die allgemeingültige Konzeption und Beschreibung der technischen und organisatorischen Maßnahmen verwiesen (Hauptdokument).

Sämtliche spezifischen Maßnahmen zum Betrieb von Cloudservices werden im Folgenden aufgeführt:

- Managed AWS-Infrastrukturbetrieb
- Managed Azure-Infrastrukturbetrieb
- Hybride Betriebsmodelle (Cloud und On Premise)

Dabei wird die BTC als Dienstleister auf Weisungen der Kunden agieren und keine eigene Cloud-Infrastruktur zur Verfügung stellen.

Im Hinblick auf die erforderliche Transparenz und notwendigen Wissenstransfer bei unseren Kunden wird dieses Dokument wesentliche Informationen zusammenfassen. Die Rechte und Pflichten der Parteien ergeben sich allein aus den vertraglichen Vereinbarungen und den gesetzlichen Bestimmungen zum Datenschutz. Insofern können aus dieser Dokumentation keine Ansprüche abgeleitet werden. Die aufgeführten Maßnahmen können im Einzelnen gemäß der vertraglichen Vereinbarung sowie aufgrund der kontinuierlichen Fortentwicklung der Kundenanforderungen variieren und ein höheres Sicherheitsniveau erwirken.

Im Zuge zahlreicher Audits wird die Schutzwirkung einzelner Maßnahmen regelmäßig überwacht und durch interne Kontrollmaßnahmen bestätigt.

## 1.2 Meldepflichten

Grundsätzlich erhebt die BTC und BTC IT Services als verantwortliche Stelle selbst Daten von ihren Mitarbeitern und setzt eigene Webservices zur Außendarstellung ein und ist dafür die verantwortliche Stelle im datenschutzrechtlichen Sinne. Diesbezüglich werden gemäß der DSGVO die gesetzlichen Informations- und Meldepflichten gegenüber den Betroffenen und der Datenschutz-Aufsichtsbehörde eingehalten.

Im Rahmen unserer beauftragten Leistungserbringung sind unsere Kunden und Partner die verantwortliche Stelle im Rahmen der Auftragsverarbeitung. Jegliche Anfragen von Betroffenen und der anfragenden Aufsichtsbehörde werden unverzüglich an die von Ihnen mitgeteilten Ansprechpartner und Meldestellen weitergeleitet, um das weitere Vorgehen und mögliche Unterstützungsleistungen abzustimmen und zu priorisieren.

Zudem stimmen wir die darüberhinausgehenden Meldepflichten im Rahmen der Vereinbarung zum Datenschutz (DSGVO Art. 28) sowie der gesetzlichen Anforderungen (DSGVO Art. 33-36) mit Ihnen ab und kommen diesen nach.

### 1.3 Kundenkorrespondierende Maßnahmen

Die Leistungserbringer werden in ihrem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht werden. Sie werden technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Kunden treffen, die den Anforderungen der Datenschutz- Grundverordnung gemäß Art. 32 DSGVO genügen.

Es sind dabei technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen.

Unseren Kunden werden die technischen und organisatorischen Maßnahmen kategorisch in diesem Dokument sowie auftragsspezifisch in angemessener Weise zur Kenntnis gebracht. Die Eignung dieser Maßnahmen kann in die kundeneigenen Risikobewertungen einfließen. Ein angemessenes Schutzniveau ist zu erreichen.

Bei besonderen Kategorien von personenbezogenen Daten oder bei hohen Risiken für die Betroffenenrechte ist es die Aufgabe unserer Kunden und Partner, eine Datenschutzfolgeabschätzung durchzuführen (DSGVO Art. 35) und in Abstimmung der Ansprechpartner für die im Rahmen des Vertrages anfallenden Datenschutzfragen ggf. spezielle technische Maßnahmen anzuweisen.

Im IT-Betrieb sowie bei dem Einsatz der Office-IT wird insbesondere die Aufrechterhaltung der Zertifizierung des Managementsystems für Informationssicherheit nach der international anerkannten Norm ISO/IEC 27001 als ein geeigneter Nachweis für die Wirksamkeit der technischen und organisatorischen Maßnahmen anerkannt und dient als Basis für datenschutzrechtliche Kontrollmaßnahmen.

Die technischen und organisatorischen Maßnahmen im IT-Betrieb der BTC IT Services sind grundsätzlich Bestandteil des integrierten Managementsystems für Informationssicherheit, Business Continuity (Notfall- und Krisenmanagement) sowie der ITIL-orientierten Betriebsprozesse.

Kundenspezifische Ausprägungen der vereinbarten Maßnahmen münden in der kundenspezifischen Konzeption der IT-Architektur und in die vereinbarten Freigabeprozesse bei der Einführung eines IT-Services sowie im Transition- und Change-Management (ITIL).

Das integrierte Managementsystem beinhaltet ein Risikomanagement, welches insbesondere die Eignung der getroffenen Risikobehandlungsmaßnahmen prozessual bewertet. Darüber hinaus werden operative Risiken zum Beispiel bei Bekanntwerden kritischer Schwachstellen im IT-Betrieb bewertet und erforderliche Maßnahmen abgestimmt. Diese werden mit den zugeteilten Ansprechpartnern für die Freigabe von Maßnahmen im Changemanagement abgestimmt. Bei Gefahr im Verzug werden unter Umständen die Freigabeprozesse umgangen und im Nachgang über die erforderlichen Maßnahmen zur Gefahrenabwehr mitgeteilt.

Sämtliche Informationssysteme sind im IT-Betrieb in einer strukturierten und kundenspezifischen IT- Inventarisierung geführt. Diese Informationen können Ihnen ggf. bei der Erarbeitung Ihres Verzeichnisses der Verarbeitungstätigkeiten (Verfahrensverzeichnis) behilflich sein.

Die getroffenen Sicherheitsmaßnahmen werden im IT-Betrieb standardmäßig im Systemkonzept (Architekturkonzept, Service Level, ggf. Betriebsführungshandbuch etc.) dokumentiert.

Fachspezifische Informationen zum Datenfluss, zum Datenexport / Schnittstellen sowie die zulässigen Speicherorte und Berechtigungskonzepte liegen dem IT-Betrieb / dem Fachsupport in der Regel nicht in dokumentierter Form vor. Sofern dies zur datenschutzrechtlichen Bewertung aus Kundensicht erforderlich ist, kann mit Unterstützung des IT-Betriebes eine entsprechende Dokumentation mittels einer beauftragten Leistungserbringung erfolgen.

Zur Erfüllung Ihrer datenschutzrechtlichen Pflichten unterstützen unsere Fach- und Kundenansprechpartner mit Lösungen für die in ihrem Datenschutzmanagement identifizierten Handlungsbedarfe.

