

Vertragsnummer/Kennung Auftraggeber: \_\_\_\_\_

Vertragsnummer/Kennung Auftragnehmer: V17823/3011135

Seite 1 von 6

## Vertrag über die Beschaffung von IT-Dienstleistungen

Zwischen

**GeoInformation Bremen**  
Lloydstr. 4  
28217 Bremen

– im Folgenden „Auftraggeber“ genannt –

und

**Dataport**  
Anstalt des öffentlichen Rechts  
Altenholzer Straße 10 - 14  
24161 Altenholz

– im Folgenden „Auftragnehmer“ genannt –

wird folgender Vertrag geschlossen:

### 1 Vertragsgegenstand und Vergütung

#### 1.1 Projekt-/Vertragsbezeichnung

DIPAS Bremen: Verfahrensinfrastruktur im Rechenzentrum sowie Technisches Verfahrensmanagement und grundschutzkonformer Betrieb

1.2 Für alle in diesem Vertrag genannten Beträge gilt einheitlich der Euro als Währung.

1.3 Die Leistungen des Auftragnehmers werden

nach Aufwand gemäß Nummer 5.1

zum Festpreis gemäß Nummer 5.2

zuzüglich Reise- und Nebenkosten – soweit in Nummer 5.3 vereinbart – vergütet.

Die zum Zeitpunkt der Leistungserbringung gültige Umsatzsteuer wird gesondert vergütet.

### 2 Vertragsbestandteile

2.1 Es gelten nacheinander als Vertragsbestandteile:

- dieses Vertragsformular (Seiten 1 bis 6)
- Allgemeine Vertragsbedingungen von Dataport (Dataport AVB) in der jeweils geltenden Fassung (s. 11.1)
- Vertragsanlage(n) Nr. 1, 2a, 2b, 3, 4a, 4b und 5 (die Reihenfolge der Anlagen ergibt sich aus Nr. 3.2.1)
- Ergänzende Vertragsbedingungen für die Erbringung von IT-Dienstleistungen (EVB-IT Dienstleistung, Fassung vom 01. April 2002)
- Vergabe- und Vertragsordnung für Leistungen – ausgenommen Bauleistungen – Teil B (VOL/B) in der bei Vertragsschluss geltenden Fassung

2.2 Weitere Geschäftsbedingungen sind ausgeschlossen, soweit in diesem Vertrag nichts anderes vereinbart ist.

Vertragsnummer/Kennung Auftraggeber: \_\_\_\_\_

Vertragsnummer/Kennung Auftragnehmer: V17823/3011135

### 3 Art und Umfang der Dienstleistungen

#### 3.1 Art der Dienstleistungen

Der Auftragnehmer erbringt für den Auftraggeber folgende Dienstleistungen:

- 3.1.1  Beratung
- 3.1.2  Projektleitungsunterstützung
- 3.1.3  Schulung
- 3.1.4  Einführungsunterstützung
- 3.1.5  Betreiberleistungen
- 3.1.6  Benutzerunterstützungsleistungen
- 3.1.7  Providerleistungen ohne Inhaltsverantwortlichkeit
- 3.1.8  sonstige Dienstleistungen:  
gemäß den Anlagen 4a, 4b, 5

#### 3.2 Umfang der Dienstleistungen des Auftragnehmers

3.2.1 Der Umfang der vom Auftragnehmer zu erbringenden Dienstleistungen ergibt sich aus

folgenden Teilen des Angebotes des Auftragnehmers vom

der Leistungsbeschreibung des Auftragnehmers

Service Level Agreement Verfahrensinfrastruktur im Dataport Rechenzentrum Teil A – Allgemeiner Teil - (SLA VI A)	Anlage(n) Nr.	4a
Service Level Agreement Verfahrensinfrastruktur im Dataport Rechenzentrum Teil B (spezifischer Teil für Verfahren DIPAS Bremen (DIPAS_HB001)) (SLA VI B)	Anlage(n) Nr.	4b
Security Service Level Agreement für Betrieb DIPAS Bremen (SSLA)	Anlage(n) Nr.	5

folgenden weiteren Dokumenten:

Ansprechpartner	Anlage(n) Nr.	1
Preisblatt Aufwände	Anlage(n) Nr.	2a
Preisblatt Festpreis	Anlage(n) Nr.	2b
Selbstauskunft Auftraggeber über Auftragsverarbeitung	Anlage(n) Nr.	3

Es gelten die Dokumente in

- obiger Reihenfolge
- folgender Reihenfolge: 1, 2a, 2b, 3, 4b, 4a, 5

3.2.2  Der Auftragnehmer wird den Auftraggeber auf relevante Veränderungen des Standes der Technik hinweisen, wenn diese für den Auftragnehmer erkennbar maßgeblichen Einfluss auf die Art der Erbringung der vertraglichen Leistungen haben.

3.2.3 Besondere Leistungsanforderungen (z. B. Service-Level-Agreements über Reaktionszeiten):

Vertragsnummer/Kennung Auftraggeber: \_\_\_\_\_

Vertragsnummer/Kennung Auftragnehmer: V17823/3011135

**3.3 Vergütungsbestimmende Faktoren aus dem Bereich des Auftraggebers**

Vergütungsbestimmende Faktoren aus dem Bereich des Auftraggebers sind

- a) die Mitwirkungs- und Beistelleistungen des Auftraggebers gemäß Nummer 8
- b) folgende weitere Faktoren:

**4 Ort der Dienstleistungen / Leistungszeitraum**

**4.1 Ort der Dienstleistungen** In den Räumlichkeiten des Auftragnehmers

**4.2 Zeiträume der Dienstleistungen**

Leistungen (gemäß Nummer 3.1)	Geplanter Leistungszeitraum		Verbindlicher Leistungszeitraum	
	Beginn	Ende	Beginn	Ende
Gemäß Nr. 3.1.8			06.11.2021	

**4.3 Zeiten der Dienstleistungen**

Die Leistungen des Auftragnehmers werden erbracht gemäß SLA VI A Pkt. 2.2.2 und SLA VI B Pkt. 2.1.1.

**4.3.1** während der üblichen Geschäftszeiten des Auftragnehmers an Werktagen (außer an Samstagen und Feiertagen)

\_\_\_\_\_ bis \_\_\_\_\_ von \_\_\_\_\_ bis \_\_\_\_\_ Uhr

**4.3.2** während sonstiger Zeiten

\_\_\_\_\_ bis \_\_\_\_\_ von \_\_\_\_\_ bis \_\_\_\_\_ Uhr  
 an Sonn- und Feiertagen am Sitz des Auftragnehmers von \_\_\_\_\_ bis \_\_\_\_\_ Uhr

**5 Vergütung gem. Preisblatt Anlagen 2a, 2b und Leistungsnachweis Dienstleistung**

**5.1**  Vergütung nach Aufwand

mit einer Obergrenzenregelung gemäß Anlage 2a

Bezeichnung des Personals/der Leistung (Leistungskategorie)					Preis innerhalb der Zeiten gemäß Nr. 4.3.
Pos. Nr.	SAP-Artikel-Nr.	Artikelbezeichnung/-code	Menge	Mengen-einheit	Einzelpreis

Die Artikel und Preise sind in der Anlage 2a enthalten.

**Reisezeiten**

- Reisezeiten werden nicht gesondert vergütet.
- Reisezeiten werden vergütet gemäß Anlage:

**Rechnungsstellung**

Die Rechnungsstellung erfolgt gemäß Anlage 2a.

**Vergütungsvorbehalt**

- Es wird ein Vergütungsvorbehalt vereinbart
- gemäß Ziffer 6.4 EVB-IT Dienstleistung
  - gemäß Ziffer 3.1 der Dataport AVB
  - anderweitige Regelung gemäß Anlage:

Vertragsnummer/Kennung Auftraggeber: \_\_\_\_\_

Vertragsnummer/Kennung Auftragnehmer: V17823/3011135

Seite 4 von 6

5.2  **Festpreis**

Der einmalige und der jährliche Festpreis setzen sich gemäß Anlage 2b zusammen.

Die Rechnungsstellung des einmaligen und des jährlichen Festpreises erfolgt gemäß Anlage 2b.

Preisänderungen dieser Leistung behält sich der Auftragnehmer gemäß Ziffer 3.1 der Dataport AVB vor.

Es werden folgende Abschlagszahlungen vereinbart:

5.3 **Reisekosten und Nebenkosten**

Reisekosten werden nicht gesondert vergütet

Reisekosten werden vergütet gemäß Anlage:

Nebenkosten werden nicht gesondert vergütet

Nebenkosten werden vergütet gemäß Anlage:

6 **Rechte an den verkörperten Dienstleistungsergebnissen**

(ergänzend zu / abweichend von Ziffer 4 EVB-IT Dienstleistung)

6.1  Ergänzend zu Ziffer 4 EVB-IT Dienstleistung ist der Auftraggeber berechtigt, folgenden Dienststellen und Einrichtungen, die seinem Bereich zuzuordnen sind, einfache, nicht übertragbare Nutzungsrechte\* an den Dienstleistungsergebnissen einzuräumen:

\_\_\_\_\_

6.2  Ergänzend zu Ziffer 4 EVB-IT Dienstleistung ist der Auftraggeber berechtigt, folgenden Dienststellen und Einrichtungen außerhalb seines Bereiches einfache, nicht übertragbare Nutzungsrechte\* an den Dienstleistungsergebnissen einzuräumen:

\_\_\_\_\_

6.3  Abweichend von Ziffer 4 EVB-IT Dienstleistung räumt der Auftragnehmer dem Auftraggeber das ausschließliche, dauerhafte, unbeschränkte, unwiderrufliche und übertragbare Nutzungsrecht an den Dienstleistungsergebnissen, Zwischenergebnissen und vereinbarungsgemäß bei der Vertragserfüllung erstellten Schulungsunterlagen ein. Dies gilt auch für die Hilfsmittel, die der Auftragnehmer bei der Erbringung der Dienstleistung entwickelt hat. Der Auftragnehmer bleibt zur beliebigen Verwendung der Hilfsmittel und Werkzeuge, die er bei der Erbringung der Dienstleistung verwendet hat, berechtigt.

6.4  Sonstige Nutzungsrechtsvereinbarungen

\_\_\_\_\_

7 **Verantwortlicher Ansprechpartner siehe Anlage 1**

des Auftraggebers: \_\_\_\_\_

des Auftragnehmers: \_\_\_\_\_

8 **Mitwirkungs- und Beistelleistungen des Auftraggebers**

Folgende Mitwirkungsleistungen (z. B. Infrastruktur, Organisation, Personal, Technik, Dokumente) werden vereinbart:

8.1. Der Auftraggeber benennt gem. Anlage 1 Ansprechpartner mindestens zwei Mitarbeiterinnen/Mitarbeiter, die dem Auftragnehmer als Ansprechpartnerinnen/Ansprechpartner zur Verfügung stehen.

8.2. Änderungen der Anlage 1 Ansprechpartner sind unverzüglich schriftlich mitzuteilen. Hierfür wird eine neue Anlage 1 vom Auftraggeber ausgefüllt. Die Anlage wird auf Anforderung durch den Kundenbetreuer zur Verfügung gestellt. Die neue Anlage ist an \_\_\_\_\_ zu senden.

8.3. Gemäß Anlage SLA VI A Pkt. 1.2, SLA VI B Pkt. 1.4 und SSLA Pkt. 5.2.

8.4. Folgende weitere Beistelleistungen werden vereinbart

Vertragsnummer/Kennung Auftraggeber: \_\_\_\_\_

Vertragsnummer/Kennung Auftragnehmer: V17823/3011135

Seite 5 von 6

Softwarelizenzen

Bei der durch Dataport im Auftrag betriebenen Software handelt es sich um eine aktuell unter der Lizenz GPLv2 veröffentlichte OpenSource-Software. Der Auftraggeber verpflichtet sich Dataport immer die aktuellste DIPAS-Version zur Verfügung zu stellen. Der Auftraggeber informiert Dataport, sobald es eine neuere Version im DIPAS Repository gibt, die installiert werden soll.

## 9 Schlichtungsverfahren

Die Anrufung folgender Schlichtungsstelle wird vereinbart:

## 10 Versicherung

Der Auftragnehmer weist nach, dass die Haftungshöchstsummen gemäß Ziffer 9.2.1 EVB-IT Dienstleistung durch eine Versicherung abgedeckt sind, die im Rahmen und Umfang einer marktüblichen deutschen Industriehaftpflichtversicherung oder vergleichbaren Versicherung aus einem Mitgliedsstaat der EU entspricht.

## 11. Sonstige Vereinbarungen

### 11.1 Allgemeines

Die Dataport AVB stehen unter [www.dataport.de](http://www.dataport.de), die EVB-IT Dienstleistungs-AGB unter [www.cio.bund.de](http://www.cio.bund.de) und die VOL/B unter [www.bmwi.de](http://www.bmwi.de) zur Einsichtnahme bereit.

### 11.2 Umsatzsteuer

Die aus diesem Vertrag seitens des Auftragnehmers zu erbringenden Leistungen unterliegen in Ansehung ihrer Art, des Zwecks und der Person des Auftraggebers zum Zeitpunkt des Vertragsschlusses nicht der Umsatzsteuer. Sollte sich durch Änderungen tatsächlicher oder rechtlicher Art oder durch Festsetzung durch eine Steuerbehörde eine Umsatzsteuerpflicht ergeben und der Auftragnehmer insoweit durch eine Steuerbehörde in Anspruch genommen werden, hat der Auftraggeber dem Auftragnehmer die gezahlte Umsatzsteuer in voller Höhe zu erstatten, ggf. auch rückwirkend.

### 11.3 Verschwiegenheitspflicht

Die Vertragspartner vereinbaren über die Vertragsinhalte Verschwiegenheit, soweit gesetzliche Bestimmungen dem nicht entgegenstehen.

### 11.4 Bremer Informationsfreiheitsgesetz

11.4.1 Dieser Vertrag unterliegt dem Bremischen Informationsfreiheitsgesetz (BreMIFG). Er wird gemäß § 11 im zentralen elektronischen Informationsregister der Freien Hansestadt Bremen veröffentlicht. Unabhängig von einer Veröffentlichung kann er Gegenstand von Auskunftsanträgen nach dem BreMIFG sein.

11.4.2  Optionale Erklärung der Nichtveröffentlichung

Der Auftraggeber erklärt mit Auswahl dieser Option, dass der Auftraggeber diesen Vertrag nicht im Informationsregister veröffentlichen wird. Sollte während der Vertragslaufzeit eine Absicht zur Veröffentlichung entstehen, wird der Auftraggeber den Auftragnehmer unverzüglich informieren.

### 11.5 Ablösungen von Vereinbarungen/ Vorvereinbarungen

Mit diesem Vertrag wird eine etwaige Vorvereinbarung abgelöst. Rechte und Pflichten der Vertragsparteien bestimmen sich ab dem Zeitpunkt seines Wirksamwerdens ausschließlich nach diesem Vertrag.

# EVB-IT Dienstvertrag



Vertragsnummer/Kennung Auftraggeber: \_\_\_\_\_

Vertragsnummer/Kennung Auftragnehmer: V17823/3011135

Seite 6 von 6

## 11.6 Laufzeit und Kündigung

Dieser Vertrag beginnt am 06.11.2021 und gilt für unbestimmte Zeit. Er kann erstmals unter Wahrung einer Frist von 6 Monaten zum 30.11.2022 gekündigt werden. Danach kann er zum Ende eines Kalenderjahres unter Wahrung einer Frist von 6 Monaten gekündigt werden. Die Kündigung bedarf der Textform.

