

## Vertrag über die Beschaffung von IT-Dienstleistungen

Zwischen

**Der Senator für Finanzen  
Abteilung 4 - Zentrales IT-Management  
Digitalisierung öffentlicher Dienste  
Rudolf-Hilferding-Platz 1  
28195 Bremen**

– im Folgenden „Auftraggeber“ (AG) genannt –

und

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

– im Folgenden „Auftragnehmer“ (AN) genannt –

wird folgender Vertrag geschlossen:

### 1 Vertragsgegenstand und Vergütung

#### 1.1 Projekt-/Vertragsbezeichnung

Alt: Verfahrensinfrastruktur für das Verfahren Antrags- und Fallmanagement (AFM) im Rechenzentrum sowie Fachliches Verfahrensmanagement, dSecureCloud und „Integrierter Dataport Oracle Service“ (IDOS) - zentrale Nutzung

Neu: Antrags- und Fallmanagement ( AFM): Verfahrensinfrastruktur für das Verfahren im Rechenzentrum sowie Fachliches Verfahrensmanagement, dSecureCloud und „Integrierter Dataport Oracle Service“ (IDOS) - zentrale Nutzung - (bis 31.12.2023)

3. Änderung: Neue Infrastruktur

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 vereinbarten Vergütungen verstehen sich zuzüglich der gesetzlichen Umsatzsteuer, soweit Umsatzsteuerpflicht besteht.

### 2 Vertragsbestandteile

2.1 Es gelten nacheinander als Vertragsbestandteile:

- dieses Vertragsformular (Seiten 1 bis 8)
- Allgemeine Vertragsbedingungen von Dataport (Dataport AVB) in der jeweils geltenden Fassung (siehe Nr. 11.1)
- Vertragsanlage(n) Nr. 1, 2a, 2b, 2c, 2d, 2e, 2f, 3, 4a, 4b, 4c, 5, 6, 7, 8a, 8b, 8c und 9 (die Reihenfolge der Anlagen ergibt sich aus Nr. 3.2.1)

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

Vertragsnummer/Kennung Auftragnehmer V15385-3/3011005

- 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.

### 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:  
gem. Anlagen 4a, 4b, 4c, 5, 6, 7, 8a, 8b, 8c

#### 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 Antrags- und Fallmanagement (AFM_ML001) (SLA VI B1)	Anlage(n) Nr.	4b
Service Level Agreement Verfahrensinfrastruktur im Dataport Rechenzentrum Teil B (spezifischer Teil für Verfahren AFM ML (AFM_ML002) (SLA VI B2)	Anlage(n) Nr.	4c
Service Level Agreement Fachliches Verfahrensmanagement zum IT-Verfahren Antrags- und Fallmanagement (SLA FVM)	Anlage(n) Nr.	5
Leistungsbeschreibung -Migration der Online-Dienste auf die neue AFM Infrastruktur - (LB)	Anlage(n) Nr.	6
Service Level Agreement Bereitstellung von Systemen in der dSecureCloud - IaaS (SLA dSecureCloud)	Anlage(n) Nr.	7
Security Service Level Agreement für Verfahrensbetrieb Antrags- und Fallmanagement (SSLA A)	Anlage(n) Nr.	8a
Security Service Level Agreement - Teil B Verfahrensbetrieb Antrags- und Fallmanagement (AFM_ML001) (SSLA B1)	Anlage(n) Nr.	8b
Security Service Level Agreement - Teil B Verfahrensbetrieb Antrags- und Fallmanagement (AFM_ML002) (SSLA B2)	Anlage(n) Nr.	8c



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

Vertragsnummer/Kennung Auftragnehmer V15385-3/3011005

folgenden weiteren Dokumenten:

Ansprechpartner	Anlage(n) Nr.	1
Preisblatt Aufwände	Anlage(n) Nr.	2a
Preisblatt Aufwände	Anlage(n) Nr.	2b
Preisblatt Aufwände	Anlage(n) Nr.	2c
Preisblatt einmaliger Festpreis	Anlage(n) Nr.	2d
Preisblatt jährlicher Festpreise bis 31.12.2023	Anlage(n) Nr.	2e
Preisblatt jährlicher Festpreise ab 01.04.2023	Anlage(n) Nr.	2f
Datenschutzrechtliche Festlegung des Auftraggebers	Anlage(n) Nr.	3
Muster Leistungsnachweis Dienstleistung	Anlage(n) Nr.	9

Es gelten die Dokumente in

obiger Reihenfolge

folgender Reihenfolge: 1, 2a, 2b, 2c, 2d, 2e, 2f, 3, 4b, 4c, 4a, 5, 6, 7, 8b, 8c, 8a, 9

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):