Für die Erfüllung der datenschutzrechtlich erforderlichen Maßnahmen ist zusammengefasst aus unserer Sicht eine enge Zusammenarbeit in folgenden Aufgabenfeldern erforderlich:

- **Verarbeitungsverzeichnis**
  - ✓ Wir benötigen von Ihnen eine Übersicht der Kategorien ihrer Datenverarbeitung, auf die sich unsere Tätigkeiten gemäß Leistungsvertrag bezieht und aus der die Risiken für die Betroffenenrechte (Schutzbedürftigkeit) sowie die Verarbeitung besonderer Kategorien (Artikel 9 DSGVO) hervorgeht.
  - ✓ Wir halten alle technischen Informationssysteme / IT-Systeme in einem kundenspezifisch geführten, elektronischen Inventar innerhalb der Cloud-Administration.
  - ✓ Die Beschreibung der allgemein anwendbaren Maßnahmen sind in diesem Dokument aufgeführt. Fachspezifische Maßnahmen sind den vereinbarten Dokumentationen zu entnehmen (Aufzeichnungen, Fachkonzepte, Leistungsbeschreibung etc.).
- **Unterstützung bei der Datenschutzfolgeabschätzung**
  - ✓ Wir können Sie dabei unterstützen, bei der Datenverarbeitung mit besonders hohen Risiken für Betroffene oder besonderer Kategorien von Daten
    - die Eignung der getroffenen Maßnahmen gemeinsam zu bewerten und
    - Empfehlungen für die Erweiterung der bisherigen technischen Maßnahmen zu erarbeiten und
    - ggf. durch Erweiterung der Leistungsvereinbarung umzusetzen
- **Anfragen durch Aufsichtsbehörden**
  - ✓ Unserer Pflicht zur Zusammenarbeit kommen wir vollumfänglich nach. Wir werden alle verfügbaren Ansprechpartner unverzüglich über Anfragen der Aufsichtsbehörden informieren und das weitere Vorgehen mit Ihnen abstimmen.
  - ✓ Sollten Sie durch eine Aufsichtsbehörde konsultiert werden, unterstützen unsere Fachkräfte Sie mit höchster Priorität in allen Belangen, die in unserer Verantwortlichkeit liegen und darüber hinaus stehen wir Ihnen soweit erforderlich mit Rat und Tat zur Seite.
  - ✓ Beachten Sie bitte, dass zahlreiche gesetzliche Forderungen aus der DSGVO und dem BDSG der verantwortlichen Stelle zugeordnet sind und diese nicht delegiert werden können.
- **Stand der Technik**
  - ✓ Das allgemeine technische Sicherheitsniveau wird unter Berücksichtigung wirtschaftlicher Aspekte angemessen aufrechterhalten und entspricht grundsätzlich dem Stand der Technik. In der Regel wird durch den gewählten Cloudprovider der Stand der Technik eingesetzter Services fortentwickelt – es wird grundsätzlich empfohlen, diese Vorteile zu nutzen und die Betriebsverantwortung z.B. für Release- und Patchmanagement eigenständig zu gestalten. Die Sicherheit der zugrunde liegenden Cloudtechnologie verantwortet der Cloudprovider eigenständig.
  - ✓ Die beauftragten Services und Dienstleistungen werden mit Ihnen gemeinsam innerhalb der Auftragsanbahnung bis zur Auftragsabwicklung abgestimmt und zur Kenntnis gebracht. Nach wirtschaftlichen und risikoorientierten Bewertungsgrundlagen kann der Einsatz zusätzlicher spezieller Sicherheitstechnologien zur Angriffserkennung und regelmäßiger Einsatz von Prüfwerkzeugen zur Schwachstellenermittlung erfolgen.

- ✓ Insbesondere Anforderungen an die Verschlüsselung, Pseudonymisierung und Anonymisierung und die Handhabung in der täglichen Praxis bedürfen eine enge fachliche Abstimmung (Testdaten, Webservices, etc.).
- ✓ Hohe Risiken sowie besondere Kategorien von personenbezogenen Daten (DSGVO) können ggf. nach aktuellstem Stand der Technik geltenden Sicherheitstechniken erfordern, die wir gemäß Ihrer Bewertung und Leistungsvertrag implementieren können.
- Datenschutz durch Technik und Voreinstellungen
  - ✓ Bei der Konzeption der Services haben Sie direkten Einfluss auf die technische Gestaltung und der Voreinstellungen zur Erhebung etwaiger Daten, die Einfluss auf die Betroffenenrechte nehmen.
- Meldung von Datenschutzverstößen
  - ✓ Verletzungen des Schutzes von personenbezogenen Daten werden wir Ihnen unverzüglich mitteilen, so dass Sie Ihrer Meldepflicht bei hohen Risiken für Betroffenenrechte unverzüglich die Aufsichtsbehörde nachkommen können.
  - ✓ Unzulässige oder zweifelhafte Anfragen zur Datenverarbeitung werden umgehend an die von Ihnen genannten Ansprechpartner für Datenschutzfragen (Datenschutz-beauftragter, Fachabteilung, etc.) mitgeteilt.
- Bewertung operativer Risiken
  - ✓ Je nach vertraglicher Vereinbarung können technische Schwachstellen ggf. automatisiert ermittelt und im Rahmen der vereinbarten Wartungsfenster behoben werden.
  - ✓ Bei Bekanntwerden von Schwachstellen mit besonders hohen Risiken, ist eine enge Abstimmung und eine kundenseitige Priorisierung der einzuleitenden Maßnahmen erforderlich.
  - ✓ Bei Datenverarbeitungen von Daten mit besonderen Risiken oder besondere Kategorien von personenbezogenen Daten (sofern zutreffend) sind die Verfahren entsprechend anzupassen und eine rechtzeitige Beseitigung von technischen und organisatorischen Maßnahmen zu erwirken.

## 1.4 Grundwerte zum Datenschutz / Informationssicherheit

Folgende Maßnahmen werden standardmäßig im Cloud-Betrieb in den Managementsystemen berücksichtigt und mit der Verarbeitung von personenbezogener Daten auf Dauer zugesichert:

Begriff	Erklärung
<b>Vertraulichkeit</b>	Die Fähigkeit zum Schutz vor unbefugtem Zugriff
<b>Integrität</b>	Die Korrektheit der personenbezogenen Daten
<b>Verfügbarkeit</b>	Die zeitgerechte Bereitstellung der Daten
<b>Belastbarkeit</b>	Die Fähigkeit, die Systeme fehlerresistent betreiben zu können

Insbesondere die Anforderungen an die Verfügbarkeit und die Belastbarkeit sind standardmäßig vertraglich durch entsprechende Leistungsangaben (Service Level Agreements, Leistungsscheine etc.) festgelegt. Daraus resultiert eine entsprechende Cloud-Architektur wie z. B. eine redundante Datenhaltung, Lastverteilung, die schnelle Wiederherstellung der Daten sowie eine performante Anbindung an das Unternehmens-Netzwerk / VPN / Internet und Perimeterschutz (Firewall, Routing etc.).

Die Cloud-Betriebsprozesse werden nach der ISO/IEC 27001 / 27017 (Managementsystem für Informationssicherheit) und der DIN ISO 9001 (Managementsystem für Qualitätsmanagement) in regelmäßigen Audits auf Wirksamkeit geprüft.