Bremen , 09.11.2021  
Ort Datum

Bremen , 16.11.21  
Ort Datum



**Ansprechpartner**  
zum Vertrag über die Beschaffung von IT-Dienstleistungen

Vertragsnummer/Kennung Auftraggeber:

Auftraggeber: Geoinformation Bremen  
Lloydstr. 4  
28217 Bremen

Rechnungsempfänger: Freie Hansestadt Bremen  
- Rechnungseingang FHB -  
Geoinformation Bremen  
28026 Bremen

Leitweg-ID:



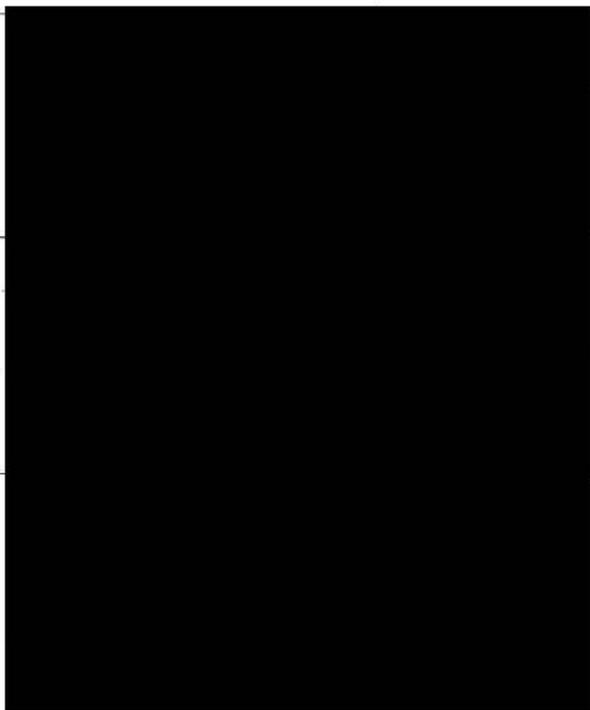
Der Rechnungsempfänger ist immer auch der Mahnungsempfänger.

Zentraler Ansprechpartner des  
Auftragnehmers:

Vertraglicher Ansprechpartner des  
Auftraggebers:

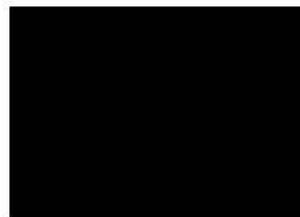
Fachliche Ansprechpartner des  
Auftraggebers:

Technische Ansprechpartner des  
Auftraggebers:



Ändern sich die Ansprechpartner in dieser Anlage, wird die Anlage gem. EVB-IT Vertrag ohne die Einleitung eines Änderungsvertrages ausgetauscht.

Ort Bremen , Datum 16.11.21



# Preisblatt Aufwände

**Gültig ab dem 03.11.2021**

Für die vom Auftragnehmer zu erbringenden Dienstleistungen  
zahlt der Auftraggeber folgende Entgelte:

Mit einer jährlichen Obergrenze von 2.000 €.

Die Abrechnung erfolgt nach Aufwand.

Die Rechnungsstellung der Pos. 10 erfolgt zum tagesaktuellen Preis nach und Bereitstellung.

Aufwandsleistungen, die über den in Anlage 2b gem. Pos. 80-90 vereinbarten Umfang hinausgehen Die Rechnungsstellung erfolgt gem. Anlage 2b.

# Preisblatt Einmaliger Festpreis

Gültig ab dem 03.11.2021

Für die vom Auftragnehmer zu erbringenden Dienstleistungen  
zahlt der Auftraggeber folgende **einmaligen Entgelte (nachrichtlich)**:

**Gesamtpreis : 338,20 €**

Die Rechnungsstellung des einmaligen Festpreises erfolgt nach Vertragsunterschrift.

Zu Pos. 40

Das Zertifikat wurde für den EHDB benötigt und wird jetzt über den Betriebsvertrag abgerechnet.

Laufzeit: 02.09.2021 bis 02.09.2022

# Preisblatt Jährlicher Festpreis

**Gültig ab dem 03.11.2021**

Für die vom Auftragnehmer zu erbringenden Dienstleistungen  
zahlt der Auftraggeber folgende **jährliche Entgelte (nachrichtlich)**:

**Gesamtpreis:** 67.849,04 €

Die Rechnungsstellung des Festpreises erfolgt zum 15.06. eines Kalenderjahres.

## Selbstauskunft Auftraggeber über Auftragsverarbeitung

### Angaben zum Vertrag über Auftragsverarbeitung

<b>Für die Verarbeitung der in Rede stehenden personenbezogenen Daten gelten folgende Datenschutzregelungen:</b>	Zutreffendes ankreuzen
Verordnung (EU) 2016/679 (DSGVO) und gfls. ergänzende landesrechtliche Regelungen	<input type="checkbox"/>
Nationale Regelungen (Landesdatenschutzgesetz bzw. Bundesdatenschutzgesetz) zur Umsetzung der RiLi (EU) 2016/680 <small>(Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit)</small>	<input type="checkbox"/>
Es findet keine Verarbeitung personenbezogener Daten statt	<input checked="" type="checkbox"/>

### Angaben zum Gegenstand der Auftragsverarbeitung <sup>1</sup>

Eine Erläuterung zu den nachfolgend zu machenden Angaben findet sich z. B. hier:

[https://www.lida.bayern.de/media/dsk\\_hinweise\\_vov.pdf](https://www.lida.bayern.de/media/dsk_hinweise_vov.pdf)

<b>1.</b>	<b>Art und Zweck der Verarbeitung</b> <small>(siehe z. B. Art. 28 Abs. 3 S. 1 DSGVO)</small>

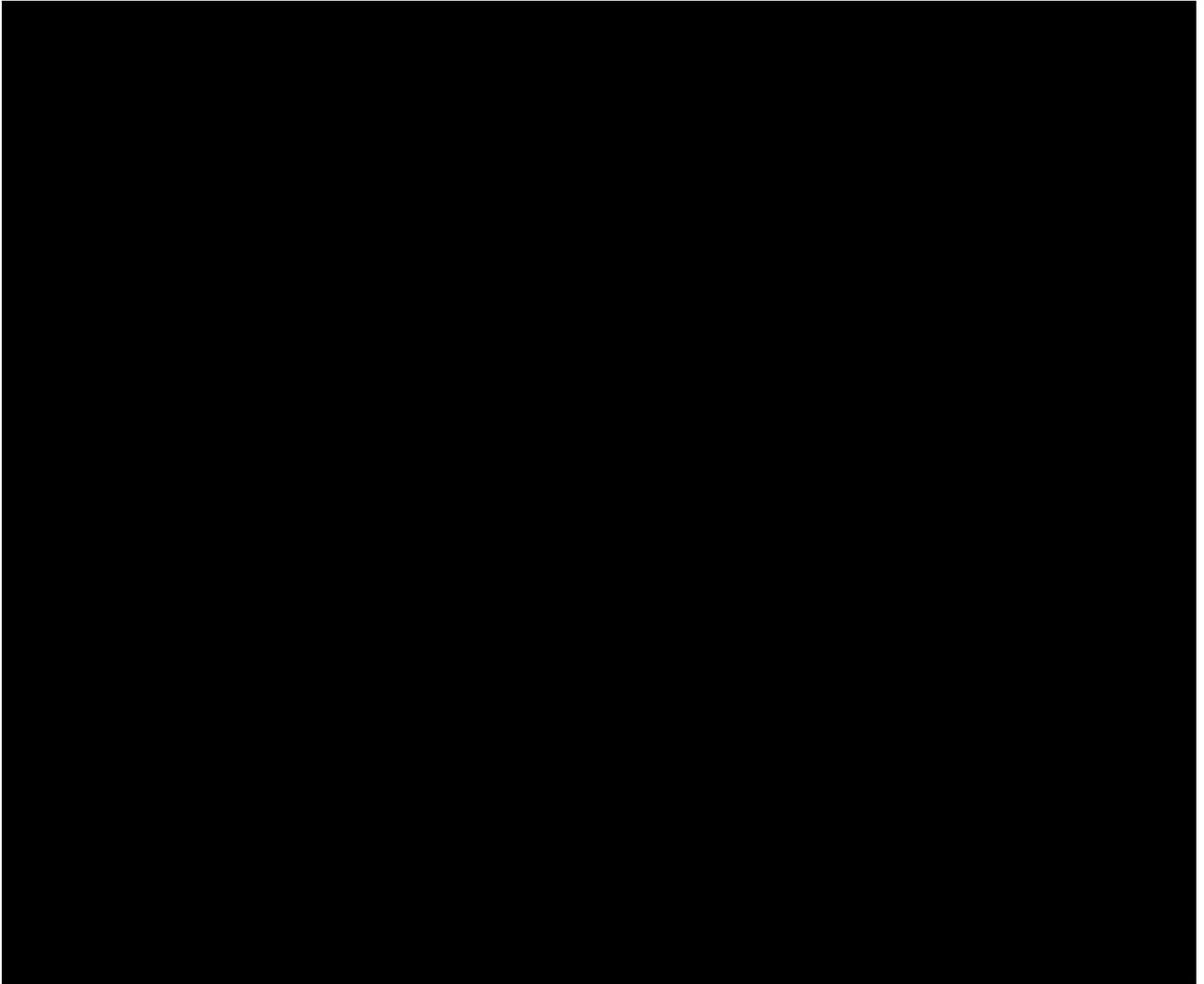
<b>2.</b>	<b>Beschreibung der Kategorien von personenbezogenen Daten</b> <small>(siehe z. B. Art. 28 Abs. 3 S. 1 DSGVO bzw. Art. 30 Abs. 1 S. 2 lit. c)</small>
	<b>darunter Kategorien besonderer personenbezogener Daten</b> <small>(siehe z. B. Art. 9 Abs.1 DSGVO)</small>

<b>3.</b>	<b>Beschreibung der Kategorien betroffener Personen</b> <small>(siehe z. B. Art. 28 Abs. 3 S. 1 DSGVO)</small>

<b>4.</b>	<b>ggf. Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation</b> <small>(siehe z. B. Art. 30 Abs. 1 S. 2 lit. e DSGVO)</small>

<sup>1</sup> Es handelt sich hierbei um gesetzliche Muss-Angaben sowohl bei Auftragsverarbeitung, die der Verordnung (EU) 2016/679 (DSGVO) unterliegt wie auch bei Auftragsverarbeitung, welche den bundes- oder landesrechtlichen Vorschriften zur Umsetzung der Richtlinie (EU) 2016/680 unterliegt. Diese Angaben sind in gleicher Form gesetzlicher Muss-Bestandteil des vom Verantwortlichen zu erstellenden Verzeichnisses aller Verarbeitungstätigkeiten (vgl. Art. 30 Abs.1 DSGVO bzw. die inhaltlich entsprechenden Bestimmungen in den LDSG'en zur Umsetzung der Richtlinie (EU) 2016/680

**Liste der weiteren Auftragsverarbeiter**





## **Service Level Agreement**

### **Verfahrensinfrastruktur im Dataport Rechenzentrum**

#### **Teil A – Allgemeiner Teil -**

**für**

**GeoInformation Bremen**

Lloydstr. 4  
28217 Bremen

nachfolgend Auftraggeber

Version: 2.02  
Stand: 08.08.2019

## Inhaltsverzeichnis

---

<b>1</b>	<b>Einleitung .....</b>	<b>3</b>
1.1	Aufbau des Dokumentes .....	3
1.2	Allgemeine Mitwirkungsrechte und –pflichten .....	3
<b>2</b>	<b>Grundlagen der Leistungserbringung.....</b>	<b>4</b>
2.1	Betrachtung der Servicekette .....	4
2.1.1	Netzwerk-Anbindung .....	4
2.2	Serviceübergreifende Regelungen .....	5
2.2.1	Wartungsfenster .....	5
2.2.2	Supportzeit Standard .....	5
2.2.3	Störungsannahme .....	6
2.2.4	Personendaten der Nutzer für die Störungsannahme .....	6
2.2.5	Changemanagement und Patchmanagement.....	6
2.2.6	Zeitfenster für Sicherheitsupdates .....	7
2.3	Serviceübergreifende Leistungskennzahlen (KPIs) .....	7
2.3.1	Reaktionszeit .....	7
2.4	Betriebsverantwortung.....	7
<b>3</b>	<b>Rollendefinition.....</b>	<b>8</b>
<b>4</b>	<b>Leistungsspezifische KPIs und Reporting.....</b>	<b>9</b>
4.1	Verfügbarkeit (Availability) .....	9
4.2	Auslastung .....	9
<b>5</b>	<b>Störungsprioritäten .....</b>	<b>10</b>
<b>6</b>	<b>Glossar.....</b>	<b>12</b>
6.1	Definition der Verfügbarkeit .....	17
6.1.1	Messung der Verfügbarkeit .....	18
6.1.2	Ausfallzeiten, die die Verfügbarkeit nicht beeinträchtigen.....	18

## 1 Einleitung

---

Dataport stellt Server-Services und Technisches Verfahrensmanagement mit vereinbartem Serviceumfang bedarfsgerecht zur Verfügung. Die allgemeinen Rahmenbedingungen für die Erbringung dieser Services sowie die für einen reibungslosen und effizienten Ablauf notwendigen Rahmenbedingungen ihrer Erbringung sind in diesem Dokument beschrieben.

### 1.1 Aufbau des Dokumentes

Diese Anlage enthält nach der Einleitung die folgenden Kapitel:

- Grundlagen der Leistungserbringung: Betrachtung der Servicekette, serviceübergreifende Regelungen, serviceübergreifende Leistungskennzahlen (KPI)
- Rollendefinitionen
- Leistungsspezifische KPIs und Reporting
- Definitionen und Glossar

### 1.2 Allgemeine Mitwirkungsrechte und –pflichten

Die von Dataport zugesagten Leistungen erfordern Mitwirkungs- und Beistelleistungen des Auftraggebers.