Oracle Leistungen: gemäß Zentralfinanzierung des Vertrages V12909-2/ 3011183

Vertragsnummer/Kennung Auftraggeber \_\_\_\_\_  
 Vertragsnummer/Kennung Auftragnehmer V15385-3/3011005

- 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** Beim Auftragnehmer

**4.2 Zeiträume der Dienstleistungen**

Leistungen (gemäß Nummer 3.1)	Geplanter Leistungszeitraum		Verbindlicher Leistungszeitraum	
	Beginn	Ende	Beginn	Ende
V15385/3011182			01.10.2020	31.03.2021
V15385-2/3011182			01.09.2022	31.08.2023
V18385-1/3011182			01.04.2021	31.08.2022
V15385-3/3011005 gem. Nr. 3.1.8			01.04.2023	
IDOS			01.04.2023	31.12.2023

**4.3 Zeiten der Dienstleistungen**

Die Leistungen des Auftragnehmers werden erbracht gem. VI A Pkt. 2.2.2, SLA VI B1 Pkt. 2.1.1, SLA VI B2 Pkt. 2.1.1, SLA FVM Pkt. 10.2 und SLA dSecureCloud Pkt. 2.1.5

**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 - 2c, 2d - 2f und Leistungsnachweis Dienstleistung**

**5.1**  Vergütung nach Aufwand

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 - 2c enthalten.

**Reisezeiten**

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

**Rechnungsstellung**

Die Rechnungsstellung erfolgt gemäß Anlage 2a - 2c.



## Vergütungsvorbehalt

Es wird ein Vergütungsvorbehalt vereinbart

- gemäß Ziffer 6.4 EVB-IT Dienstleistung
- gemäß Ziffer 3.1 der Dataport AVB
- anderweitige Regelung gemäß Anlage Nr.

## 5.2 Festpreis

Der einmalige und der jährliche Festpreis setzen sich gemäß Anlage 2d - 2f zusammen.

Die Rechnungsstellung des einmaligen und des jährlichen Festpreises erfolgt gemäß Anlage 2d - 2f.

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

- Es werden folgende Abschlagszahlungen vereinbart: gemäß Anlage 2d - 2f

## 5.3 Reisekosten und Nebenkosten

- Reisekosten werden nicht gesondert vergütet
- Reisekosten werden vergütet gemäß Anlage 2a - 2c
- 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 Gem. Anlagen SLA VI A Pkt. 1.2, SLA VI B1 Pkt. 1.4, SLA VI B2 Pkt. 1.4, SLA FVM Pkt. 3.1, LB Pkt. 3.1, SLA dSecureCloud Pkt. 2.3, SSLA A Pkt. 5.2, SSLA B1 Pkt. 4 und SSLA B2 Pkt. 4

8.4 Folgende weitere Beistelleistungen werden vereinbart

- Softwarelizenzen gemäß
- Hardware gemäß
- Dokumente gemäß
- sonstiges gemäß

## 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

#### 11.2.1 Umsatzsteuer für Leistungen, die bis zum 31.12.2024 erbracht werden

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, gegebenenfalls auch rückwirkend.

#### 11.2.2 Umsatzsteuer für Leistungen, die ab dem 01.01.2025 erbracht werden

Die aus diesem Vertrag seitens des Auftragnehmers zu erbringenden Leistungen unterliegen nicht der Umsatzsteuer, da diese aufgrund des Gesetzes zur Gewährleistung der digitalen Souveränität der Freien Hansestadt Bremen nur von juristischen Personen des öffentlichen Rechts erbracht werden dürfen (§ 2b Abs. 3 Nr. 1 UStG). Ausgenommen sind Leistungen auf dem Gebiet des Telekommunikationswesens (§ 2b Abs. 4 Nr. 5 UStG in Verbindung mit Anhang 1 Nr. 1 der RL 2006/112 EG vom 28.11.2006) sowie die Lieferung von neuen



Gegenständen, insbesondere Hardware (§ 2b Abs. 4 Nr. 5 UStG in Verbindung mit Anhang 1 Nr. 6 der RL 2006/112 EG vom 28.11.2006), die stets steuerbar und –pflichtig sind.

Bundesrechtliche Regelungen, wonach einzelne Leistungen juristischen Personen des öffentlichen Rechts vorbehalten sind (wie § 20 Abs. 3 FVG oder § 126 GBO) bleiben unberührt. Diese Leistungen sind weiterhin nicht steuerbar.

Sollte sich durch Änderungen tatsächlicher oder rechtlicher Art oder durch Festsetzung durch eine Steuerbehörde dennoch 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 Besondere Leistungsmerkmale

Oracle IDOS

Die Vergütung der in Anlage 2e aufgeführten Oracle IDOS Leistungen erfolgt durch den Zentralfinanzierungsvertrag mit dem Auftragnehmer.