Als Voraussetzung zur Erreichung der vorgenannten Zertifizierungen sowie der gesetzlichen Vorgaben finden jährlich dazu interne Audits und datenschutzrechtliche Kontrollen statt. Darüber hinaus ist bei jedem externen Audit im IT-Betrieb der Datenschutzbeauftragte involviert.

Nach unserem Kenntnisstand sind dies hinreichende Garantien für die Eignung der getroffenen Maßnahmen zum Schutz personenbezogener Daten und damit verbundenen datenschutzrechtlichen Betroffenenrechte. Dies gilt insbesondere bezüglich der Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von oder unbefugter Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden, insbesondere wenn dies zu einem physischen, materiellen oder immateriellen Schaden der Betroffenen führen würde.

## 1.5 Standarddatenschutzmodell (SDM)

Im Hinblick auf die Empfehlungen der Datenschutz-Aufsichtsbehörden wurden die Grundwerte aus der DSGVO durch die Gewährleistungsziele des Standard-Datenschutzmodells (SDM) weitergehend spezifiziert

Bei dem SDM handelt es sich um ein abgestimmtes, transparentes und nachvollziehbares System, um die rechtlichen Anforderungen der DSGVO in technische und organisatorische Maßnahmen (TOM) zu überführen. Ebenso dient es zukünftig vermehrt den Aufsichtsbehörden als ein einheitliches System zur datenschutzrechtlichen Bewertung der Verarbeitung personenbezogener Daten. Veröffentlicht wird das SDM vom „Arbeitskreis Technik der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder“.

Gewährleistungsziele:

- (1) Vertraulichkeit
- (2) Integrität
- (3) Verfügbarkeit
- (4) Transparenz
- (5) Nichtverkettung
- (6) Datenminimierung
- (7) Intervenierbarkeit

Den Empfehlungen aus dem SDM folgen wir mit diesem Dokument, um das vorherrschende besondere Augenmerk der Aufsichtsbehörden und Kunden beim Einsatz von Cloudservices bestmöglich mit einer umfangreichen Beschreibung der umgesetzten Maßnahmen und zugrunde liegender Konzeption zu begegnen.

## 1.6 Systematisierung der rechtlichen Anforderungen mit Hilfe der Gewährleistungsziele

Zuordnung der Gewährleistungsziele des SDM zu den rechtlichen Anforderungen der DSGVO.

Anforderungen der DSGVO	Gewährleistungsziele
Transparenz für Betroffene (Art. 5 Abs. 1 lit a, Art. 12 Abs. 1 und 3 bis Art. 15, Art. 34 DS-GVO)	Transparenz
Zweckbindung (Art. 5 Abs. 1 lit. b DS-GVO)	Nichtverkettung
Datenminimierung (Art. 5 Abs. 1 lit. c DS-GVO)	Datenminimierung
Richtigkeit (Art. 5 Abs. 1 lit. d DS-GVO)	Integrität
Speicherbegrenzung (Art. 5 Abs. 1 lit. e DS-GVO)	Datenminimierung
Integrität (Art. 5 Abs. 1 lit. f, Art. 32 Abs. 1 lit. b, DS-GVO)	Integrität
Vertraulichkeit (Art. 5 Abs. 1 lit. f, Art. 28 Abs. 3 lit. b, Art. 29, Art. 32 Abs. 1 lit. b, Art. 32 Abs. 4, Art. 38 Abs. 5 DS-GVO)	Vertraulichkeit
Rechenschafts- und Nachweisfähigkeit (Art. 5 Abs. 2, Art. 7 Abs. 1, Art. 24 Abs. 1, Art 28 Abs. 3 lit. a, Art. 30, Art. 33 Abs. 5, Art. 35, Art. 58 Abs. 1 lit. a und lit. e DS-GVO)	Transparenz
Identifizierung und Authentifizierung (Art. 12 Abs. 6 DS-GVO)	Intervenierbarkeit
Unterstützung bei der Wahrnehmung von Betroffenenrechten (Art. 12 Abs. 2 DS-GVO)	Intervenierbarkeit
Berichtigungsmöglichkeit von Daten (Art. 5 lit. d, Art. 16 DS-GVO)	Intervenierbarkeit
Löschbarkeit von Daten (Art. 17 Abs. 1 DS-GVO)	Intervenierbarkeit
Einschränkbarkeit der Verarbeitung von Daten (Art. 18 DS-GVO)	Intervenierbarkeit
Datenübertragbarkeit (Art. 20 Abs. 1 DS-GVO)	Intervenierbarkeit
Eingriffsmöglichkeit in Prozesse automatisierter Entscheidungen (Art. 22 Abs. 3 DS-GVO)	Intervenierbarkeit
Fehler- und Diskriminierungsfreiheit beim Profiling (Art. 22 Abs. 3, 4 i. V. m. ErwGr. 71)	Integrität
Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)	Datenminimierung, Intervenierbarkeit
Verfügbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)	Verfügbarkeit
Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)	Verfügbarkeit, Integrität, Vertraulichkeit
Wiederherstellbarkeit (Art. 32 Abs. 1 lit. b, lit. c DS-GVO)	Verfügbarkeit

Evaluierbarkeit (Art. 32 Abs. 1 lit. d DS-GVO)	<i>Umsetzung erfolgt prozessual im IMS (Risiken und Chancen, Interne sowie externe Audits)</i>
Behebung und Abmilderung von Datenschutzverletzungen (Art. 33 Abs. 3 lit. d, 34 Abs. 2 DS-GVO)	Integrität, Intervenierbarkeit, Vertraulichkeit, Verfügbarkeit
Angemessene Überwachung der Verarbeitung (Art. 32, 33, 34 DS-GVO)	Transparenz, Integrität
Einwilligungsmanagement (Art. 4 Nr. 11, Art. 7 Abs. 4 DS-GVO)	Transparenz, Intervenierbarkeit
Umsetzung aufsichtsbehördlicher Anordnungen (Art. 58 Abs. 2 lit. f und lit. j)	Intervenierbarkeit

## 1.7 Gewährleistungsziele

Nachfolgend werden die Gewährleistungsziele zusammenfassend beschrieben:

### Vertraulichkeit

Das Gewährleistungsziel Vertraulichkeit bezeichnet die Anforderung, dass keine unbefugte Person personenbezogene Daten zur Kenntnis nehmen oder nutzen kann. Unbefugte sind nicht nur Dritte außerhalb der verantwortlichen Stelle, sondern auch Beschäftigte von technischen Dienstleistern, die zur Erbringung der Dienstleistung keinen Zugriff zu personenbezogenen Daten benötigen, oder Personen in Organisationseinheiten, die keinerlei inhaltlichen Bezug zu einer Verarbeitungstätigkeit oder zu der jeweiligen betroffenen Person haben. Die Vertraulichkeit personenbezogener Daten ist auch dann sicherzustellen, wenn die unterliegenden Systeme und Dienste unerwartet hoher Last unterliegen.