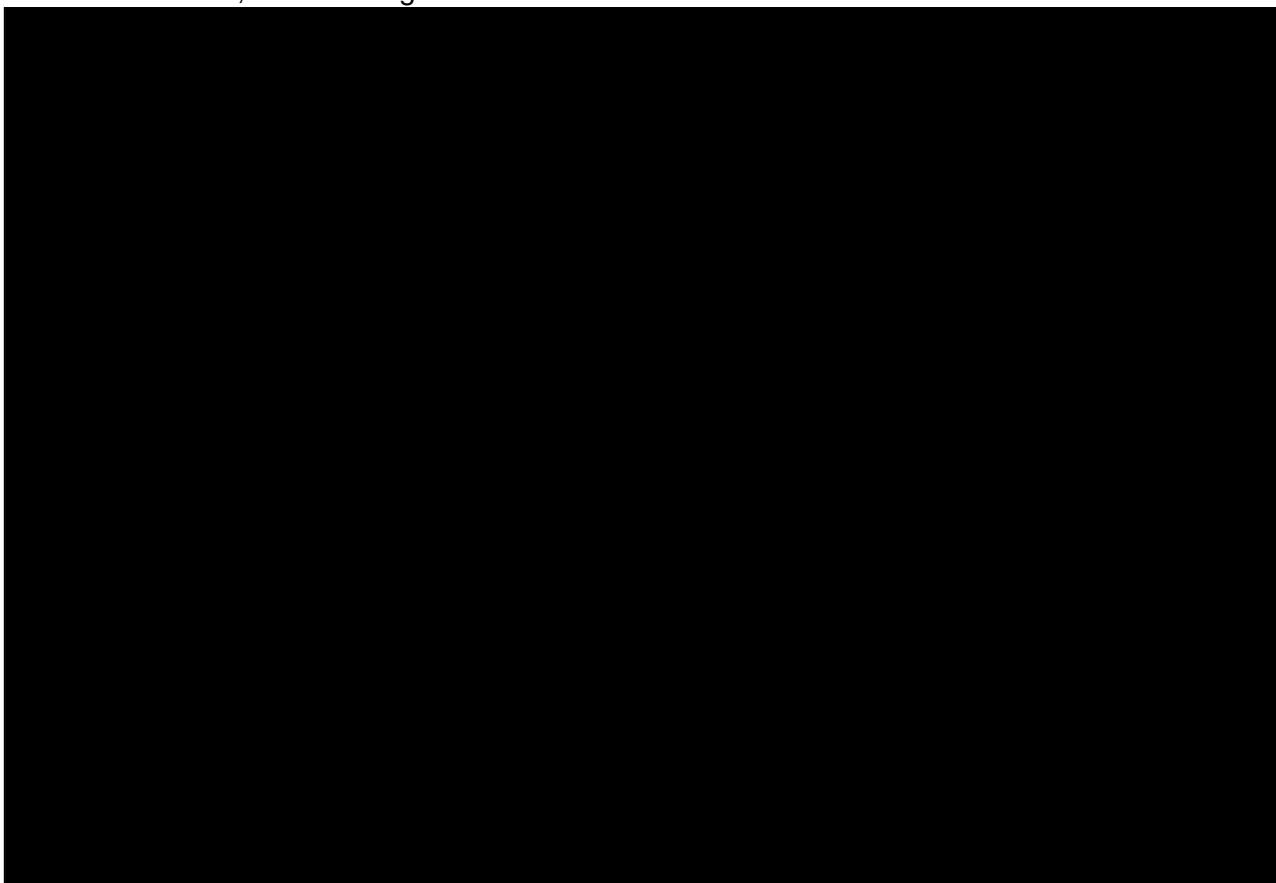
Ergibt sich aus der Unterlassung von Mitwirkungspflichten und Nichtbeistellung des Auftraggebers von vereinbarten Informationen / Daten eine Auswirkung auf die Möglichkeit der Einhaltung der Service Level, entlastet dies Dataport von der Einhaltung der vereinbarten Service Level für den Zeitraum der Unterlassung.

## 2 Grundlagen der Leistungserbringung

---

### 2.1 Betrachtung der Servicekette

Gegenstand dieses SLA sind Serverservices und Technisches Verfahrensmanagement (TVM). Beide benötigen zu ihrer Funktion weitere Infrastrukturservices, die nicht Gegenstand dieses SLA sind. Bei den Infrastrukturservices handelt es sich um die trägerlandspezifischen IT-Querschnittsservices, die eine Funktion der Clients und der Verfahren im RZ ermöglichen (wie Active Directory, File Service, Softwareverteilung, Namensauflösung usw...). Für die Services dieses SLA ist der Leistungsübergabepunkt (LÜP) die WAN-Schnittstelle am Ausgang Rechenzentrum, s. Abbildung.



#### 2.1.1 Netzwerk-Anbindung

Für Dienststellen der Verwaltung des Landes Schleswig-Holstein, der Freien und Hansestadt Hamburg, der Freien Hansestadt Bremen und des Landes Sachsen-Anhalt wird ein direkter Anschluss an das Zugangsnetz; regelhaft über das Landesnetz, vorausgesetzt.

## 2.2 Serviceübergreifende Regelungen

### 2.2.1 Wartungsfenster

Es gilt grundsätzlich folgendes zu Wartungsfenstern:

	Zeitraum
Standard-Wartungsfenster je Woche	Dienstag 19:00 Uhr bis Mittwoch 06:00 Uhr
Besondere Wartungsfenster	Sollte in Sonderfällen ein größeres oder zusätzliches Wartungsfenster erforderlich werden (z.B. wenn größere Installationsarbeiten erforderlich sind), so erfolgt dies in direkter Absprache mit dem Auftraggeber. Solche Arbeiten werden üblicherweise an einem Wochenende vorgenommen.

Der Auftraggeber kann in begründeten Einzelfällen die Nutzung eines Standard-Wartungsfensters untersagen.

### 2.2.2 Supportzeit

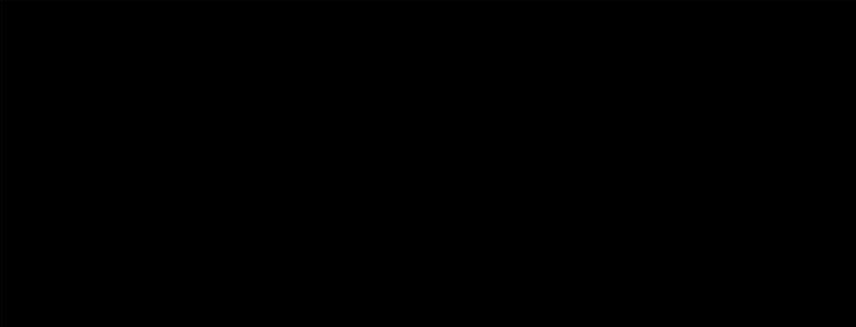
Für alle Services gilt einheitlich die Supportzeit [REDACTED]. Während der Supportzeit werden Störungen behoben und Aufträge angenommen.

Supportzeit	Montag bis Donnerstag	Freitag	Samstag / Sonntag
[REDACTED]	08:00 - 17:00 Uhr	08:00 – 15:00 Uhr	-
	<i>(ohne die für Schleswig-Holstein gültigen gesetzlichen Feiertage und ohne 24.12., 31.12.)</i>		

Bei Bedarf kann die Supportzeit für die Störungsbehebung erweitert werden (siehe Ziffer 2.1.1 Teil B)

### **2.2.3 Störungsannahme**

Das Callcenter ist grundsätzlich Ansprechpartner für Störungen in der Supportzeit [REDACTED]



Für Auftraggeber mit Full-Client-Support gelten die Meldewege gemäß der entsprechenden vertraglichen Vereinbarung.

Im Rahmen der Störungsannahme werden grundsätzlich Melderdaten (siehe 2.2.4) sowie die Störungsbeschreibung erfasst und gespeichert. Der Störungsabschluss wird dem meldenden Nutzer bekannt gemacht. Die Daten werden über den Zeitpunkt des Störungsabschlusses hinaus gespeichert. Die konkrete Art und Umfang ist dem Verfahrensverzeichnis für das Dataport Ticketsystem gemäß Artikel 30 Abs. 1 DSGVO zu entnehmen.

### **2.2.4 Personendaten der Nutzer für die Störungsannahme**

Regelhaft werden die über das Kontenpflegetool eingetragenen Personendaten aus den Active-Directories der Trägerländer für die Störungsannahme in den Tickets verwendet. Abweichende Fälle sind im Teil B unter Ziffer 1.4 geregelt.

### **2.2.5 Changemanagement und Patchmanagement**

Changes dienen zur Umsetzung von beauftragten Maßnahmen wie auch zur Aufrechterhaltung der vertragsgemäßen Leistungserbringung. Patches sind eine Teilmenge der Changes.

Generell ist der Auftragsverarbeiter verantwortlich für die Durchführung aller Maßnahmen, die dazu dienen, alle einem Verfahren zugrundeliegenden Systemkomponenten gemäß dem aktuellen Stand der Technik zu halten. (Branchenspezifische Sicherheitsstandards (B3S)).

Im Rahmen des Patchmanagements werden regelmäßig in Abhängigkeit einer Risikoeinschätzung des Auftragsverarbeiters alle Systemkomponenten mit den von den Herstellern bereitgestellten Updates versorgt. Der Auftragsverarbeiter stellt hierdurch sicher, dass alle Systemkomponenten des Fachverfahrens, welche gemäß des Dataport Standards installiert wurden, über einen aktuellen Softwarestand verfügen. Hierzu gehören auch systemnahe Anwendungen, wie z. B. Datenbanken und Webserver, für welche innerhalb des aktuellen Releases des Fachverfahrens neue Versionen oder Patches erscheinen.

Für Komponenten, welche durch den Softwarehersteller des Fachverfahrens ausgeliefert und/oder in die Fachanwendung integriert wurden, sind Aktualisierungen regelhaft in den vom Hersteller vorgegebenen Zyklen durch den Auftraggeber beizustellen.

Patchmanagement ist notwendig, damit ein sicherer Betrieb im Sinne des BSI Grundschutzes gewährleistet werden kann. Es ist Aufgabe des Auftraggebers, den Verfahrenshersteller auf die Verwendung von im Support befindlicher Software hinzuweisen und rechtzeitig einen Wechsel

einzuplanen, wenn genutzte Anwendungen ihr End of Support (EOS) erreichen, sofern diese Aufgabe durch den Auftragsverarbeiter nicht im Rahmen einer Beauftragung zum fachlichen Verfahrensmanagement erbracht wird.

### 2.2.6 Zeitfenster für Sicherheitsupdates

Jedes Serversystem erhält zusätzlich zum Wartungsfenster ein monatliches Maintenance Window (MW), in denen relevante Sicherheitsupdates automatisch installiert werden. Das MW wird im Rahmen der erstmaligen Herstellung der Betriebsbereitschaft (EHdB) für jedes Serversystems in Abstimmung mit dem Auftraggeber festgelegt und in der Verfahrensdokumentation hinterlegt. Damit ist gewährleistet, dass jedes Serversystem im Sinne des BSI Grundschutzes zeitnah mit allen kritischen Sicherheitsupdates versorgt wird. Das MW ist ein zentraler Bestandteil des Sicherheitskonzeptes für Serversysteme. Das MW kann im Rahmen des Change-Prozesses durch den Auftraggeber geändert werden.

## 2.3 Serviceübergreifende Leistungskennzahlen (KPIs)

### 2.3.1 Reaktionszeit

Es gelten einheitlich folgende Reaktionszeiten bei Störungen (je Störungspriorität und während der Supportzeit):

Störungspriorität <sup>1</sup>	Reaktionszeiten
Kritisch (1)	
Hoch (2)	
Mittel (3)	
Niedrig (4)	

Die vereinbarte Zielwahrscheinlichkeit  $P_{\text{Soll}}$  für die Erreichung der Reaktionszeiten pro Kalendermonat beträgt ██████

#### Reporting

Reports werden je Monat (nach Anforderung auch je Arbeitstag) zur Verfügung gestellt.

## 2.4 Betriebsverantwortung

Grundsätzlich liegt die Betriebsverantwortung für den Betrieb der Server-Services und der Middlewarekomponenten beim Auftragsverarbeiter. Der Auftraggeber hat keinen administrativen Zugriff auf Server, Datenbanken, Fileservice.

Ist im Einzelfall eine geteilte Betriebsverantwortung erforderlich, werden Details in Teil B geregelt.

<sup>1</sup> Für eine detaillierte Definition siehe Ziffer 4 in diesem Dokument

### 3 Rollendefinition

---

Die allgemeine Zuordnung von Aufgaben zu Rollen ist wie folgt definiert:

Rolle	Rollendefinition
Auftraggeber (AG)	Rolle des Auftraggebers im Sinne der DSGVO
Auftragsverarbeiter (AV)	Zentraler Betrieb, Auftragsverarbeiter im Sinne der DSGVO
Auftragsberechtigte (AB)	Abruf von im Vertrag definierten Services des Auftragsverarbeiters Der Abruf erfolgt durch vom Auftraggeber benannte autorisierte Auftragsberechtigte. Der Auftraggeber benennt diese Personen und pflegt die Liste der autorisierten Auftragsberechtigten.
Nutzer	Nutzer sind alle Endanwender, die das Verfahren nutzen. Nutzer müssen nicht Mitarbeiter des Auftraggebers sein.

## 4 Leistungsspezifische KPIs und Reporting

---

### 4.1 Verfügbarkeit (Availability)

Definition siehe Teil A; Ziffer 6.1

Die Verfügbarkeit des Business Services wird am Leistungsübergabepunkt je Umgebung der Verfahrensinfrastruktur gemessen und monatlich berichtet. Je Verfahrensumgebung (Produktion, Qualitätssicherung, Test / Entwicklung und Schulung) wird ein gesonderter Report erstellt.

### 4.2 Auslastung

Das monatliche Auslastungs-Reporting ist eine Darstellung der Auslastung der Verfahrensumgebungen zur Einschätzung des System-Sizings.

- Der Grad der Auslastung wird in Form eines Ampel-Reports grafisch und mit Prozentwerten dargestellt.
- Der Report umfasst alle beauftragten Verfahrensumgebungen.
- Im Auslastungsreporting wird je technischer Servicekomponente die Auslastung im Verhältnis zur beauftragten Kapazität ausgewiesen. Im typischen Fall wird also je Server die CPU-, RAM- sowie Speicherauslastung im Messzeitraum angegeben.

## 5 Störungsprioritäten

Die Störungsmeldungen von Auftraggeber / Nutzern werden durch den Auftraggeber wie folgt kategorisiert und vom Auftragsverarbeiter bearbeitet:

Auswirkung		Großflächig / Verbreitet	Erheblich / Groß	Moderat / Begrenzt	Gering / Lokal
Dringlichkeit	Kritisch	Kritisch	Kritisch	Hoch	Hoch
	Hoch	Kritisch	Hoch	Hoch	Mittel
	Mittel	Hoch	Hoch	Mittel	Niedrig
	Niedrig	Hoch	Mittel	Niedrig	Niedrig

Die Priorisierung ergibt sich nach der oben abgebildeten Matrix aus den Komponenten Auswirkung und Dringlichkeit. Die Auswirkung bezeichnet den Einfluss, den die Störung auf die geschäftliche Aktivität hat. Die Dringlichkeit einer Störung ist davon abhängig, ob Ersatzwege für die betroffene Tätigkeit möglich sind oder die Tätigkeit zurückgestellt bzw. nachgeholt werden kann. Die Priorität (innerer Teil der Matrix) legt die Geschwindigkeiten fest, mit denen die Störung bearbeitet wird und bestimmt die Überwachungsmechanismen:

Priorität	Kritisch	Führt zur umgehenden Bearbeitung durch Dataport und unterliegt einer intensiven Überwachung des Lösungsfortschritts
	Hoch	Führt zur bevorzugten Bearbeitung durch Dataport und unterliegt einer besonderen Überwachung des Lösungsfortschritts.
	Mittel	Führt zur forcierten Bearbeitung durch Dataport und unterliegt der Überwachung des Lösungsfortschritts.
	Niedrig	Führt zur standardmäßigen Bearbeitung durch Dataport und unterliegt der Überwachung des Lösungsfortschritts.