### 11.6 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.

### 11.7 Weisungen

Die Disposition und das alleinige arbeitsrechtliche Weisungsrecht gegenüber dem vom Auftragnehmer zur Dienstleistungserbringung eingesetzten Personals bzgl. Art, Ort, Zeit sowie Ablauf und Einteilung der Arbeiten obliegt dem Auftragnehmer. Das Personal des Auftragnehmers wird nicht in die Betriebsorganisation des Auftraggebers eingegliedert. Die im Rahmen der Vertragsdurchführung anfallenden Arbeiten werden vom Auftragnehmer eigenverantwortlich erbracht.

### 11.8 Laufzeit und Kündigung

Dieser Vertrag beginnt am 01.04.2023 und gilt für unbestimmte Zeit. Er ersetzt den Vertrag/die Änderungsverfahren gemäß Nummer 4.2 und führt dessen/deren Leistungen fort, soweit diese nicht durch Erfüllung oder auf sonstige Weise erledigt sind. Er kann erstmals unter Wahrung einer Frist von 6 Monat(en) zum 31.03.2024 gekündigt werden. Danach kann er zum Ende eines Kalenderjahres unter Wahrung einer Frist von 6 Monat(en) gekündigt werden. Die Kündigung eines Auftraggebers wirkt sich für und gegen die Auftraggeber der Verträge V15140-3/2900016, V15378-3/1041000 und V15387-3/3200740 aus, mit der Folge, dass die Kündigung für alle Auftraggeber Wirkung entfaltet. Im Falle einer Kündigung durch einen Auftraggeber wird der Auftragnehmer der verbleibenden Auftraggebern über die Leistung dieses Vertrages vor Vertragsbeendigung ein neues Vertragsangebot unterbreiten. Die Kündigung bedarf der Textform.

### 11.9 Auftragsverarbeitung

Die im Namen des Auftraggebers gegenüber dem Auftragnehmer zur Erteilung von Aufträgen bzw. ergänzenden Weisungen zu technischen und organisatorischen Maßnahmen im Rahmen der Auftragsverarbeitung berechtigten Personen (Auftragsberechtigte), sind vom Auftraggeber mit Abschluss des Vertrages in Textform zu benennen und Änderungen während der Vertragslaufzeit unverzüglich in Textform mitzuteilen.

# EVB-IT Dienstvertrag



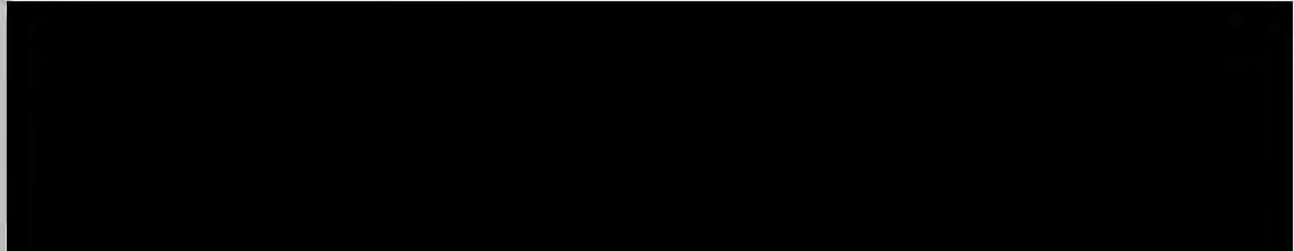
Vertragsnummer/Kennung Auftraggeber \_\_\_\_\_

Vertragsnummer/Kennung Auftragnehmer V15385-3/3011005

Seite 8 von 8

Bremen \_\_\_\_\_ , 20.04.2023 \_\_\_\_\_  
Ort Datum

\_\_\_\_\_ , \_\_\_\_\_  
Ort Datum





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

**Vertragsnummer/Kennung Auftraggeber:**

**Auftraggeber:**

Der Senator für Finanzen  
Abteilung 4 - Zentrales IT-Management  
Digitalisierung öffentlicher Dienste  
Rudolf-Hilferding-Platz 1  
28195 Bremen

**Rechnungsempfänger:**

Freie Hansestadt Bremen  
- Rechnungseingang FHB -  
Senator für Finanzen  
28026 Bremen

**Leitweg-ID**

[REDACTED]

Der Rechnungsempfänger ist immer auch der Mahnungsempfänger.

**Zentrale Ansprechpartner des  
Auftragnehmers:**

**Vertragliche Ansprechpartner  
des Auftraggebers:**

1.

**Fachliche Ansprechpartner des  
Auftraggebers:**

1.

2.