### Verfügbarkeit

Das Gewährleistungsziel Verfügbarkeit bezeichnet die Anforderung, dass der Zugriff auf personenbezogene Daten und ihre Verarbeitung unverzüglich möglich ist und sie ordnungsgemäß im vorgesehenen Prozess verwendet werden können. Dazu müssen sie im Zugriff von Berechtigten liegen und die vorgesehenen Methoden zu deren Verarbeitung müssen auf sie angewendet werden können. Die Verfügbarkeit umfasst die konkrete Auffindbarkeit von Daten z. B. durch Datenmanagement-Systeme, strukturierte Datenbanken und Suchfunktionen und die Fähigkeit der verwendeten technischen Systeme, Daten auch für Menschen angemessen darzustellen. Darüber hinaus müssen zur Umsetzung der Verfügbarkeit Maßnahmen ergriffen werden, die sicherstellen, dass personenbezogene Daten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können. Es müssen auch Maßnahmen umgesetzt werden, die die Verfügbarkeit der personenbezogenen Daten und der Systeme und Dienste, die diese verarbeiten, garantieren, wenn diese unter einer der Verarbeitung angemessenen zu erwartenden Last stehen und im Falle unerwartet hoher Last sicherstellen, dass der Schutz der personenbezogenen Daten nicht gefährdet ist (Belastbarkeit).

## **Integrität**

Das Gewährleistungsziel Integrität bezeichnet einerseits die Anforderung, dass informationstechnische Prozesse und Systeme die Spezifikationen kontinuierlich einhalten, die zur Ausübung ihrer zweckbestimmten Funktionen für sie festgelegt wurden. Integrität bezeichnet andererseits die Eigenschaft, dass die zu verarbeitenden Daten unversehrt, vollständig, richtig und aktuell bleiben. Abweichungen von diesen Eigenschaften müssen ausgeschlossen werden oder zumindest feststellbar sein, damit sie berücksichtigt und korrigiert werden können. Dies gilt auch dann, wenn die unterliegenden Systeme und Dienste unerwartet hoher Last unterliegen (Belastbarkeit).

## **Datenminimierung**

Das Gewährleistungsziel Datenminimierung erfasst die grundlegende datenschutzrechtliche Anforderung, die Verarbeitung personenbezogener Daten auf das dem Zweck angemessene, erhebliche und notwendige Maß zu beschränken. Datenminimierung konkretisiert und operationalisiert im Verarbeitungsprozess den Grundsatz der Notwendigkeit, der von diesem Prozess insgesamt wie auch von jedem seiner Schritte verlangt, nicht mehr personenbezogene Daten zu verarbeiten, als für das Erreichen des Verarbeitungszwecks benötigt werden.

## **Nichtverkettung**

Das Gewährleistungsziel Nichtverkettung bezeichnet die Anforderung, dass personenbezogene Daten nicht zusammengeführt, also verkettet, werden. Sie ist insbesondere dann faktisch umzusetzen, wenn die zusammenzuführenden Daten für unterschiedliche Zwecke erhoben wurden. Neben der Pseudonymisierung sind hierfür auch Maßnahmen geeignet, mit denen die Weiterverarbeitung organisations- bzw. systemseitig getrennt von der Ursprungsverarbeitung geschieht.

## **Transparenz**

Das Gewährleistungsziel Transparenz bezeichnet die Anforderung, dass in einem unterschiedlichen Maße sowohl Betroffene, als auch die Betreiber von Systemen sowie zuständige Kontrollinstanzen erkennen können, welche Daten wann und für welchen Zweck bei einer Verarbeitungstätigkeit erhoben und verarbeitet werden, welche Systeme und Prozesse dafür genutzt werden, wohin die Daten zu welchem Zweck fließen und wer die rechtliche Verantwortung für die Daten und Systeme in den verschiedenen Phasen einer Datenverarbeitung besitzt.

## **Intervenierbarkeit**

Das Gewährleistungsziel Intervenierbarkeit bezeichnet die Anforderung, dass den betroffenen Personen die ihnen zustehenden Rechte auf Benachrichtigung, Auskunft, Berichtigung, Löschung Einschränkung, Datenübertragbarkeit, Widerspruch und Erwirkung des Eingriffs in automatisierte Einzelentscheidungen bei Bestehen der gesetzlichen Voraussetzungen unverzüglich und wirksam gewährt werden und die verarbeitende Stelle verpflichtet ist, die entsprechenden Maßnahmen umzusetzen.

## 2 Zertifizierungen und Testate

Nachfolgend führen wir die relevanten Zertifizierungen des Marktangebots Managed Cloud Services sowie der Public Cloud Provider auf. Die Zertifikate können auf Anfrage bereitgestellt werden.

### 2.1 BTC Managed Cloud Services

- ISO9001
- ISO27001
- ISO27017

### 2.2 AWS

AWS weist eine Vielzahl von weltweiten Zertifizierungsstandards auf. Nachfolgend sind alle für den deutschen Markt relevanten Zertifizierungen die AWS nachweisen kann dargestellt.



- |             |  |
|-------------|--|
| • BSI C5    | Cloud Computing Compliance Controls Catalog                                  |
| • SOC 1/2/3 | Sicherheits-, Verfügbarkeits- und Vertraulichkeitsbericht                    |
| • ISO9001   | Weltweiter Qualitätsstandard: International Organization for Standardization |
| • ISO 27001 | Informationssicherheitsmanagement  |
| • ISO 27017 | Informationssicherheitsmaßnahmen im Cloud Umfeld                             |
| • ISO 27018 | Schutz personenbezogener Daten bei AV in der Public Cloud                    |

## 2.3 Microsoft

Microsoft weist eine Vielzahl von weltweiten Zertifizierungsstandards auf. Nachfolgend sind alle für den deutschen Markt relevanten Zertifizierungen die Microsoft nachweisen kann dargestellt.



- BSI C5 Cloud Computing Compliance Controls Catalog
- SOC 1/2/3 Sicherheits-, Verfügbarkeits- und Vertraulichkeitsbericht
- ISO9001 Weltweiter Qualitätsstandard: International Organization for Standardization
- ISO 27001 Informationssicherheitsmanagement
- ISO 27017 Informationssicherheitsmaßnahmen im Cloud Umfeld
- ISO 27018 Schutz personenbezogener Daten bei AV in der Public Cloud
- ISO27701 Datenschutzmanagement auf Basis eines ISMS

## 3 Maßnahmen zur Erreichung der Gewährleistungsziele

### 3.1 Vertraulichkeit

Maßnahme	Umsetzung
Festlegung eines Berechtigungs- und Rollenkonzeptes nach dem Erforderlichkeitsprinzip auf der Basis eines Identitätsmanagements durch die verantwortliche Stelle	<ul style="list-style-type: none"> <li>• Administrative Nutzer der Cloud Services werden nach least-privilege berechtigt</li> <li>• Vergabe erfolgt dokumentiert im Ticketsystem</li> <li>• Angeforderte Berechtigungen müssen genehmigt werden</li> <li>• Das grundlegende Vorgehen zur Nutzerverwaltung der Cloud Services ist in einem Betriebskonzept festgelegt</li> </ul>