Auswirkung	Großflächig / Verbreitet	Viele Nutzer sind betroffen. Geschäftskritische Systeme sind betroffen. Die Geschäftstätigkeit kann nicht aufrechterhalten werden.
	Erheblich / Groß	Die Geschäftstätigkeit kann eingeschränkt aufrechterhalten werden.
	Moderat / Begrenzt	Wenige Nutzer sind von der Störung betroffen. Geschäftskritische Systeme sind nicht betroffen. Die Geschäftstätigkeit kann mit leichten Einschränkungen aufrechterhalten werden.
	Gering / Lokal	Die Störung betrifft einzelne Nutzer. Die Geschäftstätigkeit ist nicht eingeschränkt.

Dringlichkeit	Kritisch	Ersatz steht nicht zur Verfügung. Die Tätigkeit, bei der die Störung auftrat, kann nicht verschoben oder anders durchgeführt werden.
	Hoch	Ersatz steht kurzfristig nicht zur Verfügung. Die Tätigkeit, bei der die Störung auftrat, muss kurzfristig durchgeführt werden.
	Mittel	Ersatz steht nicht für alle betroffenen Nutzer zur Verfügung. Die Tätigkeit, bei der die Störung auftrat, kann später oder auf anderem Wege evtl. mit mehr Aufwand durchgeführt werden.
	Niedrig	Ersatz steht zur Verfügung und kann genutzt werden, oder das betroffene System muss aktuell nicht genutzt werden. Tätigkeiten, deren Durchführung durch die Störung behindert wird, können später durchgeführt werden.

Die Bewertung erfolgt unter Einbeziehung der Einschätzung des Nutzers durch das Service-Desk.

Der Prozess zur Störungsbearbeitung bei Dataport enthält Eskalationsverfahren, die sicherstellen, dass die zugesagten Reaktionszeiten eingehalten werden und dass eine zuverlässige und schnellstmögliche Störungsbearbeitung erfolgt.

Als Ergänzung können im SLA Verfahrensinfrastruktur Teil B spezifische Festlegungen zur Kategorie von Störungsmeldungen getroffen werden. Insbesondere bei Eingrenzung der Berechtigung zur Störungsmeldung (Ziffer 1.4 Teil B) kann der Auftraggeber die Störungspriorität festlegen.

## 6 Glossar

Begriff	Definition
Application Layer Gateway (ALG)	Sicherheitskomponente in einem Computernetzwerk
Bearbeitungszeit	Die Bearbeitungszeit ist die Zeitspanne zwischen der Beauftragung eines Services bzw. einer Aktivität durch den Auftraggeber über einen vorgegebenen Weg (z. B. Auftrag zum Einrichten eines Telefonanschlusses) bis zur erfolgreichen Durchführung des beauftragten Services bzw. der Aktivität.
Betriebszeit	Die Betriebszeit ist der Zeitraum, in dem die vereinbarten Ressourcen (Services) vom Auftragsverarbeiter (AV) zur Verfügung gestellt werden und grundsätzlich genutzt werden können. Dies ist generell an 365 Tagen pro Jahr, 24 h pro Tag, der Fall. Die Betriebszeit wird eingeschränkt durch Zeiten, zu denen auf Grund von höherer Gewalt keine Dienstleistung möglich ist und durch Wartungsarbeiten.
Bezugsgröße	Messgröße, bezogen auf die eine Leistungskennziffer definiert ist. Beispiel: Die Leistungskennziffer „Reaktionszeit“ ist bezogen auf die Bezugsgröße „Supportzeit“ definiert.
Bezugszeitraum (Messzeitraum)	Der Zeitraum, auf den sich eine Leistungskennziffer bezieht und in dem die tatsächlich erbrachte Qualität der Leistung gemessen wird. Sofern nicht anders angegeben (z. B. im Fall der Verfügbarkeit) beziehen sich alle angegebenen Metriken jeweils auf einen Messzeitraum von einem Kalendermonat.
Business Service (BS)	Bündelung von IT-Services
Callcenter	Das Callcenter ist grundsätzlich Ansprechpartner für Störungen.
Fachliches Verfahrensmangement (FVM)	Das fachliche Verfahrensmangement umfasst administrative Tätigkeiten innerhalb der Verfahrensoftware (nicht auf Systemebene oder innerhalb systemnaher Software). Ein Nutzer mit einer Rolle und Aufgaben im FVM hat administrative Rechte im Verfahren und damit weitergehende Rechte als ein normaler Verfahrensnutzer.
IT Infrastructure Library (ITIL)	Sammlung von „Best Practice“ Prozessen und Methoden zur Definition, Erbringung und Veränderung von IT-Services für Auftraggeber und Nutzer sowie zum Management von Störungen der Serviceerbringung.
Key Performance Indikator (KPI)	Vertragliche Leistungskennzahl, für das leistungsabhängige Soll-Werte definiert sind, die gegen Ist-Werte gemessen werden (oder werden sollen).

Begriff	Definition
Kundenreport	Auftraggeber-spezifischer Bericht über die SLA-Erfüllung und ggfs. weitere Business Service-Details (z.B. Bestände).
Leistung	Elemente von Services mit OLA zur Dataport-internen Steuerung
Leistungsübergabepunkt (LÜP)	Bezugspunkt der Definition von Service Leveln. Die Services werden dem Auftraggeber am LÜP zur Verfügung gestellt. Einflüsse auf die Servicequalität ab LÜP sind nicht Bestandteil der vom Auftragsverarbeiter zugesagten Leistungen. Analog sind die Details der Serviceerbringung durch den Auftragsverarbeiters bis zum LÜP alleine unter der Verantwortung des AV.
Operational Level Agreement (OLA)	Dataport-interne Beschreibung von Leistungen nach ihrer Qualität und Ausprägung. Zweck ist die interne Absicherung der nach außen bzw. gegenüber dem Auftraggeber zugesagten Service Levels.
Reaktionszeit	Die Reaktionszeit ist die Zeitspanne zwischen der Meldung einer Störung über den vereinbarten Störmeldeweg und dem Beginn der inhaltlich qualifizierten Bearbeitung durch Dataport. Zur Messung der Reaktionszeit wird der Zeitpunkt der Störungsmeldung und der Status „in Bearbeitung“ in der ITSM Suite bei Dataport verwendet. Die Reaktionszeit ist grundsätzlich abhängig von der Priorität der Störung. Je nach SLA-Klasse im Servicekatalog sind die Prioritäten „kritisch“ oder „hoch“ evtl. nicht verfügbar.
Twin Data Center	Dataport Rechenzentren in Alsterdorf und Norderstedt
Security Service Level Agreement (SSLA)	Ergänzung eines SLA zur Verfahrensinfrastruktur. Mit dem Security Service Level Agreement wird zwischen den Vertragspartnern vereinbart, wie der Betrieb unter Informationssicherheitsgesichtspunkten auf Basis des IT-Grundschutzes des Bundesamtes für Informationssicherheit (BSI) unter Nutzung des Sicherheitsmanagementsystems des Auftragsverarbeiters erfolgt.
Service	Standardisierte Bündelung von Leistungen; aufgeführt im Servicekatalog und relevant für die Preisgestaltung
Service Desk	Das Service Desk ist die Anlaufstelle für die Nutzer, d.h. alle Störungen werden hier zunächst angenommen und bearbeitet. Regelmäßig wird diese Aufgabe vom Callcenter übernommen

Begriff	Definition
Service Fernzugriff Administrativ (SFA)	<p>Der Service stellt dem Auftraggeber für administrative Aufgaben personalisierte Accounts zur Verfügung und beinhaltet folgende Leistungen:</p> <ul style="list-style-type: none"> <li>• Einrichtung von Accounts für Administratoren des Auftraggebers</li> <li>• Bereitstellung der Infrastruktur für den Administrativen Zugang einschließlich der Lizenzkosten für Clientkomponenten</li> <li>• Durchführung der ITIL Prozesse durch Dataport</li> <li>• Technische Beratungsleistung für die Umsetzung der administrativen Aufgaben (z.B. Anmeldung, Administration eines Servers,...)</li> </ul> <p>Die Betriebsverantwortung für Fachverfahren/ Applikationen liegt beim Auftraggeber (i.d.R. keine oder nur eingeschränkte TVM-Services durch Dataport). Die zugrundeliegenden technischen Infrastrukturen dafür sind über die entsprechenden Server Services gesondert zu bestellen.</p>
Service-Koordination	Dataport-Ansprechpartner für den Auftraggeber und Auftragsberechtigte hinsichtlich individueller Serviceanfragen bei bestehenden Verträgen.
Service Level Agreement (SLA)	Beschreibung von Business Services nach ihrer Qualität und Ausprägung. Ein SLA beschreibt verkaufsfähig gebündelte Leistungen sowie ihre Messung und ihr Reporting gegenüber dem Auftraggeber.
Service Request (SR)	Anfrage nach einem Service, der den Rahmen des vordefinierten Standards in Verträgen übersteigt und gesondert / individuell betrachtet und beantwortet werden muss.
Service-Kette	Gesamtheit der von einem Auftraggeber genutzten Business Services über alle Kategorien und Verträge des Auftraggebers hinweg.
Sollwert	Zu erreichender Wert einer Kennziffer. Für eine vereinbarungsgemäße Erbringung einer Leistung muss die tatsächliche Leistungsqualität (z. B. Verfügbarkeit, Reaktionszeit) gleich oder besser als der Sollwert sein (z. B. $Verfügbarkeit_{Ist} \geq Verfügbarkeit_{Soll}$ ; $Reaktionszeit_{Ist} \leq Reaktionszeit_{Soll}$ ).
Standard Service Request (SSR)	Vordefiniertes Serviceangebot in einem Vertrag, das von Auftragsberechtigten bei Dataport mit bestimmten Konditionen (z. B. festgelegten Bearbeitungszeiten) und üblicherweise über bestimmte Wege (über einen Shop oder ein Portal) beauftragt werden kann.

Begriff	Definition
Supportzeit	<p>Die Supportzeit Standard beschreibt den Zeitraum, in dem Störungen und Anfragen entgegengenommen werden und auf sie reagiert wird.</p> <p>In der erweiterten Supportzeit werden nur Störungen entgegengenommen und bearbeitet.</p> <p>Die Supportzeit liegt innerhalb der Betriebszeit und kann sich auch über das Wartungsfenster erstrecken</p>
Technisches Verfahrensmanagement (TVM)	<p>Das technische Verfahrensmanagement umfasst administrative Tätigkeiten in systemnaher Software (Middleware oder Betriebssystem), die nicht verfahrensspezifisch sind. Dabei kann es sich um Zugriffe auf Datenbanken, Webserver, Terminal-Services oder Virtualisierungslösungen handeln. Das technische Verfahrensmanagement setzt auf der Systemadministration auf.</p>
User Help Desk (UHD)	<p>Der User Help Desk ist eine besondere Ausprägung des Service Desk bei Dataport bei entsprechender gesonderter vertraglicher Grundlage.</p> <p>Der UHD hat die schnellstmögliche Wiederherstellung der Arbeitsfähigkeit der Nutzerin/des Nutzers im Falle von IT-Störungen zum Ziel. Dazu übernimmt der User Help Desk in einem definierten Rahmen für definierte Produkte Handling Hilfe im Rahmen der Erstlösung für die Nutzerin/den Nutzer. Der User Help Desk übernimmt auch die Annahme und die Bearbeitung von Incidents.</p>
Verfahren	<p>Die IT-Unterstützung für die Durchführung von Fachaufgaben des Auftraggebers</p>

Begriff	Definition
Verfahrens-umgebungen	<p>Verfahrensumgebungen können in folgenden Produktionsstufen bereitgestellt werden:</p> <ul style="list-style-type: none"> <li>• Schulung: Abbild der Produktivumgebung in einem geringeren Umfang. Ohne Anbindung an produktive Systeme; keine Verarbeitung von Echtdaten</li> <li>• Test: Umgebung für den Test neuer Softwareversionen, die i.d.R. eingekauft werden. keine Verarbeitung von Echtdaten</li> <li>• Entwicklung: Umgebung, auf der Software entwickelt und weiterentwickelt wird. Im Zuge dessen erfolgen auch Softwaretests auf dieser Umgebung. keine Verarbeitung von Echtdaten</li> <li>• Qualitätssicherung: Stellt ein Abbild der Produktivumgebung da; im Regelfall in deutlich reduzierter Skalierung. Updates des Fachverfahrens sowie Patche der Betriebssysteme oder Middleware werden auf dieser Umgebung eingespielt, um vor Produktivsetzung die Funktion zu testen; einschließlich Test der Schnittstellen. Regelmäßig keine Verarbeitung von Echtdaten</li> <li>• Produktion: Die Umgebung auf der das Fachverfahren betrieben wird; Verarbeitung der Echtdaten</li> </ul>
Vertrag	<p>Ein Vertrag kontrahiert eine gegen Entgelt angebotene Bündelung eines oder mehrerer Business Services.</p>
Wide Area Network (WAN)	<p>Rechnernetz, welches sich über einen sehr großen geografischen Bereich erstreckt.</p>
Wartungsfenster	<p>Zeitfenster für Wartungsarbeiten an den Systemen. Es wird zwischen dem Standard-Wartungsfenster (regelmäßig pro Woche) und besonderen Wartungsfenstern (auf gesonderte Vereinbarung) unterschieden.</p> <p>Das Wartungsfenster liegt in der Betriebszeit.</p> <p>Während des Wartungsfensters muss nicht generell von einer Nichtverfügbarkeit der Services ausgegangen werden. Jedoch sind im Wartungsfenster Serviceunterbrechungen möglich.</p> <p>Sollte in Sonderfällen ein längeres Wartungsfenster beansprucht werden, so erfolgt dies in direkter Absprache mit dem Auftraggeber. Der Auftraggeber wird nur in begründeten Fällen die Durchführung von Wartungsmaßnahmen einschränken. Der Auftragsverarbeiter wird in diesen Fällen unverzüglich über sich ggf. daraus ergebenden Mehraufwand und Folgen informieren.</p>

Begriff	Definition
Zielwahrscheinlichkeit ( $P_{\text{Soll}}$ )	<p>Zusätzlich zum Sollwert kann eine Wahrscheinlichkeit angegeben werden, mit der der Sollwert während des Bezugszeitraumes (Messzeitraumes) erreicht werden soll. Ist keine Zielwahrscheinlichkeit angegeben, so gilt eine Zielwahrscheinlichkeit von 100%, d.h. alle gemessenen Leistungen müssen gleich oder besser als der Sollwert sein.</p> <p>Eine Zielwahrscheinlichkeit kann nur für Kennziffern angegeben werden, die in vielen Einzelmessungen oder Einzelereignissen bestimmt werden (z. B. Reaktionen auf einzelne Störungen).</p> <p>Beispiel: Leistungskennziffer sei die Reaktionszeit, der Sollwert sei 30 Minuten, die Zielwahrscheinlichkeit sei 90%, der Bezugszeitraum sei ein Kalendermonat. Dies bedeutet, dass in einem Kalendermonat mindestens 90% aller tatsächlichen Reaktionszeiten <math>\leq 30</math> Minuten betragen müssen.</p>

### 6.1 Definition der Verfügbarkeit

Die Verfügbarkeit ist der prozentuale Anteil an der zugesagten Bezugszeit, in der die jeweilige Verfahrensinfrastruktur am Leistungsübergabepunkt erreichbar ist.

$$\text{Verfügbarkeit} = \frac{\text{Bezugszeit} - \text{ungeplanter Ausfallzeit}}{\text{Bezugszeit}}$$

Betrachtet auf den Bezugszeitraum. Geplante Ausfallzeiten sind grundsätzlich mit dem Auftraggeber abgestimmt.