**Technische Ansprechpartner  
des Auftraggebers:**

1.

2.

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

Ort

, Datum

## Preisblatt Aufwände

**Gültig ab dem 01.04.2023**

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

- mit einer jährlichen Obergrenze für Pos. 10 - 50 von 12.000,00 €.
- mit einer jährlichen Obergrenze für Pos. 60 - 80 von 10.000,00 €.
- mit einer jährlichen Obergrenze für Pos. 90 - 100 von 20.000,00 €.

Die Abrechnung erfolgt nach Aufwand.  
Die Rechnungsstellung der Pos. 10 - 40, 60 und 80 erfolgt kalendermonatlich nachträglich gem.  
Leistungsnachweis.

Der Leistungsnachweis für Personalleistungen wird kalendermonatlich nachträglich erstellt und zugesandt. Er gilt für jeden Monat als genehmigt, wenn und soweit der Auftraggeber nicht innerhalb von 14 Kalendertagen nach Erhalt Einwände geltend macht.

Sachleistungen (Pos. 50, 70 und 90-100):  
Die Rechnungsstellung erfolgt nach erbrachter Leistung.

Die Verteilung der Kosten für Pos. 10 - 80 erfolgt analog des normalisierten Königsteiner Schlüssels.



## Preisblatt Aufwände

**Gültig ab dem 01.04.2023**

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

mit einer einmaligen Obergrenze von 6.067,00 €.

Die Abrechnung erfolgt nach Aufwand.

Die Rechnungsstellung für die Pos. 110 - 150 und Pos. 170 erfolgt kalendermonatlich nachträglich gem. Leistung

Der Leistungsnachweis für Personalleistungen wird kalendermonatlich nachträglich erstellt und zugesandt. Er

*Sachleistungen (Pos. 160):*

*Die Rechnungsstellung erfolgt nach erbrachter Leistung.*

Die Verteilung der Kosten für Pos. 110 - 170 erfolgt analog des normalisierten Königsteiner Schlüssels.





## Preisblatt Aufwände

**Gültig ab dem 01.04.2023**

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

mit einer einmaligen Obergrenze von 47.850,00 €.

Die Abrechnung erfolgt nach Aufwand.  
Die Rechnungsstellung erfolgt für Pos. 180 - 220 und Pos. 240 kalendermonatlich nachträglich gem.  
Leistungsnachweis.

Der Leistungsnachweis für Personalleistungen wird kalendermonatlich nachträglich erstellt und zugesandt. Er gilt für jeden Monat als genehmigt, wenn und soweit der Auftraggeber nicht innerhalb von 14 Kalendertagen nach Erhalt Einwände geltend macht.

Sachleistungen (230):  
Die Rechnungsstellung erfolgt nach erbrachter Leistung.

## Preisblatt Einmaliger Festpreis

**Gültig ab dem 01.04.2023**

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

**Gesamtpreis:**                     2.000,00 €



Die Rechnungsstellung des einmaligen Festpreises erfolgt nach Vertragsunterschrift.



## Preisblatt Jährlicher Festpreis

**Gültig vom 01.04.2023 bis 31.12.2023**

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

**Gesamtpreis:** 229.985,22 €

verbindliche Leistungen gemäß Dataport-Servicekatalog

A large black rectangular area covers the majority of the page, indicating that the specific service details and pricing breakdown have been redacted.

Die Rechnungsstellung des Festpreises erfolgt anteilig jeweils zum 15.03. und 15.09. jeden Kalenderjahres.

Die Verteilung der Kosten für Pos. 350 - 410 erfolgt analog des normalisierten Königsteiner Schlüssels.

## Preisblatt Jährlicher Festpreis

**Gültig ab dem 01.01.2024**

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

**Gesamtpreis:** 179.879,62 €

verbindliche Leistungen gemäß Dataport-Servicekatalog

Die Rechnungsstellung des Festpreises erfolgt anteilig jeweils zum 15.03. und 15.09. eines Kalenderjahres.

Die Verteilung der Kosten für Pos. 530 - 580 erfolgt analog des normalisierten Königsteiner Schlüssels.