Implementierung eines sicheren Authentifizierungsverfahrens	<ul style="list-style-type: none"> <li>• Richtlinien hinsichtlich der Komplexität von Passwörtern ist eingeführt und umgesetzt</li> <li>• MFA ist zwingende Voraussetzung für den Zugriff auf die Managementkonsole</li> <li>• Ausschließliche Verwendung von personalisierten Usern</li> <li>• Logging aller Anmeldevorgänge</li> <li>• Root Passwörter werden nicht für reguläre, operative Tätigkeiten verwendet</li> <li>• Nicht genutzte Accounts werden automatisch nach einer definierten Zeitspanne deaktiviert</li> </ul>
<p>Eingrenzung der zulässigen Personalkräfte auf solche, die nachprüfbar</p> <p>zuständig (örtlich, fachlich), fachlich befähigt, zuverlässig (ggf.</p> <p>sicherheitsüberprüft) und formal zugelassen sind sowie keine</p>	<ul style="list-style-type: none"> <li>• Zur Administration eingesetztes Personal verfügt über eine umfassende Ausbildung und wird regelmäßig geschult</li> <li>• Alle Mitarbeiter der BTC sind zur Geheimhaltung vertraglich verpflichtet</li> <li>• Neue Mitarbeiter werden nach einem festgelegten Prozess eingearbeitet</li> </ul>
Interessenskonflikte bei der Ausübung aufweisen	
Festlegung und Kontrolle der Nutzung zugelassener Ressourcen insbesondere Kommunikationskanäle	<ul style="list-style-type: none"> <li>• Separierung von Systemen in verschiedene Subnets</li> <li>• Mehrstufige Trennung des Netzwerkverkehrs (Security Groups, Network Access Control List, Transit Gateway)</li> </ul>
Spezifizierte, für die Verarbeitungstätigkeit ausgestattete Umgebungen	<ul style="list-style-type: none"> <li>• Die Anforderungen an die Umgebung in der Cloud, stimmen wir am Anfang des Projekts ab</li> <li>• Dabei werden die individuellen Anforderungen erfasst und bei Bedarf zusätzliche Sicherheitsmaßnahmen implementiert, welche über das grundlegende Schutzniveau hinaus gehen</li> </ul>
Festlegung und Kontrolle organisatorischer Abläufe, interner Regelungen und vertraglicher Verpflichtungen	<ul style="list-style-type: none"> <li>• Abschluss von AVV mit den Cloud Providern (Data Processing Addendum)</li> <li>• Festlegung von geographischen Regionen, in denen Daten verarbeitet werden</li> <li>• Bei Verstoß gegen vertragliche Verpflichtungen können disziplinarische Maßnahmen gegen den Mitarbeiter eingeleitet werden</li> </ul>
Verschlüsselung von gespeicherten oder transferierten Daten sowie Prozesse zur Verwaltung und zum Schutz der kryptografischen Informationen (Kryptokonzept)	<ul style="list-style-type: none"> <li>• Verschlüsselung von Daten at Rest (EBS, EFS u.ä.) sowie von Daten in Transit (TLS, IPSEC)</li> <li>• Richtlinie zum Einsatz von kryptologischen Verfahren sowie zum Schlüsselmanagement</li> </ul>

---

Schutz vor äußeren Einflüssen (Spionage, Hacking)

- Es ist ein integriertes Managementsystem (IMS) in der BTC eingeführt, dies umfasst den Schutz der eingesetzten Betriebsmittel als auch die Berücksichtigung der Anforderungen in den Leistungsangeboten
  - Ein Zugriff auf die Systeme bei Fernwartung erfolgt in der Regel mit cloud nativen Services um eine öffentliche Erreichbarkeit zu verhindern – situationsbedingte Ausnahmen werden mit dem Weisungsberechtigten abgestimmt
  - Bei der Nutzung von Diensten wie SSH oder RDS wird der IP-Adressbereich eingeschränkt, aus dem ein Zugriff erlaubt ist (IP-Whitelisting)
  - Schwachstellen bei den Systemen werden bei managed Services durch die Cloud Provider automatisch bereinigt. Auf Anforderung durch den Auftraggeber kann dies durch den Einsatz von Schwachstellenscannern bei nicht verwalteten Systemen ergänzt werden
  - Sicherheitspatches werden bei managed Services durch die Cloud Provider installiert. Systeme, die in der Verantwortung der BTC liegen, werden automatisch täglich, wöchentlich oder monatlich Sicherheitspatches installiert. Die Zeiträume werden im Rahmen der Betriebsübernahme mit dem Auftraggeber abgestimmt. Eine Dokumentation erfolgt durch die Loggingdienste der Cloudprovider. Bei Gefahr im Verzug handeln wir im Rahmen des abgestimmten Incidentsprozesses, ggf. auch ohne vorherige Zustimmung durch den Auftraggeber, soweit dies notwendig ist, um weiteren Schaden abzuwenden.
  - Bei Sicherheitsvorfällen werden die vorher festgelegten Ansprechpartner/innen auf Seiten des Auftraggebers informiert. Die Behandlung des Vorfalls erfolgt gem. des abgestimmten Incidentprozesses (Transitionsphase bei der Einführung eines neuen Cloudservice).
-

### 3.2 Verfügbarkeit

Maßnahme	Umsetzung
Anfertigung von Sicherheitskopien von Daten, Prozesszuständen, Konfigurationen, Datenstrukturen, Transaktionshistorien u.ä. gemäß eines getesteten Konzepts	<ul style="list-style-type: none"> <li>• Backups werden gemäß dargelegtem Schutzbedarf / Sicherheitsanforderung umgesetzt</li> <li>• Regelmäßige und automatisierte Erstellung von Snapshots der Datenquellen/Datenbanken</li> <li>• Zentrales und versioniertes Repository von verwendeten Skripten und Code</li> </ul>
Schutz vor äußeren Einflüssen (Schadsoftware, Sabotage, höhere Gewalt)	<ul style="list-style-type: none"> <li>• Äquivalent zu den Maßnahmen zum Schutz der Vertraulichkeit</li> </ul>
Redundanz von Hard- und Software sowie Infrastruktur	<ul style="list-style-type: none"> <li>• Nutzung der hochverfügbaren Infrastruktur der Public Cloud Provider</li> <li>• Umsetzung von angemessenen Konzepten, entsprechend dem Schutzbedarf</li> <li>• Multi AZ sowie Multi Regional bei Bedarf möglich</li> <li>• Festlegung von Georedundanzen</li> </ul>
Erstellung eines Notfallkonzepts zur Wiederherstellung einer Verarbeitungstätigkeit	<ul style="list-style-type: none"> <li>• BTC legt über eine übergreifende, strategische Richtlinie zum Krisen- und Notfallmanagement die Anforderungen und Zuständigkeiten / Verantwortlichen fest</li> <li>• In Notfällen wird die Cloud-Infrastruktur bei vorgesehenen Services automatisch wiederhergestellt (Self Healing), dieser Prozess wird regelmäßig getestet</li> <li>• Bei Kundensystemen wird im Rahmen von Einführungsprojekten oder bei Migrationsprojekten die Anforderung an das spezifische Notfallkonzept abgestimmt</li> <li>• Zusätzliche Backup/Recovery Konzepte können mit den kundenseitigen Fachabteilungen je nach Schutzbedürftigkeit nach Bedarf realisiert werden</li> </ul>
Vertretungsregelungen für abwesende Mitarbeitende	<ul style="list-style-type: none"> <li>• Die Arbeitszeit- und fachlichen Kapazitäten der Mitarbeiter werden vorausschauend geplant</li> <li>• Zuständigkeiten und Prozess zur Ressourcenanforderung sind etabliert</li> <li>• Für die fachspezifischen Rollen sind Vertreter benannt</li> </ul>