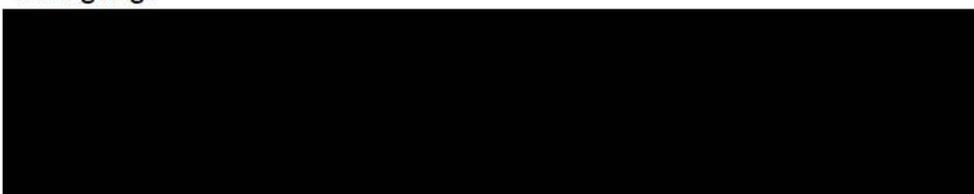
Für die Bezugszeit gilt:

Bezogen auf die Betriebszeit werden die Verfahrensinfrastrukturen grundsätzlich mit der Verfügbarkeitsklasse ██████████ zur Verfügung gestellt.

Ausnahme: wenn für die Verfahrensinfrastruktur die Verfügbarkeitsklasse „Economy“ ausgewählt wurde, erfolgt keine Verfügbarkeitszusage bezogen auf die Betriebszeit

Bezogen auf die Supportzeit werden die Verfahrensinfrastrukturen mit der jeweils vereinbarten Verfügbarkeitsklasse (Economy bis Premium +) bereitgestellt. Die Supportzeit umfasst auch die optionalen zu beauftragenden erweiterten Supportzeiten.

Grundsätzlich stehen folgenden Verfügbarkeitsklassen für Verfahrensinfrastrukturen zur Verfügung:



### **6.1.1 Messung der Verfügbarkeit**

Die Verfügbarkeit der Verfahrensinfrastruktur wird konkret ermittelt durch eine Verarbeitung der Systemmeldungen der jeweils relevanten Komponenten, die mittels eines jeweils individuellen Modells, das Redundanzen und Abhängigkeiten berücksichtigt, den Gesamtwert ergeben. Zum Reporting siehe Teil B; Ziffer 4.2

### **6.1.2 Ausfallzeiten, die die Verfügbarkeit nicht beeinträchtigen**

Bei der Berechnung der Verfügbarkeit werden nicht berücksichtigt:

- Geplante Ausfallzeiten im Wartungsfenster
- Ungeplante Ausfallzeiten aufgrund von höherer Gewalt und Katastrophen
- Ausfallzeiten aufgrund minderer Qualität von beigestellter Software, z.B. durch
  - den Verzicht auf eine Qualitätssicherungs-Umgebung erhöht das entsprechende Risiko in der Produktionsumgebung oder
  - fehlerhafte Verfahrensupdates und -patches
- Unterbrechung aufgrund von Vorgaben des Auftraggebers
- Ausfallzeiten infolge Unterbleibens oder verzögerter Erfüllung von Mitwirkungspflichten durch den Auftraggeber
  - Hier auch insbesondere in Folge geteilter Betriebsverantwortung



## **Service Level Agreement**

### **Verfahrensinfrastruktur im Dataport Rechenzentrum**

#### **Teil B (spezifischer Teil für Verfahren DIPAS Bremen (DIPAS\_HB001))**

**für**

##### **GeoInformation Bremen**

Lloydstr. 4  
28217 Bremen

nachfolgend Auftraggeber

Version: 1.0  
Stand: 06.09.2021



## Inhaltsverzeichnis

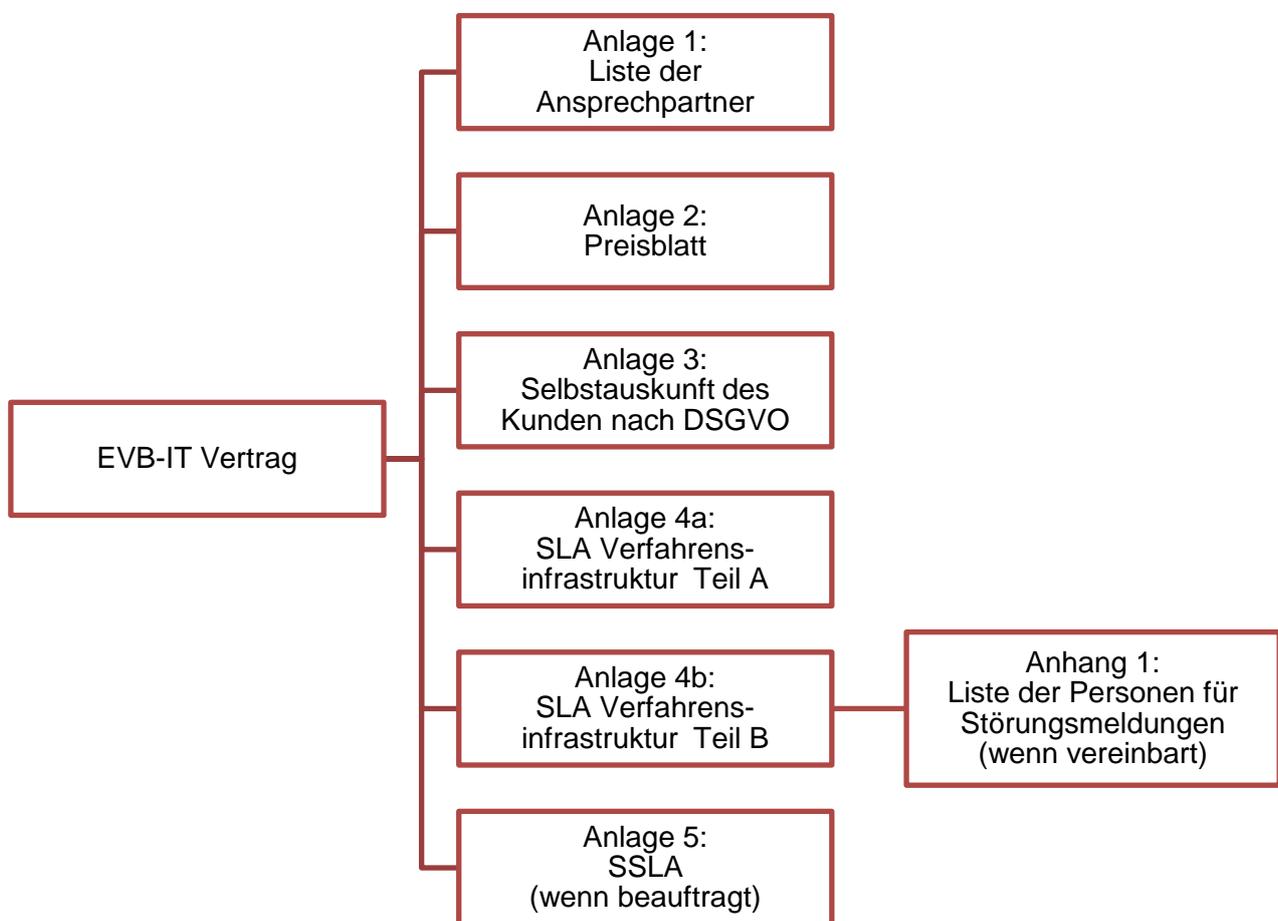
---

<b>Inhaltsverzeichnis .....</b>	<b>2</b>
<b>1 Einleitung .....</b>	<b>3</b>
1.1 Einbindung des SLAs in die Vertragsstruktur .....	3
1.2 Aufbau des Dokumentes .....	3
1.3 Rollenzuordnung.....	3
1.4 Mitwirkungsrechte und –pflichten .....	4
<b>2 Rahmen der Leistungserbringung .....</b>	<b>5</b>
2.1 Servicerelevante Regelungen .....	5
2.1.1 Supportzeiten.....	5
<b>3 Leistungsbeschreibung Verfahrensinfrastruktur .....</b>	<b>5</b>
3.1 Beschreibung des Fachverfahrens .....	5
3.2 Bereitgestellte Umgebungen .....	5
3.2.1 Leistungsbeschränkung bei Verzicht von zusätzlichen Umgebungen .....	5
3.3 Details zu Server-Services .....	6
3.3.1 Bereitgestellte Server-Services .....	6
3.3.2 Zentraler Fileservice .....	7
3.3.3 Fileservice Economy.....	7
3.3.4 Application Level Gateway-Funktionalität (ALG).....	7
3.3.5 Backup & Recovery .....	7
3.4 Geteilte Betriebsverantwortung/ Service Fernzugriff Administrativ (SFA).....	8
3.4.1 Mitwirkungsleistungen des Auftraggebers.....	8
3.5 Details zum Technischen Verfahrensmanagement.....	8
3.5.1 Serviceklassifikation .....	8
3.5.2 Schnittstellen zu anderen Fachverfahren .....	9
3.5.3 Benutzerverwaltung .....	9
3.5.4 Betrieb und Implementierung von Non-Standard Datenbanken.....	9
3.5.5 Zeitlich befristeter und überwachter Fernzugriff .....	9
<b>4 Leistungsspezifische KPIs und Reporting.....</b>	<b>11</b>
<b>5 Maßnahmen bei Beendigung der Leistung .....</b>	<b>12</b>

## 1 Einleitung

Dataport stellt Verfahrensinfrastrukturen (Server-Services und Technisches Verfahrensmanagement) im vereinbartem Serviceumfang bedarfsgerecht zur Verfügung. Die spezifischen Rahmenbedingungen für die Erbringung dieser Services, sowie die für einen reibungslosen und effizienten Ablauf notwendigen Festlegungen ihrer Erbringung, sind in diesem Dokument beschrieben.

### 1.1 Einbindung des SLAs in die Vertragsstruktur



### 1.2 Aufbau des Dokumentes

Diese Anlage enthält nach der Einleitung die folgenden Kapitel:

- Mitwirkungsleistungen des Auftraggebers, konkrete Rollenfestlegung
- die Leistungsbeschreibung: Server-Services und TVM

### 1.3 Rollenzuordnung

Für diesen SLA sind die Rollen wie folgt zugeordnet:

Rolle	Rolleninhaber
Auftraggeber (AG)	Siehe EVB-IT
Auftragsverarbeiter (AV)	Siehe EVB-IT
Nutzer	Nutzer der Verfahrensinfrastruktur, müssen nicht dem Auftraggeber zugehörig sein

Die Definitionen der Rollen können dem Glossar (Teil A, Abschnitt 3) entnommen werden.

## 1.4 Mitwirkungsrechte und –pflichten

Der Auftraggeber kann den Kreis der Nutzer, die berechtigt sind Störungen zu melden, eingrenzen. (z.B. auf IT-Verantwortliche oder fachliche Leitstellen). Diese sind in einem gesonderten Anhang zu benennen. Die im Anhang aufgeführten Personen / Einrichtungen sind berechtigt, die Priorität von Störungsmeldungen festzulegen.

Der Auftraggeber, die Auftragsberechtigten und die Nutzer verpflichten sich, den Auftragsverarbeiter in geeigneter Weise bei der Abwicklung von Aufträgen, der Aufdeckung und Beseitigung von Mängeln sowie der Bearbeitung von Sicherheitsvorfällen zu unterstützen.

Ein Sonderfall der Mitwirkung des Auftraggebers ist die geteilte Betriebsverantwortung (siehe Abschnitt 3.5).

Der Auftraggeber stellt dem Auftragsverarbeiter die Fachanwendung und die notwendigen Lizenzen zur Verfügung.

## 2 Rahmen der Leistungserbringung

---

### 2.1 Servicerelevante Regelungen

#### 2.1.1 Supportzeiten

Die Supportzeit Standard (siehe Teil A; Abschnitt 2.2.2) kann für die Störungsannahme und –bearbeitung erweitert werden. In der, über die Supportzeit Standard hinausgehenden, Erweiterten Supportzeit erfolgt keine Auftragsannahme.

Es wird keine Erweiterte Supportzeit beauftragt.

## 3 Leistungsbeschreibung Verfahreninfrastruktur

---

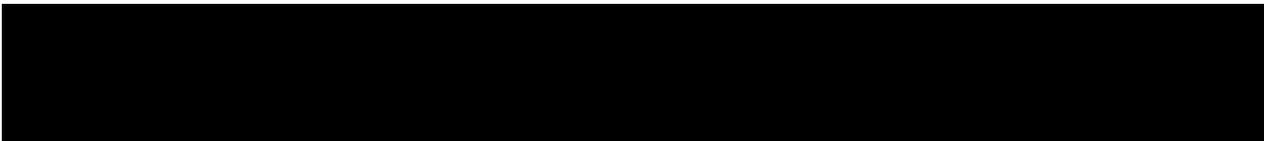
Für das nachfolgend beschriebene Fachverfahren werden eine oder mehrere Umgebungen entsprechend den jeweiligen Produktionsstufen im Rechenzentrum von Dataport bereitgestellt. Die jeweilige Umgebungsstruktur nutzt die RZ-Basisdienste entsprechend der ausgewählten SLA-Klasse, dem Sicherheitsbereich, den erforderlichen Serverrollen und dem Umfang an Verfahrensbetriebsleistungen.

Grundlage der Verfahreninfrastruktur, die sich aus den Server-Services und dem Technischen Verfahrenmanagement zusammensetzt, sind die entsprechenden Services aus dem Servicekatalog von Dataport in der aktuell gültigen Fassung.

### 3.1 Beschreibung des Fachverfahrens

DIPAS verbindet das Hamburger Online-Beteiligungstool mit digitalen Planungstischen zu einem integrierten digitalen System zur Bürgerbeteiligung. Mit DIPAS können Bürgerinnen und Bürger von zu Hause aus mit dem Smartphone oder in Veranstaltungen mithilfe interaktiver Datentische digitale Karten, Luftbilder, 3D Modelle sowie weitere Geodaten abrufen und ein genau lokalisiertes Feedback zu Planungsvorhaben geben.

### 3.2 Bereitgestellte Umgebungen



#### 3.2.1 Leistungsbeschränkung bei Verzicht von zusätzlichen Umgebungen

Durch den Verzicht auf eine Qualitätssicherungsumgebung, gemäß Abschnitt 6: Glossar des Teil A dieses SLAs, werden Produktionsausfälle der Fachapplikation, die auf das Einspielen von Updates oder auf Folge von Patches der Betriebssysteme oder Middleware zurückzuführen sind, nicht auf die vereinbarte Zielverfügbarkeit des definierten Services (Servicelevel) angerechnet.

### 3.3 Details zu Server-Services

Alle nachfolgenden Server-Services werden nur mit Betriebssystemen und Middleware bereitgestellt, die sich im offiziellen Herstellersupport befindet. Bei absehbarem Auslaufen des Herstellersupports wird der Auftragsverarbeiter rechtzeitig (regelhaft mit mindestens 24 Monaten Vorlaufzeit) auf den Auftraggeber zum Zweck des Updates der Verfahrensinfrastruktur zukommen.

Der Auftraggeber hat keinen Anspruch auf Weiterbetrieb von Verfahrensinfrastrukturen mit Betriebssystemen oder Middleware, für die kein Herstellersupport mehr besteht.