IAP-Nummer: 32182-1  
 (wird von Dataport ausgefüllt)

**Anlage Datenschutzrechtliche Festlegung des Auftraggebers**

**Angaben des Verantwortlichen gem. Art. 28 DSGVO zur Auftragsverarbeitung<sup>1</sup>**

<b>Für die Verarbeitung der in Rede stehenden personenbezogenen Daten gelten folgende Datenschutzregelungen:</b>	
Verordnung (EU) 2016/679 (DSGVO)	<input checked="" type="checkbox"/>
Zusätzlich folgende bundes- bzw. landesrechtliche Regelungen (bitte Gesetz bzw. VO benennen)	<input type="checkbox"/>
Folgende bundes- bzw. landesrechtliche Regelungen zur Umsetzung der RiLi (EU) 2016/680 <sup>2</sup> (bitte Gesetz bzw. VO benennen)	<input checked="" type="checkbox"/>
Es findet keine Verarbeitung personenbezogener Daten statt	<input type="checkbox"/>

<b>1.</b>	<b>Art und Zweck der Verarbeitung</b> (siehe z. B. Art. 28 Abs. 3 S. 1 DSGVO)
	Aufbau, Betrieb und Weiterentwicklung einer technischen Infrastruktur, auf deren Basis personenbezogene Daten erhoben werden können.

<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 im BDSG und in den LDSG'en zur Umsetzung der Richtlinie (EU) 2016/680.

Als Hilfestellung zum Ausfüllen siehe daher:

[https://www.datenschutzkonferenz-online.de/media/ah/201802\\_ah\\_verzeichnis\\_verarbeitungstaetigkeiten.pdf](https://www.datenschutzkonferenz-online.de/media/ah/201802_ah_verzeichnis_verarbeitungstaetigkeiten.pdf)

<sup>2</sup> 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.

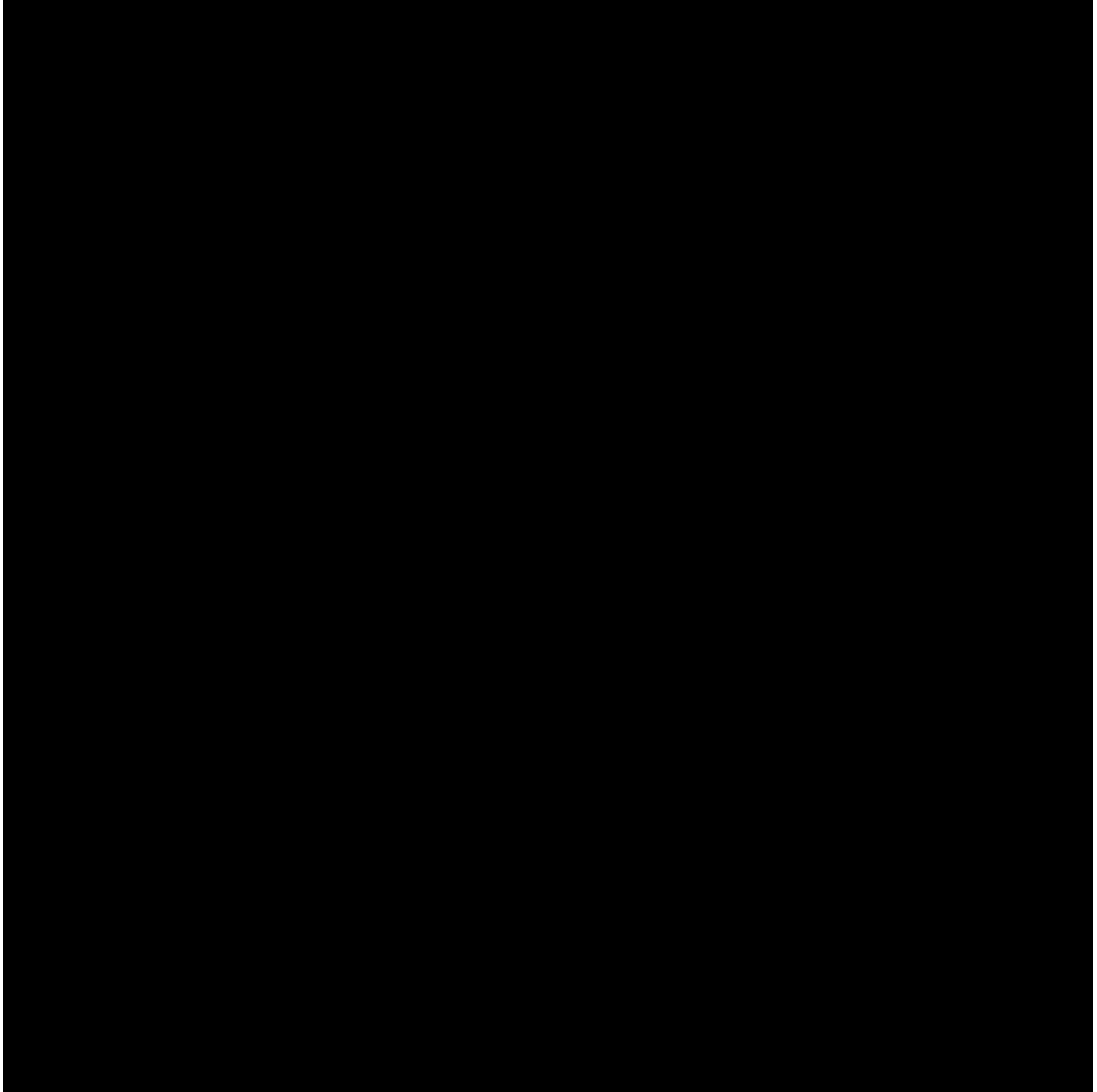
IAP-Nummer: 32182-1  
(wird von Dataport ausgefüllt)