### 3.3 Integrität

Maßnahme	Umsetzung
Einschränkung von Schreib- und Änderungsrechten	<ul style="list-style-type: none"> <li>• Administrative Nutzer der Cloud Services werden nach least-privilege berechtigt</li> <li>• Trennung von Umgebungen mittels Organizations</li> <li>• Zu Kontrollzwecken werden Read-Only Rollen eingesetzt, um eine Veränderung von Daten zu verhindern</li> </ul>
Einsatz von Prüfsummen, elektronischen Siegeln und Signaturen in Datenverarbeitungsprozessen gem. eines Kryptokonzepts	<ul style="list-style-type: none"> <li>• Logs können bei besonders hohen Schutzbedarfen zusätzlich signiert werden</li> <li>• Zugriff per SSH erfolgt falls notwendig zertifikatsbasiert</li> <li>• Richtlinie zum Einsatz von kryptologischen Verfahren sowie zum Schlüsselmanagement sind umgesetzt und etabliert</li> </ul>
Dokumentierte Zuweisung von Berechtigungen und Rollen	<ul style="list-style-type: none"> <li>• Vergabe von Nutzerrechten ist im Ticketsystem sowie im Bestellsystem dokumentiert</li> <li>• Sämtliche Zugriffe werden protokolliert und sind namentlichen Nutzern zugeordnet</li> </ul>
Löschen oder Berichtigen falscher Daten	<ul style="list-style-type: none"> <li>• Die rein technische Lösungsverfahren von Daten bei den Cloud Providern erfolgt nach dem Stand der Technik</li> <li>• Für die Löschung in den führenden Informationssystemen ist der kundenseitig zuständige Fachbereich verantwortlich</li> </ul>
Härten von IT-Systemen, so dass diese keine oder möglichst wenige Nebenfunktionalitäten aufweisen	<ul style="list-style-type: none"> <li>• Standradhärtungsmaßnahmen werden angewendet <ul style="list-style-type: none"> <li>○ Zugriffe auf Systeme werden auf Ebene des Netzwerkinterfaces beschränkt</li> <li>○ Verwendung von angepassten Images, bspw. dedizierte Images für Container</li> </ul> </li> <li>• Regulär werden die Images der Cloud Provider verwendet</li> <li>• Eine spezielle Härtung kann bei besonders hohem Schutzbedarf durchgeführt werden</li> </ul>
Prozess zur Aufrechterhaltung der Aktualität von Daten	<ul style="list-style-type: none"> <li>• Änderungen an Daten in der Cloud Umgebung werden nur auf Anweisung des Auftraggebers durchgeführt</li> <li>• Verantwortung für Daten auf Ebene der Applikation, kann nur nach vorheriger vertraglicher Abstimmung übernommen werden</li> </ul>
Prozess zur Identifizierung und Authentifizierung von Personen und Gerätschaften	<ul style="list-style-type: none"> <li>• Alle API Aufrufe innerhalb der Cloud müssen authentifiziert werden</li> <li>• Sämtliche Accounts sind verantwortlichen Personen zugeordnet</li> </ul>

Festlegung des Sollverhaltens von Prozessen und regelmäßiges Durchführen von Tests zur Feststellung und Dokumentation der Funktionalität, von Risiken sowie Sicherheitslücken und Nebenwirkungen von Prozessen	<ul style="list-style-type: none"> <li>• Die Prozesse der Managed Cloud Services sind dokumentiert und werden regelmäßigen Reviews unterzogen</li> <li>• Interne Audits erfolgen jährlich im Rahmen des IMS</li> <li>• Externe Audits gemäß ISO27001 sowie ISO9001 erfolgen jährlich</li> </ul>
Festlegen des Sollverhaltens von Abläufen bzw. Prozessen und regelmäßiges Durchführen von Tests zur Feststellbarkeit bzw. Feststellung der Ist-Zustände von Prozessen	<ul style="list-style-type: none"> <li>• Prozesse werden im Rahmen des IMS dokumentiert</li> <li>• Prozessreviews werden unterjährig durchgeführt</li> <li>• Kundenspezifische Anforderungen an Prozesse werden in der Transitionsphase beidseitig abgestimmt</li> </ul>
Schutz vor äußeren Einflüssen (Spionage, Hacking)	<ul style="list-style-type: none"> <li>• Äquivalente Maßnahmen wie zum Schutz der Vertraulichkeit (siehe oben).</li> </ul>

### 3.4 Nichtverkettung

Maßnahme	Umsetzung
Einschränkung von Verarbeitungs-, Nutzungs- und Übermittlungsrechten	<ul style="list-style-type: none"> <li>• Datenübermittlungen strikt nach Kundenvorgabe und Architekturkonzept</li> <li>• Separierung von Umgebungen erfolgt mehrstufig                             <ul style="list-style-type: none"> <li>○ Trennung in verschiedene Accounts</li> <li>○ Separierung in Subnetzen</li> </ul> </li> <li>• Vergabe von Nutzerrechten nach Least-Privilege</li> </ul>
programmtechnische Unterlassung bzw. Schließung von Schnittstellen bei Verarbeitungsverfahren und Komponenten	<ul style="list-style-type: none"> <li>• Nutzung von Schnittstellen strikt nach abgestimmten Architekturkonzept</li> <li>• Ggf. Deaktivierung von Schnittstellen in Absprache mit dem Kunden-Fachbereich</li> </ul>
regelnde Maßgaben zur Sicherheit der Software/Softwareentwicklung sowie qualitätssichernde Maßnahmen	<ul style="list-style-type: none"> <li>• Sorgfältige Auswahl der eingesetzten Cloudprovider und Cloudservices sowie Berücksichtigung von Qualitätsstandards und Zertifizierungen</li> <li>• Interne Software- und Systementwicklung erfolgt nach festgelegtem Prozess, welche entsprechende Qualitätssicherungsmaßnahmen beinhaltet</li> </ul>
Trennung nach Organisations-/Abteilungsgrenzen	<ul style="list-style-type: none"> <li>• Innerhalb der Business Unit findet eine Trennung nach Aufgabenbereichen statt</li> <li>• Die Zugriffsmöglichkeiten werden entsprechend den Anforderungen vergeben</li> <li>• Änderungen der Aufgabenbereiche erfolgen nur nach Freigabe durch die Leitung der Unit</li> </ul>