In den Server-Services ist ohne gesonderte Beauftragung durch den Auftraggeber eine systemtechnische Speicherleistung in ausreichender Größe für das Betriebssystem und die Middleware enthalten.

### **3.3.2 Zentraler Fileservice**

Nicht Bestandteil des SLAs.

### **3.3.3 Fileservice Economy**

Nicht Bestandteil des SLAs.

### **3.3.4 Application Level Gateway-Funktionalität (ALG)**

Webanwendungen im Internet-Data Center (DC) dürfen keine direkten Verbindungen zu Intranet-DCs aufbauen, sondern müssen diese Verbindung über ein ALG aufbauen. Je nach Anwendungsprotokoll (http, xml, soap, proprietäre Protokolle) werden entsprechende Filterregeln auf einem ALG konfiguriert oder (bei komplexeren Protokollen oder zustandsbasierten Prüfungen) eigene Filterprogramme entwickelt und implementiert. Diese speziell angepassten ALGs stellen sicher, dass die dokumentierte Verfahrens-Syntax eingehalten wird. Nichtkonforme Datensätze werden abgewiesen und die Verbindung getrennt.

### **3.3.5 Backup & Recovery**

Programm-, Konfigurations- und Nutzdaten-Dateien, sowie Verfahrensdaten, die in der Windows Registry abgelegt sind, gehören zu den Systemdaten, die durch die Systemsicherung entsprechend zu sichern sind. Diese werden durch den Auftragverarbeiter standardmäßig eingerichtet.

Die Datensicherung sämtlicher Daten, die zur fachlichen Nutzung und für den Betrieb der Verfahren notwendig sind, wird gemäß Anforderung des Auftraggebers eingerichtet.

Grundsätzlich erfolgt für Application Server-, Web Server- und Terminal Server-Services einmal wöchentlich eine Vollsicherung sowie eine tägliche inkrementelle Sicherung.

Bei der Datensicherung des Database Server-Services wird die Wiederherstellung eines täglichen Sicherungsstands gewährleistet. Die Logsicherung erfolgt im Laufe des Dialogbetriebs alle drei Stunden. Für die Zeiträume der Aufbewahrung der Datensicherungen / Wiederherstellbarkeit aus der Datensicherung gelten die in Abschnitt 3.3.1. ausgewählten Daten.

Die gesicherten Daten werden an beiden Standorten des Twin Data Center gesichert.

Im Fehlerfall bzw. auf Anforderung des Auftraggebers erfolgt eine Wiederherstellung der Daten. Die Dauer der Wiederherstellung ist dabei abhängig vom Datenvolumen und der Anzahl der wiederherzustellenden Dateien. Bei großem Umfang kann die Wiederherstellung einen Zeitraum von mehreren Tagen benötigen.

### **3.4 Geteilte Betriebsverantwortung/ Service Fernzugriff Administrativ (SFA)**

Nicht Bestandteil des SLAs.

#### **3.4.1 Mitwirkungsleistungen des Auftraggebers**

Der Auftraggeber sorgt für folgende Rahmenbedingungen:

- Erstellung einer Konzeption für den grundschutz-konformen Fernzugriff. Diese beschreibt u.a. Regelungen zur Protokollierung, (Verfahrens-)Dokumentation und Revisionstätigkeiten
- Personalisierte Accounts im AD des Auftraggebers
- Vertrauensstellung des ADs zum Dataport Rechenzentrum
- Erfolgreiche Sicherheitsüberprüfungen des jeweiligen Mitarbeiters des Auftraggebers
- Protokollierung aller administrativen Tätigkeiten. Die Nachweise sind bei Bedarf an Dataport zu liefern.

*Entfällt bei von Dataport-gemanageten Clients:*

- Nachweis über Maßnahmen zur Clientsicherheit (u.a. angemessener Passwortschutz; aktuelle Betriebssysteme/Virens Scanner und Patchstände)

Der Auftraggeber verpflichtet sich aufgrund der Anforderungen an den BSI-Grundschutz im Falle eines Audits zur Lieferung der entsprechenden Dokumente und dem Erteilen von Auskünften gegenüber dem BSI.

### **3.5 Details zum Technischen Verfahrensmanagement**

#### **3.5.1 Serviceklassifikation**

Für das technische Verfahrensmanagement wird folgende Ausprägung vereinbart:

<b>Spezifikation der Leistungsklasse</b>	
Anzahl Benutzer (named)	
Anzahl Umgebungen	
Anzahl / Art Server	
Anzahl Updates	
Anzahl Schnittstellen	

### 3.5.2 Schnittstellen zu anderen Fachverfahren

Im Rahmen des technischen Verfahrensmanagements werden nachfolgend benannte Schnittstellen zu den einzelnen Umgebungen berücksichtigt:

- **Produktionsumgebung**  
Es existieren folgende Schnittstellen:

■ [REDACTED]

### 3.5.3 Benutzerverwaltung

Die Benutzerverwaltung für die Verfahrensinfrastruktur erfolgt:

- Verfahrensintern

Die Benutzerverwaltung ist nicht Bestandteil dieser Leistungsvereinbarung.

### 3.5.4 Betrieb und Implementierung von Non-Standard Datenbanken

Die im Service Katalog aufgeführten Datenbank Management Systeme (DBMS) bilden den sog. Standard.

Auf Anforderung des Auftraggebers übernimmt der Auftragverarbeiter den Betrieb von Non-Standard Datenbanken. Anwendungskennnisse hält der Auftragverarbeiter nur insoweit vor, wie sie für die Bereitstellung und den Betrieb notwendig sind.

Für Non-Standard Datenbanken werden folgende Leistungen angeboten:

- Installation der Datenbankkomponente und Bereitstellung einer Datenbank
- Patchmanagement
- Sicherheitstechnische Grundeinstellungen
- Störungsbehebungen<sup>1</sup>

### 3.5.5 Zeitlich befristeter und überwachter Fernzugriff

---

<sup>1</sup> Je nach Umfang der Störungsbehebung muss ggf. der Softwarehersteller bzw. ein Dienstleister hinzugezogen werden. Diese Leistungen sind separat zu beauftragen.



Voraussetzung für einen zeitlich befristeten und überwachten Fernzugriff ist eine gesondert getroffene Vereinbarung über Sicherheitsmaßnahmen für den Fernzugriff zwischen dem Auftraggeber und dem externen Dienstleister.

**Ablauf des konkreten Fernzugriffs**

Der jeweilige konkrete Fernzugriff für den externen Dienstleister muss durch einen Mitarbeiter des Auftragsverarbeiters freigeschaltet werden. Der externe Dienstleister muss, bevor er sich an einem System authentisieren kann, Kontakt mit dem Auftragsverarbeiter aufnehmen.

Der Support des externen Dienstleisters des Fachverfahrens wird über einen Fernzugriff realisiert. Hierzu wird ein vom Auftragverarbeiter betriebenes Verfahren folgendermaßen eingesetzt:

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

Nach Durchführung des Fernzugriffs wird die Fernzugriffsberechtigung wieder entzogen.

Der jeweilige administrative Zugriff wird revisionssicher protokolliert. (Die Protokollierung beantwortet folgende Fragen zum Zugriff: wann, warum, wer und was?) Der Auftraggeber kann die Daten im Rahmen seiner Kontrollpflichten beim Auftragsverarbeiter einsehen.



## **4 Leistungsspezifische KPIs und Reporting**

---

Es werden keine Leistungsspezifischen KPIs und Reporting beauftragt.

## **5 Maßnahmen bei Beendigung der Leistung**

---

Es werden zum aktuellen Zeitpunkt keine Maßnahmen bei Beendigung der Leistung definiert.

# **Security Service Level Agreement für Betrieb DIPAS Bremen**

**für**

GeoInformation Bremen  
**Lloydstr. 4**  
**28217 Bremen**

nachfolgend Auftraggeber

## Inhaltsverzeichnis

<b>1.</b>	<b>Einleitung</b> .....	<b>3</b>
1.1	Aufbau des Dokumentes .....	3
1.2	Leistungsgegenstand.....	3
<b>2.</b>	<b>Leistungsumfang und -beschreibung</b> .....	<b>4</b>
2.1	Informationssicherheitsmanagementsystem (ISMS) .....	4
2.2	Verfahrensbezogener IT-Sicherheitskoordinator (ITSK) .....	4
2.3	Grundsatzkonformer Betrieb.....	5
2.4	Erstellung und Pflege der Sicherheitsdokumentation.....	5
2.4.1	Umfang .....	5
2.4.2	Struktur und Standardordner .....	5
2.4.3	Optionale Ordner und Dokumente.....	8
2.5	Gemeinsamer Workshop .....	8
2.6	Bereitstellung .....	9
2.7	Prüfung der Umsetzung .....	9
<b>3.</b>	<b>Abgrenzung der Leistungen</b> .....	<b>10</b>
3.1	Spezifische datenschutzrechtliche Anforderungen .....	10
3.2	Abgrenzung des betrachteten Informationsverbundes.....	10
3.3	Einsicht in interne Dokumente des Auftragnehmers .....	10
3.4	Abweichungen .....	11
3.5	Fortschreibung des IT-Grundschatzes .....	11
3.6	Änderungen im betrachteten Informationsverbund .....	11
<b>4.</b>	<b>Ausgeschlossene Leistungen</b> .....	<b>12</b>
4.1	Geteilte Verantwortung auf Bausteinebene.....	12
4.2	Datenexport .....	12
<b>5.</b>	<b>Leistungsvoraussetzungen</b> .....	<b>13</b>
5.1	Schutzbedarfsfeststellung und Risikoanalyse nach IT-Grundschatz .....	13
5.2	Mitwirkungspflichten des Auftraggebers.....	13
5.3	Vertraulichkeit der Sicherheitsdokumentation, Weitergabe.....	14

## 1. Einleitung

---

Der Auftragnehmer stellt dem Auftraggeber IT-Ressourcen einschließlich Hardware und systemnaher Software sowie IT-Dienstleistungen in definiertem Leistungsumfang zur Verfügung. Die Leistungen, die der Auftragnehmer im Rahmen dieser Vereinbarung erbringt, folgen der Vorgehensweise, die im BSI-Standard 200-1 (Managementsysteme für Informationssicherheit) sowie im BSI-Standard 200-2 (IT-Grundschutz-Vorgehensweise) beschrieben wird.

### 1.1 Aufbau des Dokumentes

Diese Anlage enthält die folgenden Kapitel:

**Leistungsumfang und -beschreibung (Kapitel 2):** Inhaltliche Beschreibung der vom Auftragnehmer bereitgestellten Leistungen.

**Abgrenzung der Leistungen (Kapitel 3):** Inhaltliche Beschreibung der vom Auftragnehmer bereitgestellten Leistungen in Abgrenzung weiterer Leistungen.

**Ausgeschlossenen Leistungen (Kapitel 4):** Inhaltliche Beschreibung der vom Auftragnehmer nicht über diesen SSLA bereitgestellten Leistungen.

**Leistungsvoraussetzungen (Kapitel 5):** Regelung von Rechten und Pflichten von Auftraggeber und Auftragnehmer, Änderung bzw. Kündigung der Vereinbarung sowie Übergangsbestimmungen.

### 1.2 Leistungsgegenstand

Mit dem **Security Service Level Agreement (SSLA)** wird zwischen den Vertragspartnern ergänzend vereinbart, wie der Betrieb unter Informationssicherheitsgesichtspunkten auf Basis des IT-Grundschutzes des Bundesamtes für Informationssicherheit (BSI) unter Nutzung des Sicherheitsmanagementsystems des Auftragnehmers erfolgt. Ferner wird festgelegt, wie die vom Auftragnehmer in dessen Zuständigkeitsbereich getroffenen Sicherheitsanforderungen gegenüber dem Auftraggeber dokumentiert werden.

## 2. Leistungsumfang und -beschreibung

---

### 2.1 Informationssicherheitsmanagementsystem (ISMS)

Der Auftragnehmer betreibt ein Informationssicherheitsmanagementsystem (ISMS) auf Basis des BSI-Standards 200-1<sup>1</sup>. Wesentliche Elemente des ISMS sind:

- die im IT-Sicherheits- und Datenschutzmanagementhandbuch des Auftragnehmers festgelegten und mit denen im Geschäftsverteilungsplan (GVP<sup>2</sup>) dokumentierten Funktionsträger
- die im IT-Sicherheits- und Datenschutzmanagementhandbuch des Auftragnehmers festgelegten Prozesse des Informationssicherheitsmanagements:
  - der Betrieb des ISMS
  - die Umsetzung der Grundschutz-Vorgehensweise auf Grundlage des BSI-Standards 200-2
  - die Sicherheitskonzepterstellung
  - das Sicherheitsvorfallmanagement
  - das Notfall- und Notfallvorsorgemanagement
- sowie das sicherheitsrelevante Regelwerk des Auftragnehmers zur Informationssicherheit

Das ISMS des Auftragnehmers stellt sicher, dass nach dem im BSI-Standard 200-2 festgelegten Schema die einschlägigen Sicherheitsanforderungen der IT-Grundschutz-Kataloge ausgewählt und umgesetzt werden können. Es liefert dem Auftragnehmer die Berücksichtigung relevanter Sicherheitsanforderungen bei Planung, Errichtung und Betrieb von Verfahren des Auftraggebers sowie die Grundlagen für den Nachweis über die aktuell umgesetzten Sicherheitsanforderungen.

### 2.2 Verfahrensbezogener IT-Sicherheitskoordinator (ITSK)

Der Auftragnehmer benennt gegenüber dem Auftraggeber einen IT-Sicherheitskoordinator (ITSK) als Ansprechpartner. Die Benennung des ITSK bzw. die Veränderung der Rollenbesetzung wird dem Auftraggeber angezeigt. Die Benennung wird im Geschäftsverteilungsplan des Auftragnehmers dokumentiert.

Der ITSK steht für die Beantwortung verfahrensbezogener Sicherheitsfragen im Verantwortungsbereich des Auftragnehmers zur Verfügung. Er ist für das verfahrensbezogene Sicherheitsvorfallmanagement beim Auftragnehmer verantwortlich und damit die Schnittstelle des Auftraggebers in die Sicherheitsmanagementorganisation und die Sicherheitsmanagementprozesse des Auftragnehmers.

Der ITSK ist verantwortlich für die Erstellung des auftragsbezogenen Sicherheitskonzeptes sowie die jährliche Bereitstellung des Sicherheitsnachweises<sup>3</sup> (siehe Kapitel 2.4). Er überwacht während der Vertragslaufzeit die Aufrechterhaltung des grundschutzkonformen Betriebes für die vom Auftragnehmer verantwortete, auftragsbezogene Infrastruktur.

---

<sup>1</sup> [https://www.bsi.bund.de/clin\\_165/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards\\_node.html](https://www.bsi.bund.de/clin_165/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html)

<sup>2</sup> Der Geschäftsverteilungsplan als nicht kundenöffentliches Dokument kann entsprechend der Regelungen des Kapitels 3.3 (Einsicht in interne Dokumente des Auftragnehmers) eingesehen werden.

<sup>3</sup> Der Sicherheitsnachweis ist die Dokumentation des Umsetzungsstandes aller relevanten Sicherheitsanforderungen.