2.	<b>Beschreibung der Kategorien von personenbezogenen Daten</b> (siehe z. B. Art. 28 Abs. 3 S. 1 DSGVO bzw. Art. 30 Abs. 1 S. 2 lit. c)
	Daten, die von Behörden aufgrund fachgesetzlicher Grundlagen erhoben werden dürfen. Eine entsprechende Regelung erfolgt durch entsprechende Nutzungsbedingungen. Ausgenommen sind Daten von besonderem Schutzbedarf.
	<b>darunter folgende Kategorien besonderer personenbezogener Daten</b> (siehe z. B. Art. 9 Abs.1 DSGVO)
	Nein.

3.	<b>Beschreibung der Kategorien betroffener Personen</b> (siehe z. B. Art. 28 Abs. 3 S. 1 DSGVO)
	divers, siehe oben. Geregelt durch Fachgesetze und Nutzungsbedingungen.

4.	<b>Übermittlung von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation</b> (siehe z. B. Art. 30 Abs. 1 S. 2 lit. e DSGVO)
	divers, siehe oben. Geregelt durch Fachgesetze und Nutzungsbedingungen.

**Liste der weiteren Auftragsverarbeiter**







## **Service Level Agreement**

### **Verfahrensinfrastruktur im Dataport Rechenzentrum**

#### **Teil A – Allgemeiner Teil -**

## Inhaltsverzeichnis

---

<b>Inhaltsverzeichnis</b>	<b>2</b>
<b>1 Einleitung</b>	<b>3</b>
1.1 Aufbau des Dokumentes	3
1.2 Allgemeine Mitwirkungsrechte und -pflichten	3
<b>2 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
2.2.7 Release Management	7
2.3 Serviceübergreifende Leistungskennzahlen (KPIs)	8
2.3.1 Reaktionszeit	8
2.4 Betriebsverantwortung	8
<b>3 Rollendefinition</b>	<b>8</b>
<b>4 Leistungsspezifische KPIs und Reporting</b>	<b>9</b>
4.1 Verfügbarkeit (Availability)	9
4.2 Auslastung	9
<b>5 Störungsprioritäten</b>	<b>10</b>
<b>6 Glossar</b>	<b>12</b>
6.1 Definition der Verfügbarkeit	16
6.1.1 Messung der Verfügbarkeit	17
6.1.2 Ausfallzeiten, die die Verfügbarkeit nicht beeinträchtigen	17

## 1 Einleitung

---

Dataport stellt Verfahrensinfrastrukturen (Server-Services und Technisches Verfahrensmanagement) im vereinbarten Serviceumfang bedarfsgerecht zur Verfügung. Die allgemeinen 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 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 Mitwirkungspflichten 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.