Trennung mittels Rollenkonzepten mit abgestuften Zugriffsrechten auf der Basis eines Identitätsmanagements durch die verantwortliche Stelle und eines sicheren Authentifizierungsverfahrens	<ul style="list-style-type: none"> <li>• Vergabe von Berechtigungen erfolgt nach dem Prinzip Least Privilege</li> <li>• Vergabe erfolgt dokumentiert im Ticketsystem</li> <li>• Angeforderte Berechtigungen müssen genehmigt werden</li> </ul>
Zulassung von integriertem Identitätsmanagement durch den Auftraggeber	<ul style="list-style-type: none"> <li>• Einbindung von Trusted Identity Providern gem. Vorgabe des Auftraggebers ist möglich</li> </ul>
Einsatz von zweckspezifischen Pseudonymen, Anonymisierungsdiensten, anonymen Credentials, Verarbeitung pseudonymer bzw. anonymisierter Daten	<ul style="list-style-type: none"> <li>• Bei der Vergabe von Nutzerzugängen wird ein pseudonymisierter Nutzernamen verwendet, um Dritten ein Ableiten des Namens zu erschweren</li> </ul>
gezielte Zweckänderungsverfahren	<ul style="list-style-type: none"> <li>• Ausschließlich auf Weisung des Kunden erfolgt eine Zweckänderung</li> </ul>

### 3.5 Transparenz

Maßnahme	Umsetzung
Dokumentation im Sinne einer Inventarisierung aller Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO	<ul style="list-style-type: none"> <li>• Dokumentation der Tätigkeiten, welche für die Auftraggeber erbracht werden, sind gesteuert im Rahmen des Accountmanagements</li> <li>• Bei der Erfüllung der Pflichten werden die Auftraggeber vertragsgemäß unterstützt</li> </ul>
Dokumentation der Bestandteile von Verarbeitungstätigkeiten insbesondere der Geschäftsprozesse, Datenbestände, Datenflüsse und Netzpläne, dafür genutzte IT-Systeme, Betriebsabläufe, Beschreibungen von Verarbeitungstätigkeiten, Zusammenspiel mit anderen Verarbeitungstätigkeiten	<ul style="list-style-type: none"> <li>• Bestandteile, welche in der Verantwortung der Unit Cloud Services liegen, werden dokumentiert</li> <li>• Dies umfasst bspw. Abläufe, Architektur und Accountstruktur</li> </ul>
Dokumentation von Tests, der Freigabe und ggf. der Datenschutz-Folgenabschätzung von neuen oder geänderten Verarbeitungstätigkeiten	<ul style="list-style-type: none"> <li>• Test, Änderungen sowie Freigaben erfolgen nach einem festgelegten Ablauf (Changemanagement)</li> <li>• Der Auftraggeber wird bei der Erstellung einer DSFA mit technischen Informationen auf Anfrage unterstützt</li> </ul>
Dokumentation von Tests, der Freigabe und ggf. der Datenschutz-Folgenabschätzung von neuen oder geänderten Verarbeitungstätigkeiten	<ul style="list-style-type: none"> <li>• Test, Änderungen sowie Freigaben erfolgen nach einem festgelegten Ablauf (Changemanagement)</li> <li>• Der Auftraggeber wird bei der Erstellung einer DSFA mit technischen Informationen auf Anfrage unterstützt</li> </ul>

<p>Dokumentation der Verträge mit den internen Mitarbeitenden, Verträge mit externen Dienstleistern und Dritten, von denen Daten erhoben bzw. an die Daten übermittelt werden, Geschäftsverteilungspläne, Zuständigkeitsregelungen</p>	<ul style="list-style-type: none"> <li>• Es sind BTC weite Prozesse bei der Beauftragung von Fremddienstleistern implementiert</li> <li>• Interne Vertragsverhältnisse werden zentral durch HR betreut</li> </ul>
<p>Dokumentation von Einwilligungen, deren Widerruf sowie Widersprüche</p>	<ul style="list-style-type: none"> <li>• Die Dokumentation der Einwilligungen der BTC erfolgt gesteuert im Rahmen des CRM zum Zwecke von Marketing und Vertriebsaktivitäten (Interessenten, BTC Newsletter)</li> </ul>
<p>Protokollierung von Zugriffen und Änderungen</p>	<ul style="list-style-type: none"> <li>• Alle Zugriffe auf die Cloudumgebung werden mittels cloud nativen Diensten aufgezeichnet</li> <li>• Automatisierte Auswertung von Logs auf Anomalien sowie nach definierten Regeln</li> <li>• Logfiles werden zusätzlich in einen separaten Account kopiert, um eine Manipulation zu unterbinden</li> <li>• Im Rahmen des Changeprozesses werden Abnahmekriterien der Systeme festgelegt, dies beinhaltet auch die Funktionalität der Protokollierung</li> <li>• Ein Ausfall der cloud nativen Services wird über entsprechende Kanäle der Cloud Provider kommuniziert</li> </ul>
<p>Versionierung</p>	<ul style="list-style-type: none"> <li>• Die für die Cloud Umgebungen genutzten Skripte, werden zentral in einem Repository verwaltet und versioniert</li> </ul>
<p>Dokumentation der Verarbeitungsprozesse mittels Protokollen auf der Basis eines Protokollierungs- und Auswertungskonzepts</p>	<ul style="list-style-type: none"> <li>• Alle Aufrufe innerhalb der Cloudumgebung werden protokolliert, bspw. mittels CloudTrail</li> <li>• Die korrekte Funktion von Systemen wird mittels Monitoring Lösungen überwacht und sichergestellt</li> <li>• Zusätzliche Regeln zur Einhaltung von Complianceanforderungen kann durch Cloud Services in Absprache mit dem Kunden eingerichtet werden</li> </ul>
<p>Dokumentation der Quellen von Daten, bspw. des Umsetzens der Informationspflichten gegenüber Betroffenen, wo deren Daten erhoben wurden sowie des Umgangs mit Datenpannen</p>	<ul style="list-style-type: none"> <li>• Cloudservices die Daten von Betroffenen verarbeiten, sind im Inventar in kundenseitiger Abstimmung spezifisch zu kennzeichnen (im Betrieb liegt in der Regel das Detailwissen über die Hintergründe der Verarbeitung nicht vor) bzw. im kundenseitigen Verzeichnisse vorzuhalten</li> <li>• Im Falle eines Vorfalls bei welchem der Verdacht besteht, dass personenbezogene Daten betroffen sein könnten, wird der jeweils festgelegte Ansprechpartner unmittelbar informiert</li> <li>• Ebenfalls wird der festgelegte Ansprechpartner bei der weiteren Kommunikation mit Betroffenen oder Aufsichtsbehörden unterstützt</li> </ul>