Der ITSK ist auf Seiten des Auftragnehmers für die Planung und Koordination von datenschutzrechtlichen Kontrollen des Auftraggebers im Rahmen der Auftragsdatenverarbeitung verantwortlich. Das beinhaltet insbesondere die Abstimmung von Terminen sowie die Sicherstellung der Verfügbarkeit von erforderlichen Personen und Ressourcen (z.B. Räumen oder Dokumenten für die Einsichtnahme vor Ort). Prüfungen wie Audits, Zertifizierungen o.ä. die über eine datenschutzrechtliche Kontrolle hinausgehen, sind nicht Teil der hier vereinbarten Leistung (vgl. Kapitel 2.7).

## 2.3 Grundsatzkonformer Betrieb

Der Auftragnehmer verpflichtet sich, die vom BSI in den IT-Grundsatzkatalogen<sup>4</sup> vorgegebenen BASIS- und STANDARD-Anforderungen, die in den Zuständigkeitsbereich des Auftragnehmers fallen, für den von dieser Vereinbarung betroffenen Informationsverbund umzusetzen.

Die Identifikation und Umsetzung von Sicherheitsanforderungen erfolgt auf Basis der Bausteine der IT-Grundsatzkataloge in der beim Auftragnehmer eingesetzten Fassung und unter Einhaltung der für BSI-Zertifizierungen geltenden Übergangsfristen.

Die für den betrachteten Informationsverbund maßgeblichen Sicherheitsanforderungen und dessen jeweiliger Umsetzungsstand werden im Sicherheitskonzept dokumentiert. Sofern zusätzliche Sicherheitsanforderungen umgesetzt werden müssen, sind diese im SSLA Teil B zu benennen und dessen Umsetzung zu beauftragen.

## 2.4 Erstellung und Pflege der Sicherheitsdokumentation

### 2.4.1 Umfang

Der Auftragnehmer erstellt und pflegt ein in Form und Struktur standardisiertes, grundsatzkonformes Sicherheitskonzept und weist dem Auftraggeber auf dieser Basis den grundsatzkonformen Betrieb nach (Sicherheitsnachweis).

Das Sicherheitskonzept beschreibt die nach IT-Grundsatz-Methodik zusammengefasste Struktur des betrachteten Informationsverbundes sowie die maßgeblichen<sup>5</sup> Sicherheitsanforderungen im Zuständigkeitsbereich des Auftragnehmers.

Der Auftragnehmer stellt die dauerhafte Umsetzung der Sicherheitsanforderungen sicher. Zu diesem Zweck prüft regelmäßig den Umsetzungsstand der Sicherheitsanforderungen und dokumentiert diesen im Sicherheitsnachweis.

Die Betrachtung und Prüfung von Sachverhalten im Verantwortungsbereich des Auftraggebers, die über die Leistungen nach Kapitel 2.5 hinausgehen, sind nicht Gegenstand der Leistungsvereinbarung.

### 2.4.2 Struktur und Standardordner

---

<sup>4</sup> Die aktuelle Version der IT-Grundsatz-Kataloge kann beim BSI abgerufen werden ([www.bsi.bund.de](http://www.bsi.bund.de)).

<sup>5</sup> Die Festlegung der relevanten Sicherheitsanforderungen erfolgt auf Grundlage der Modellierungsvorschriften des BSI-Standards 200-2.

Die Sicherheitsdokumentation wird strukturiert in verschiedenen Unterordnern übergeben. Die Struktur sowie das Namensschema der Ordner orientieren sich dabei an den Vorgaben des BSI, insbesondere der im BSI-Standard 200-2 festgelegten Vorgehensweise. Der Inhalt der jeweiligen Ordner ist in den nachfolgenden Kapiteln 2.4.2.1 bis 2.4.2.6 näher erläutert. Eine detaillierte Beschreibung der einzelnen Ordner einschließlich der Inhalte liegt ferner der übergebenen Sicherheitsdokumentation bei.

Je nach technischen und betrieblichen Rahmenbedingungen, insbesondere in Abhängigkeit des im SLA vereinbarten Leistungsschnitts, kann der Dokumentationsumfang (beispielsweise im Ordner "A.D1 Begleitdokumentation") variieren.

#### **2.4.2.1 A.0 Richtlinien für Informationssicherheit**

Die Rahmenbedingungen zur Umsetzung des grundschutzkonformen Betriebes beim Auftragnehmer sind in dem jeweils geltenden Regelwerk des Auftragnehmers festgelegt. Der Auftragnehmer stellt dem Auftraggeber das Regelwerk auf der Ebene der Leitlinien und Richtlinien als Teil der Sicherheitsdokumentation für die interne Bewertung zur Verfügung.

Betriebliche Detaildokumentation, die über die Ebene der Richtlinien hinausgeht (wie beispielsweise detaillierte physikalische Netzpläne, IP-Adresskonzepte, Firewall-Policies oder spezifische sicherheitsrelevante Konfigurationsvorgaben) hält der Auftragnehmer vor Ort zur Einsichtnahme durch den Auftraggeber bereit.

#### **2.4.2.2 A.1 IT-Strukturanalyse**

Der Auftragnehmer erstellt eine standardisierte Übersicht über die zu dem betrachteten Verfahren gehörige IT-Infrastruktur. Diese beinhaltet:

- Beschreibung des betrachteten IT-Verbundes sowie dessen Abgrenzung
- Dokumentation zu Aufbau und Leistungen des Informationssicherheitsmanagementsystems (ISMS)
- Übersicht über die relevanten Kommunikationsverbindungen
- Komponentenlisten zu den jeweils betroffenen Komponenten beim Auftragnehmer
  - Gebäude und Räume
  - Server und Netzwerkkomponenten
  - Systeme, die dem Verfahrensbetrieb dienen einschl. unmittelbar genutzter Managementsysteme für den Systembetrieb, die Netzinfrastruktur und administrative Clients
  - Übersicht über am Verfahren beteiligte Dataport-Administratoren und deren Clients
  - ergänzende Zielobjekte wie Anwendungen und Dienste, sofern sie in den eingesetzten IT-Grundschutz-Katalogen betrachtet und vom Auftragnehmer bereitgestellt werden
- Übersicht über die beteiligten Netze (verdichtete Netzpläne in der IT-Grundschutzsystematik)
- Beschreibung der Administratorrollen

Sofern für die Betrachtung relevante Teile bereits in anderen Sicherheitskonzepten vollständig betrachtet wurden (beispielsweise das der IT-Grundschutzzertifizierung unterliegende Sicherheitskonzept des Rechenzentrums), werden diese Teilkonzepte beigefügt, mindestens jedoch darauf verwiesen (siehe 2.4.2.5 A.D0 Ergänzende Sicherheitskonzepte).

#### **2.4.2.3 A.3 Modellierung des IT-Verbundes**

Der Auftragnehmer weist in Form eines Reports aus der eingesetzten Verwaltungssoftware nach, welche Bausteine des IT-Grundschutz-Katalogs auf die Objekte des Informationsverbundes des Auftragnehmers angewendet werden. Die Bausteine beinhalten eine vom BSI vorgegebene Auswahl betrachteter Gefährdungslagen (Risiken) und festgelegter Sicherheitsanforderungen.

Die Zuweisung der Bausteine erfolgt nach den in den IT-Grundschutz-Katalogen beschriebenen Regeln.

#### **2.4.2.4 A.4 Grundschutzerhebung (Sicherheitsnachweis)**

In Form eines Reports aus der Verwaltungssoftware weist der Auftragnehmer den Umsetzungsstand der sich aus der Modellierung ergebenden Sicherheitsanforderungen nach (Sicherheitsnachweis). Dabei folgt die Dokumentation des Umsetzungsstandes dem vom BSI vorgegebenen Schema in fünf Stufen:

- Ja (Sicherheitsanforderungen ist vollständig umgesetzt)
- Teilweise (Sicherheitsanforderungen ist teilweise umgesetzt)
- Nein (Sicherheitsanforderungen ist nicht umgesetzt)
- Entbehrlich (Sicherheitsanforderungen /Baustein wird als nicht relevant bewertet)
- Unbearbeitet

Der Report beinhaltet Angaben zur Durchführung der Prüfung (Datum, Personen), eine Beschreibung der Umsetzung, Verweise zum jeweils maßgeblichen Regelwerk des Auftragnehmers sowie bei Abweichungen eine Beschreibung der Abweichungen von IT-Grundschutz sowie den Umgang mit den festgestellten Abweichungen (vgl. auch Kapitel 3.4).

#### **2.4.2.5 A.D0 Ergänzende Sicherheitskonzepte**

Sofern für den unter dieser Vereinbarung betrachteten Informationsverbund weitere Sicherheitskonzepte maßgeblich sind, werden diese in diesem Ordner beigelegt.<sup>6</sup>

Teil-Sicherheitskonzepte, bei denen die verantwortliche Stelle nicht identisch mit dem hier relevanten Auftraggeber ist, können ohne Zustimmung der jeweils verantwortlichen Stelle nicht herausgegeben werden. Liegt dem Auftragnehmer eine entsprechende Freigabe vor, werden diese Teil-Sicherheitskonzepte der Sicherheitsdokumentation im Ordner A.D0 beigelegt.

#### **2.4.2.6 A.D1 Begleitdokumentation**

Sofern für das vom Auftragnehmer erstellte Sicherheitskonzept weitere Dokumente zum Verständnis oder zum Nachweis der Umsetzung erforderlich sind, werden diese in die Sicherheitsdokumentation (Ordner A.D1) aufgenommen.

Dokumente, die als intern bzw. nicht kundenöffentlich eingestuft sind, stehen nur zur Einsichtnahme bereit.

---

<sup>6</sup> Für Verfahren, die mindestens in Teilen im Twin Data Center (TDC) betrieben werden, ist dies das der BSI-Zertifizierung unterliegende Sicherheitskonzept des Rechenzentrums.

## **2.4.3 Optionale Ordner und Dokumente**

### **2.4.3.1 A.2 Schutzbedarfsfeststellung**

Bei der Schutzbedarfsfeststellung nach BSI-Standard 200-2 handelt es sich um eine Mitwirkungsleistung des Auftraggebers (vgl. Kapitel 5.1). Sofern der Auftraggeber das Ergebnis der Schutzbedarfsfeststellung bereitstellt, wird dieses in die Sicherheitsdokumentation des Auftragnehmers aufgenommen.

### **2.4.3.2 A.5 Risikoanalyse**

Bei der ergänzenden Sicherheits- und Risikoanalyse nach BSI-Standard 200-3 handelt es sich um eine Mitwirkungsleistung des Auftraggebers (vgl. Kapitel 5.1). Sofern der Auftraggeber die Ergebnisse der ergänzenden Sicherheits- und Risikoanalyse bereitstellt, werden diese in die Sicherheitsdokumentation des Auftragnehmers aufgenommen.

Die Bereitstellung der Ergebnisse der Risikoanalyse ersetzt jedoch nicht die konkrete Beauftragung von zusätzlichen Sicherheitsanforderungen (z.B. im Rahmen des SSLA Teil B).

### **2.4.3.3 A.6 Risikobehandlung**

Nicht oder nicht vollständig umgesetzte Sicherheitsanforderungen des betrachteten Informationsverbundes werden im Rahmen der Sicherheitschecks dokumentiert und dem Auftraggeber zur Verfügung gestellt. Sofern z.B. für Zwecke der Zertifizierung ein separater Risikobehandlungsplan erforderlich ist, werden nicht vollständig umgesetzte Sicherheitsanforderungen sowie ggf. ergänzende Informationen zur Risikobewertung und Behandlung auf Wunsch des Auftraggebers separat ausgewiesen.

## **2.5 Gemeinsamer Workshop**

Der Auftragnehmer führt mit dem Auftraggeber einen gemeinsamen Workshop zur Sicherheitsbetrachtung der für den Informationsverbund maßgeblichen Fachanwendung durch. Gegenstand des Workshops ist die Durchführung von Sicherheitschecks für den oder die maßgeblichen Anwendungsbau- steine (wie Allgemeine Anwendung, Webanwendung oder WebServices).

Sofern weitere Bausteine eine gemeinsame Betrachtung erfordern, werden diese in diesem Workshop behandelt (siehe Kapitel 4.1 Geteilte Verantwortung auf Bausteinebene). Kommt keine Fachanwendung zum Einsatz (z.B. bei einem reinen Infrastrukturbetrieb) kann der Workshop entbehrlich sein.

Die Dokumentation der Ergebnisse erfolgt in der Verwaltungssoftware des Auftragnehmers und wird im Rahmen des Sicherheitsnachweises (Ordner A.4) in die übergebene Sicherheitsdokumentation aufgenommen.

Die Planung und Durchführung des Workshops erfolgt unter Beachtung der Verfügbarkeit des erforderlichen Personals des Auftraggebers und des Auftragnehmers.

Lehnt der Auftraggeber die Teilnahme an dem Workshop ab, werden Sicherheitsanforderungen in seinem Verantwortungsbereich im Sicherheitskonzept des Auftragnehmers als entbehrlich dokumentiert.

## 2.6 Bereitstellung

Der Auftraggeber erhält jährlich eine Aktualisierung des Sicherheitsnachweises (vgl. Kapitel 2.4). Gleichzeitig erfolgt die Aufnahme in das Sicherheitskonzept des betroffenen Informationsverbundes.

Die erstellte bzw. aktualisierte Sicherheitsdokumentation wird in elektronischer Form zur Verfügung gestellt. Eine davon abweichende Übergabeform kann zwischen den Vertragsparteien formlos vereinbart werden.

## 2.7 Prüfung der Umsetzung

Der Auftragnehmer ermöglicht dem Auftraggeber die Prüfung von Angemessenheit, Wirksamkeit und Umsetzungsstand des Sicherheitskonzeptes nach IT-Grundschutz-Vorgehensweise. Dies beinhaltet die Beantwortung von Fragen zur übergebenen Dokumentation durch den ITSK sowie die Überprüfung des Regelwerkes und der Umsetzung der Sicherheitsanforderungen vor Ort beim Auftragnehmer.

Die Koordination einer Überprüfung erfolgt auf Seiten des Auftragnehmers durch den benannten ITSK. Die Durchführung von Prüfungen ist vom Auftraggeber mit angemessenem Vorlauf anzukündigen, um den entsprechenden Personal- bzw. Ressourcenbedarf einplanen und einen reibungslosen Ablauf der Kontrolle gewährleisten zu können. Sofern die Prüfung der Umsetzung durch den Auftraggeber einen jährlichen Aufwand von 16 Stunden beim Auftragnehmer überschreitet, ist diese Leistung gesondert zu beauftragen.

Prüfungen wie Audits, Zertifizierungen o.ä., die durch Dritte durchgeführt werden und die über eine datenschutzrechtliche Kontrolle der Auftragsdatenverarbeitung hinausgehen, sind nicht Leistungsgegenstand dieser Vereinbarung und gesondert zu beauftragen.