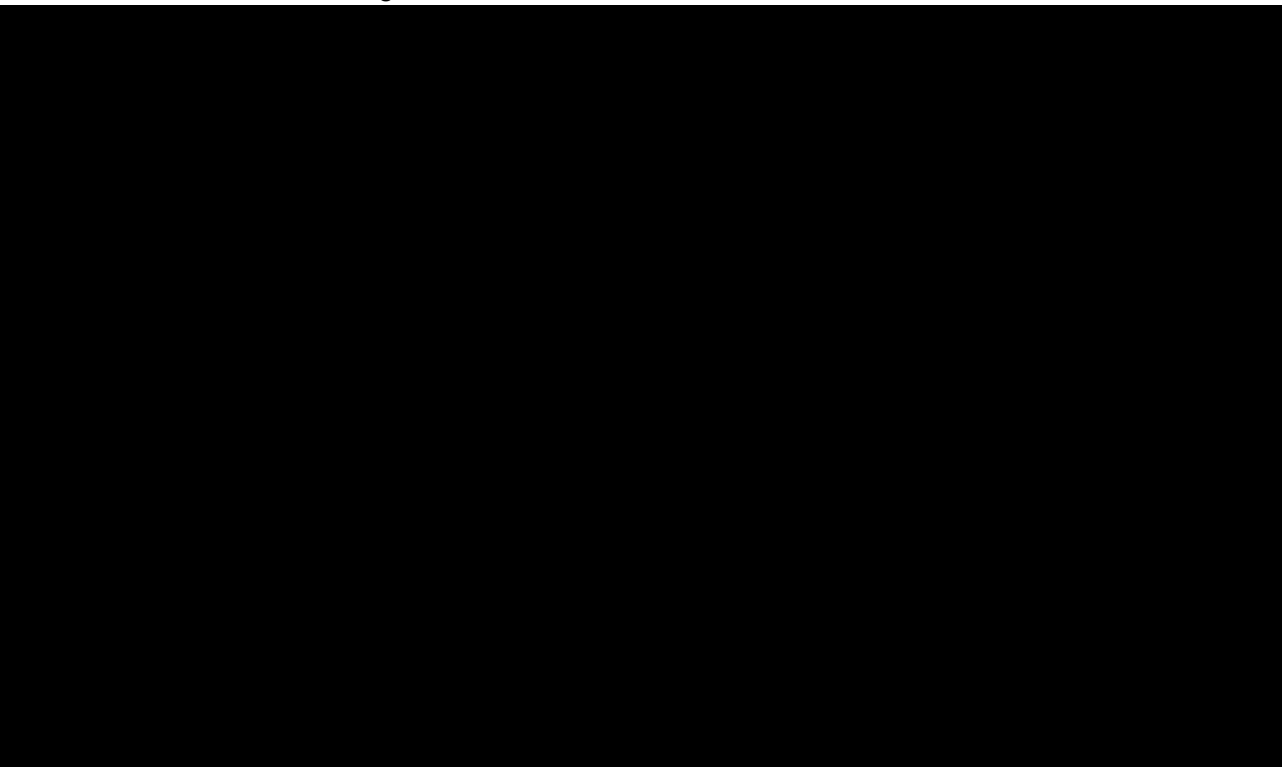


## 2 Grundlagen der Leistungserbringung

---

### 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 Standard

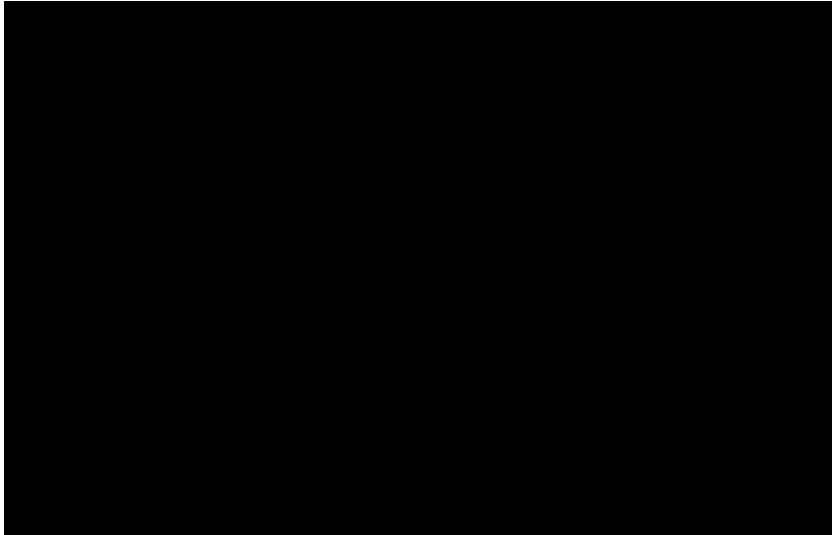
Für alle Services gilt einheitlich die Supportzeit Standard. Während der Supportzeit werden Störungen behoben und Aufträge angenommen.

Supportzeit	Montag bis Donnerstag	Freitag	Samstag / Sonntag
Standard	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 Standard.



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 Directorys 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 der 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 Erstmöglichen 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.

### **2.2.7 Release Management**

Der Auftragsverarbeiter entscheidet eigenständig über den Einsatz von Releases oder Patches für die jeweils betriebenen Softwarekomponenten auf Ebene Betriebssystem und systemnaher Software.

Nachfolgend werden die Mitwirkungsleistungen / Verpflichtungen des Auftraggebers in Bezug auf die Release-Zyklen der standardisierten Software-Komponenten (Betriebssystem, Middleware) definiert.

Release Updates müssen regelmäßig durchgeführt werden. Ca. alle drei Jahre ist mit Neuaufbau / Installation zu rechnen. Im Zuge dessen werden erhöhte Mitwirkungsleistungen des Auftraggebers bei den Releases, insbesondere bei Einhaltung der Zeit der Parallelbereitstellung, benötigt. Mit dem Auftraggeber abgestimmte Parallelbereitstellungen sind bis zu einer Dauer von vier Wochen im Leistungsumfang der regulären Verfahrensinfrastruktur enthalten. Eine vom Auftragsverarbeiter gewünschte oder verantwortete längere Parallelbereitstellung ist ebenfalls enthalten.