	<ul style="list-style-type: none"> <li>• Der festgelegte Ansprechpartner wird bei der Erstellung der notwendigen Informationen an Betroffene unterstützt</li> </ul>
Benachrichtigung von Betroffenen bei Datenpannen oder bei Weiterverarbeitungen zu einem anderen Zweck	<ul style="list-style-type: none"> <li>• Im Falle eines Vorfalls bei welchem der Verdacht besteht, dass personenbezogene Daten betroffen sein könnten, wird der festgelegte Ansprechpartner unmittelbar informiert</li> <li>• Ebenfalls wird der festgelegte Ansprechpartner bei der weiteren Kommunikation mit Betroffenen oder Aufsichtsbehörden unterstützt</li> </ul>
Nachverfolgbarkeit der Aktivitäten der verantwortlichen Stelle zur Gewährung der Betroffenenrechte	<ul style="list-style-type: none"> <li>• Dokumentation bei Datenschutzvorfällen erfolgt und wird dem festgelegten Ansprechpartner zur Verfügung gestellt</li> </ul>
Berücksichtigung der Auskunftsrechte von Betroffenen im Protokollierungs- und Auswertungskonzept	<ul style="list-style-type: none"> <li>• Dokumentation bei Datenschutzvorfällen erfolgt und wird dem festgelegten Ansprechpartner zur Verfügung gestellt</li> </ul>
Bereitstellung von Informationen über die Verarbeitung von personenbezogenen Daten an Betroffene	<ul style="list-style-type: none"> <li>• BTC unterstützt unsere Kunden durch die zur Verfügungstellung von Informationen über die in unserer Verantwortung liegenden Bestandteile der Umgebung</li> </ul>

### 3.6 Intervenierbarkeit

Maßnahme	Umsetzung
Maßnahmen für differenzierte Einwilligungs-, Rücknahme- sowie Widerspruchsmöglichkeiten	<ul style="list-style-type: none"> <li>• Bereitstellung eines Single Point of Contact für weisungsberechtigte Mitarbeiter</li> <li>• Bei Anfragen durch Betroffene werden diese an die verantwortliche Stelle wie kundenseitig festgelegt verwiesen</li> </ul>
Schaffung notwendiger Datenfelder z. B. für Sperrkennzeichen, Benachrichtigungen, Einwilligungen, Widersprüche, Gegendarstellungen	<ul style="list-style-type: none"> <li>• Unterstützung des Kunden bei der Gestaltung der Applikation</li> <li>• Datenfelder können nach Bedarf entsprechend angepasst werden</li> </ul>
dokumentierte Bearbeitung von Störungen, Problembearbeitungen und Änderungen an Verarbeitungstätigkeiten sowie an den technischen und organisatorischen Maßnahmen	<ul style="list-style-type: none"> <li>• Dokumentation der Tätigkeiten erfolgt im kundenseitig zugänglichen Ticketsystem</li> </ul>
Deaktivierungsmöglichkeit einzelner Funktionalitäten ohne Mitleidenschaft für das Gesamtsystem	<ul style="list-style-type: none"> <li>• Unterstützung bei der Gestaltung von verteilten Architekturen</li> </ul>

Identifizierung und Authentifizierung der Personen, die Betroffenenrechte wahrnehmen möchten	<ul style="list-style-type: none"> <li>• Bereitstellung eines Single Point of Contact für weisungsberechtigte Mitarbeiter</li> <li>• Bei Anfragen durch Betroffene werden diese an die verantwortliche Stelle wie kundenseitig festgelegt verwiesen</li> </ul>
Einrichtung eines Single Point of Contact (SPoC) für Betroffene	<ul style="list-style-type: none"> <li>• Bereitstellung eines Single Point of Contact für weisungsberechtigte Mitarbeiter</li> <li>1. Bei Anfragen durch Betroffene werden diese an die verantwortliche Stelle wie kundenseitig festgelegt verwiesen</li> </ul>

### 3.7 Datenminimierung

Maßnahme	Umsetzung
Reduzierung von erfassten Attributen der betroffenen Personen	<ul style="list-style-type: none"> <li>• Verantwortung des kundenseitigen Fachbereiches</li> <li>• Technische Unterstützung erfolgt auf Anfrage</li> </ul>
Reduzierung der Verarbeitungsoptionen in Verarbeitungsschritten	<ul style="list-style-type: none"> <li>• Verantwortung des kundenseitigen Fachbereiches</li> </ul>
Reduzierung von Möglichkeiten der Kenntnisnahme vorhandener Daten	<ul style="list-style-type: none"> <li>• Technische Unterstützung erfolgt auf Anfrage</li> </ul>
Festlegung von Voreinstellungen für betroffene Personen, die die Verarbeitung ihrer Daten auf das für den Verarbeitungszweck erforderliche Maß beschränken.	<ul style="list-style-type: none"> <li>• Verantwortung des kundenseitigen Fachbereiches</li> </ul>
Bevorzugung von automatisierten Entscheidungsprozessen), die eine Kenntnisnahme verarbeiteter Daten entbehrlich machen und die Einflussnahme begrenzen, gegenüber im Dialog gesteuerten Prozessen	<ul style="list-style-type: none"> <li>• Datentransformation erfolgt mittels spezifischen automatisierter Funktionen</li> <li>• Die Verwendung automatischer Entscheidungsprozesse ist der verfolgte Grundprinzip bei der Gestaltung der Cloud-Betriebsprozesse</li> </ul>
Implementierung von Datenmasken, die Datenfelder unterdrücken, sowie automatischer Sperr- und Löschroutinen, Pseudonymisierungs- und Anonymisierungsverfahren	<ul style="list-style-type: none"> <li>• Verantwortung des kundenseitigen Fachbereiches</li> <li>• Technische Unterstützung erfolgt auf Anfrage</li> </ul>

---

Festlegung und Umsetzung eines Löschkonzepts

- Wenn die Löschung von Daten seitens einer weisungsbefugten Person beantragt wird, dann führen wir eine Erhebung der zu löschenden Daten durch und weisen im Rahmen eines Individualgespräches nach, dass alle zu löschenden Daten gelöscht sind. Nach Beendigung des Gespräches wird ein Dokument erstellt, welches als Nachweis gilt.

---

Regelungen zur Kontrolle von Prozessen zur Änderung von

- Regelmäßige Selbstbewertungen von Maßnahmen
- Interne und externe Audits

Verarbeitungstätigkeiten

---

## 4 Dokumentenlenkung

### 4.1 Abkürzungen

Abkürzung	Begriff
SDM	Standard-Datenschutzmodell
DSK	Datenschutzkonferenz
AK	Arbeitskreis

### 4.2 Quellen

Thema	Link
Standard-Datenschutzmodell	<a href="https://www.datenschutzzentrum.de">Das Standard-Datenschutzmodell (SDM) - ULD (datenschutzzentrum.de)</a>
AWS Compliance	<a href="#">Cloud Compliance - Amazon Web Services (AWS)</a>
AWS Artifacts	<a href="#">AWS Artifact - Amazon Web Services (AWS)</a>
Azure Compliance	<a href="#">Dokumentation zur Azure-Compliance   Microsoft Docs</a>
DSGVO	<a href="#">EUR-Lex - 32016R0679 - DE - EUR-Lex (europa.eu)</a>

Version	Abschnitt	Gegenstand der Änderung	Autor	Datum
1.0	alle	Initiale Erstellung Cloud Security Specialist und Servicemanager	Marc Schröder Rene Schönemann	14.05.21
1.1	alle	Korrektur und Ergänzung	Maik Evers (DSB)	09.09.21