### **3. Abgrenzung der Leistungen**

---

#### **3.1 Spezifische datenschutzrechtliche Anforderungen**

Der mit dem SSLA vereinbarte IT-Grundsatzkonforme Betrieb behandelt die Grundwerte der Informationssicherheit (Vertraulichkeit, Verfügbarkeit, Integrität). Der unter Kapitel 2 aufgeführte Leistungsumfang ist grundsätzlich geeignet, die Sicherheitsanforderungen sowie ihren Umsetzungsstand in geeigneter Form nachzuweisen und damit einen wesentlichen Beitrag zur Erfüllung datenschutzrechtlicher Anforderungen zu leisten. Der alleinige Abschluss des SSLAs ist jedoch nicht ausreichend, um alle datenschutzrechtlichen Verpflichtungen des Verantwortlichen (des Auftraggebers) zu erfüllen. Abdeckungslücken können sich insbesondere aus spezifischen datenschutzrechtlichen Dokumentations- und Meldepflichten sowie der Gewährleistung der Grundsätze für die Verarbeitung personenbezogener Daten, wie z. B. der Datenminimierung und der Zweckbindung, ergeben.

Die Umsetzungsverantwortung dafür liegt beim Verantwortlichen und geht im Zuge der Auftragsverarbeitung nicht auf den Auftragsverarbeiter (Auftragnehmer) über. Besondere Sicherheits- oder Dokumentationsanforderungen, die sich aus solchen spezifisch datenschutzrechtlichen Anforderungen ergeben, sind - soweit nicht an anderer Stelle im EVB-IT-Vertrag berücksichtigt - gesondert zu beauftragen.

#### **3.2 Abgrenzung des betrachteten Informationsverbundes**

Der im Rahmen der Sicherheitskonzepterstellung betrachtete Informationsverbund umfasst ausschließlich Komponenten, die im Verantwortungsbereich des Auftragnehmers liegen. Die unter Kapitel 5 (Leistungsvoraussetzungen) aufgeführten und vom Auftragnehmer zu erbringenden Leistungen stellen dann aus Sicht des Auftraggebers unter Umständen kein vollständiges, IT-Grundsatzkonformes Sicherheitskonzept des betreffenden Verfahrens dar.

Die Umsetzung von Sicherheitsanforderungen kann nur dann zugesichert und geeignet nachgewiesen werden, wenn die jeweilige Umsetzungsverantwortung ausschließlich beim Auftragnehmer liegt (siehe hierzu Kapitel 5 Leistungsvoraussetzungen sowie 4.1 Geteilte Verantwortung auf Bausteinebene).

Verfahrenskomponenten des Auftraggebers, die auf Basis anderer vertraglicher Vereinbarungen betrieben oder sicherheitstechnisch betrachtet werden, sind von dem betrachteten Informationsverbund abgegrenzt und daher nicht Teil des hier betrachteten Informationsverbundes.

#### **3.3 Einsicht in interne Dokumente des Auftragnehmers**

Interne Dokumente des Auftragnehmers wie z.B. der Geschäftsverteilungsplan oder die detaillierte Umsetzungsdokumentation konkreter technischer Sicherheitsanforderungen sind nicht Teil des übergebenen Sicherheitskonzeptes. Diese als nicht kundenöffentlich bezeichneten Dokumente können jedoch in Rücksprache vor Ort, in Begleitung des ITSK oder eines Vertreters des Sicherheitsmanagements des Auftragnehmers, eingesehen werden.

### 3.4 Abweichungen

Im laufenden Betrieb können temporäre Abweichungen zwischen der Dokumentation des Umsetzungsstandes und der tatsächlichen Umsetzung einzelner Sicherheitsanforderungen auftreten. Die Ursachen für temporäre Abweichungen können in der Änderung der IT-Infrastruktur oder durch neue oder veränderte IT-Grundschutzanforderungen (z.B. Fortschreibung oder Veränderung der BSI-Standards) verursacht werden.

Werden im Rahmen der Durchführung von Sicherheitschecks solche Abweichungen festgestellt, werden diese im Sicherheitsnachweis dokumentiert (vgl. 2.4.2.4). Der ITSK koordiniert die Umsetzung von Sicherheitsanforderungen mit den jeweils verantwortlichen Fachbereichen.

Nicht oder nicht vollständig umgesetzte Sicherheitsanforderungen, die im Rahmen der regelmäßigen Prüfung durch Prüfungen identifiziert wurden, werden in der beim Auftragnehmer eingesetzten Verwaltungssoftware dokumentiert. Diese Dokumentation umfasst:

- eine Beschreibung der Abweichung
- geplante und erforderliche Aktivitäten zur vollständigen Umsetzung von Sicherheitsanforderungen
- ein Zieldatum, bis zu dem die Umsetzung abgeschlossen werden soll

Unter Einhaltung dieser Regelungen stellt eine solche temporäre Abweichung keinen Leistungsmangel dar.

Sofern es sich bei einer Abweichung um eine dauerhafte Abweichung handelt, wird diese unter Einbeziehung des Auftraggebers durch den Auftragnehmer bewertet und im Risikobehandlungsplan gesondert ausgewiesen (vgl. 2.4.2.4 sowie 2.4.3.3).

### 3.5 Fortschreibung des IT-Grundschutzes

Der IT-Grundschutz des Bundesamtes für Informationssicherheit unterliegt der ständigen Fortschreibung. Hieraus kann sich z.B. bei wesentlichen Neuerungen oder Änderungen der IT-Grundschutzstandards (z.B. neue oder geänderte Sicherheitsanforderungen) eine Veränderung des Leistungsumfanges ergeben.

Zusätzliche Aufwände, die sich aus einer solchen Veränderung ergeben, sind nicht Teil dieser Vereinbarung. Der ITSK informiert den Auftraggeber über derartige Änderungen und stimmt das weitere Vorgehen insbesondere den Umgang diesen Änderungen ab.

### 3.6 Änderungen im betrachteten Informationsverbund

Änderungen an der unter dieser Vereinbarung betrachteten Infrastruktur können eine Anpassung des Sicherheitskonzeptes erfordern, welche über die bloße Aktualisierung des Sicherheitsnachweises (A.4) hinausgeht. Dies kann beispielsweise der Fall sein, wenn die für die Sicherheitsbetrachtung maßgebliche Verfahrensinfrastruktur aus- oder umgebaut wird. Sofern diese Änderungen durch den Auftraggeber veranlasst werden, sind die gegebenenfalls erforderlichen Zusatzaufwände zur Aktualisierung der Sicherheitsdokumentation gesondert zu beauftragen.

## 4. Ausgeschlossene Leistungen

---

Folgende für ein nach BSI-Standard 200-2 vollständiges Sicherheitskonzept erforderliche Leistungen sind nicht Teil der vorliegenden Vereinbarung:

1. Durchführung der Schutzbedarfsfeststellung
2. Durchführung der ergänzenden Sicherheits- und Risikoanalyse nach BSI-Standard 200-3
3. Umsetzung zusätzlicher, über den Schutzbedarf "Normal" hinausgehende Sicherheitsanforderungen
4. Berücksichtigung übergeordneter Regelungen beim Auftraggeber
5. Erfassung der zum Informationsverbund gehörenden Geschäftsprozesse des Auftraggebers
6. Dokumentation und Umsetzung spezifischer Datenschutz- und Sicherheitsanforderungen des Auftraggebers (wie etwa an das Datensicherungskonzept oder das Notfallvorsorgekonzept gem. IT-Grundschutz)
7. Prüfung auf Eignung von Sicherheitsfunktionen in der von Dritten bereitgestellten Fachanwendung(en)/Fachanwendungssoftware oder Infrastrukturkomponenten

Sofern der Auftraggeber die Erbringung dieser Leistungen durch den Auftragnehmer wünscht, müssen diese gesondert beauftragt werden (z.B. im Rahmen eines SSLA Teil B).

### 4.1 Geteilte Verantwortung auf Bausteinebene

In den beim Auftragnehmer modellierten IT-Grundschutz-Bausteinen können sich Sicherheitsanforderungen befinden, für die die Umsetzungsverantwortung beim Auftraggeber liegt<sup>7</sup>. Sofern die Umsetzung dieser Anforderungen beim Auftragnehmer nicht beauftragt wurde, werden diese Sicherheitsanforderungen als "entbehrlich" dokumentiert. Erfolgt die Prüfung der Umsetzung in einem gemeinsamen Workshop (vgl. Kapitel 2.4.2), wird der Umsetzungsstand in der Verwaltungssoftware des Auftragnehmers dokumentiert.

### 4.2 Datenexport

Ein Datenexport aus der beim Auftragnehmer eingesetzten Verwaltungssoftware, der über die bereitgestellten Reports als Teil der Sicherheitsdokumentation hinausgeht, ist nicht Bestandteil der zu erbringenden Leistungen. Sofern auf Nachfrage ein Datenexport durch den Auftragnehmer erbracht wird, besteht jedoch kein Anspruch auf die Verwendung einer spezifischen Verwaltungssoftware oder einer spezifischen Softwareversion.

---

<sup>7</sup> Bausteine die einer "geteilten" Verantwortung unterliegen, finden sich insbesondere auf Schicht der Anwendungen wieder (beispielsweise Anforderungen an Freigabeprozesse für Patches der Fachanwendung, Einrichtung eines Internet-Redaktionsteams, Freigabe von Webseiteninhalten bei Webservern, Anforderungen an die Beschaffung, Anforderungen an den sicherheitsbezogenen Leistungsumfang einer Anwendungssoftware etc.)

## 5. Leistungsvoraussetzungen

---

### 5.1 Schutzbedarfsfeststellung und Risikoanalyse nach IT-Grundschutz

Die Festlegung des Schutzbedarfes erfolgt durch den Auftraggeber. Bei festgestelltem erhöhten Schutzbedarf oder besonderen Sicherheitsanforderungen ist durch den Auftraggeber eine ergänzende Sicherheitsanalyse sowie bei Bedarf eine Risikoanalyse nach BSI-Standard 200-3 durchzuführen. Die ergänzende Risikoanalyse dient der Identifikation erhöhter Risiken sowie geeigneter Sicherheitsanforderungen zur Risikobehandlung.

Sofern diese zusätzlichen Sicherheitsanforderungen zu den bereits im Kapitel 2 (Leistungsumfang und -beschreibung) und im Verantwortungsbereich des Auftragnehmers umzusetzen sind, ist die gesonderte Beauftragung dieser Sicherheitsanforderungen erforderlich. Die Beauftragung dieser zusätzlichen Sicherheitsanforderungen erfolgt gesondert im SSLA Teil B.

Legt der Auftraggeber keinen Schutzbedarf fest oder werden keine zusätzlichen Sicherheitsanforderungen beauftragt, wird für die Erstellung des Sicherheitskonzeptes vom Schutzbedarf Normal ausgegangen (Umsetzung der für diesen Schutzbedarf maßgeblichen Sicherheitsanforderungen).

Sicherheitsanforderungen, die bereits im Standardleistungsumfang enthalten sind, bedürfen keiner gesonderten Beauftragung.

### 5.2 Mitwirkungspflichten des Auftraggebers

Für ein vollständiges IT-Grundschutz-konformes Sicherheitskonzept und den durchgängigen IT-Grundschutzkonformen Betrieb des gesamten Informationsverbundes ist die Betrachtung aller relevanten Verfahrensteile erforderlich. Der Auftragnehmer kann Grundschutzkonformität jedoch nur für die von ihm verantworteten Komponenten sicherstellen. Sicherheitsanforderungen, die im Verantwortungsbereich des Auftraggebers liegen, sind durch diesen selbst umzusetzen.

Bei der Planung und Umsetzung von Sicherheitsanforderungen durch den Auftragnehmer sind zum Teil weitergehende Informationen, Regelungen, Dokumente und/oder Leistungen durch den Auftraggeber oder auch durch Dritte beizusteuern (z.B. Hersteller der zu betreibenden Software/Komponenten). Diese Mitwirkung ist zur Gewährleistung des grundschutzkonformen Betriebes im Verantwortungsbereich des Auftragnehmers erforderlich.

Die Mitwirkung ist insbesondere bei folgenden Leistungen für den Auftraggeber verpflichtend:

- 1) Benennung eines Ansprechpartners beim Auftraggeber für die:
  - a) Klärung sicherheitsrelevanter, verfahrensspezifischer Fragestellungen
  - b) Klärung / Zulieferung von anwendungsspezifischen Angaben
  - c) Unterstützung bei der Erstellung eines verfahrensspezifischen Notfallkonzeptes
  - d) Etablierung von Prozessschnittstellen für das Sicherheitsvorfall- und Notfallmanagement

- 2) Risikobewertung<sup>8</sup> bei der Erweiterung des betrachteten IT-Verbundes um fachliche oder technische Komponenten oder der Erweiterung um Kommunikationsschnittstellen, insbesondere zu Verfahren mit niedrigerem Sicherheitsniveau<sup>9</sup>
- 3) Bereitstellung von relevanten anwendungs- bzw. verfahrensspezifischen Informationen/Dokumentationen/Konzepten wie beispielsweise:
  - a) Berechtigungskonzept (Rollen- und Rechtenkonzept)
  - b) Protokollierungskonzept (bspw. für die zu betreibende Fachanwendung)
  - c) Mandantenkonzept
  - d) Schnittstellenkonzept
  - e) Installations- und Betriebshandbuch bzw. Betriebsvorgaben des Herstellers
  - f) Dokumentation von Sicherheitsfunktionen in relevanten Softwareprodukten
- 4) Bereitstellung und Freigabe von Sicherheitsupdates, Patches und hierfür notwendiger Installationsdokumentation für die betreffende Fachanwendung (einschließlich der erforderlichen Middleware) oder Infrastrukturkomponenten

Die Mitwirkungsleistungen sind unter Umständen durch Dritte zu erbringen, mit denen der Auftragnehmer keine Vereinbarung über den Bezug dieser Leistungen geschlossen hat (z.B. Hersteller der Verfahrensssoftware). Der Auftraggeber ist dafür verantwortlich, die Beistellung relevanter Leistungen oder Informationen durch geeignete vertragliche Regelungen zu gewährleisten.

Im Rahmen der Sicherheitskonzepterstellung können sich in Abhängigkeit zur verwendeten Verfahrensinfrastruktur weitere Mitwirkungsleistungen für spezifische Sicherheitsanforderungen ergeben. Der Auftragnehmer teilt diese dem Auftraggeber bei Kenntniserlangung unverzüglich mit.

### 5.3 Vertraulichkeit der Sicherheitsdokumentation, Weitergabe

Die Parteien verpflichten sich, die im Rahmen des SSLAs ausgetauschten Informationen, wie beispielsweise sicherheitsbezogene Dokumentationen, Konzepte, Konfigurationsanleitungen, Softwarematerialien oder Daten, unabhängig von der Art der Bereitstellung als ihr anvertraute Betriebsgeheimnisse streng vertraulich zu behandeln und Dritten gegenüber geheim zu halten.

Durch die jeweils entgegennehmende Partei wird sichergestellt, dass sämtliche Mitarbeiter und Mitarbeiterinnen, denen die Informationen zugänglich gemacht werden müssen, der Geheimhaltung im gleichen und im gesetzlich möglichen Rahmen unterworfen werden.

Für die Weitergabe an Dritte (z.B. externe Berater, andere Auftragnehmer etc.) gelten die gleichen Vorgaben. Die Weitergabe an Dritte bedarf immer der Zustimmung der jeweils anderen Partei.

---

<sup>8</sup> ggf. schließt das auch die Aktualisierung der Risikoanalyse nach BSI-Standard 200-3 mit ein

<sup>9</sup> z.B. zu Verfahren, die nicht IT-Grundschutzkonform betrieben werden