Bei Verfahren die nicht auf dem aktuellen, generell supporteten Software-Komponenten betrieben werden, müssen durch den Auftragsverarbeiter zusätzliche Maßnahmen getroffen werden. Wenn gesonderte Software Lizenzen Support bei EOL (End-of-Life) von Software Komponenten notwendig ist, ist dieser kein Bestandteil der regulären Verfahrensinfrastruktur und muss gesondert vereinbart werden. Auch ein „Umzug“ des Verfahrens in den Sicherheitsbereich „Minimalschutz“ ist nicht im regulären Leistungsumfang der Verfahrensinfrastruktur enthalten.

## 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 Middleware Komponenten 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.

## 3 Rollendefinition

---

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

---

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

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 Auftragsverarbeiter bis zum LÜP alleine unter der Verantwortung des AV.
Maintenance Window (MW)	Das Maintenance Window hat den primären Fokus Sicherheitsupdates oder Patche der standardisierten SW-Komponenten (Betriebssystem, Middleware) auf den Servern durchzuführen.
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>
Verfahrens-umgebungen	<p>Verfahrens-umgebungen 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>



Begriff	Definition
Verfahrensupdates	Grundsätzlich nicht Gegenstand des Wartungsfensters oder des Maintenance Windows. Sind separat zu vereinbaren.
Vertrag	Ein Vertrag kontrahiert eine gegen Entgelt angebotene Bündelung eines oder mehrerer Business Services.
Wide Area Network (WAN)	Rechnernetz, welches sich über einen sehr großen geografischen Bereich erstreckt.
Wartungsfenster	<p>Zeitfenster für Wartungsarbeiten an den Systemen mit dem primären Fokus: Updates / Erneuerungen / Wartungsarbeiten an den RZ-Diensten und der Netzinfrastruktur durchzuführen. 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>
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 Verfahrnsinfrastruktur 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.

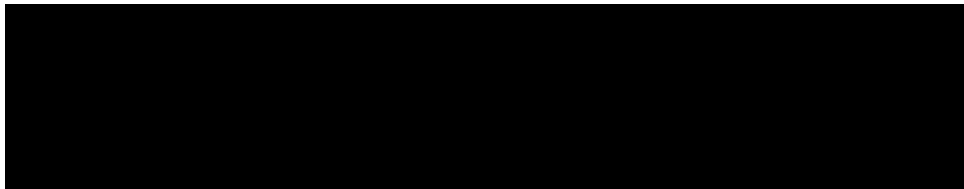
Für die Bezugszeit gilt:

Bezogen auf die Betriebszeit werden die Verfahrensinfrastrukturen grundsätzlich mit der Verfügbarkeitsklasse [REDACTED] 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 Antrags- und Fallmanagement (AFM\_ML001))**



## Inhaltsverzeichnis

---

<b>Inhaltsverzeichnis .....</b>	<b>2</b>
<b>1 Einleitung .....</b>	<b>4</b>
1.1 Einbindung des SLAs in die Vertragsstruktur .....	4
1.2 Aufbau des Dokumentes .....	4
1.3 Rollenzuordnung .....	5
1.4 Mitwirkungsrechte und -pflichten .....	5
<b>2 Rahmen der Leistungserbringung .....</b>	<b>6</b>
2.1 Servicerelevante Regelungen .....	6
2.1.1 Supportzeiten .....	6
2.1.2 Störungsannahme .....	6
2.1.3 Service Request Management .....	6
<b>3 Leistungsbeschreibung Verfahrensinfrastruktur .....</b>	<b>7</b>
3.1 Beschreibung des Fachverfahrens .....	7
3.2 Bereitgestellte Umgebungen .....	7
3.3 Details zu Server-Services .....	7
3.3.1 Bereitgestellte Server-Services .....	8
3.3.2 Zentraler Fileservice .....	12
3.3.3 Fileservice Economy .....	12
3.3.4 Application Level Gateway-Funktionalität (ALG) .....	12
3.3.5 Backup & Recovery .....	13
3.3.6 Container .....	13
3.4 Geteilte Betriebsverantwortung/ Service Fernzugriff Adminplattform (SFA) .....	13
3.5 Details zum Technischen Verfahrensmanagement .....	13
3.5.1 Serviceklassifikation .....	13
3.5.2 Schnittstellen zu anderen Fachverfahren .....	14
3.5.3 Benutzerverwaltung .....	14
3.5.4 Zeitlich befristeter und überwachter Fernzugriff .....	14
3.6 Leistungseinschränkungen .....	15
3.6.1 Leistungsbeschränkung bei geteilter Betriebsverantwortung .....	15
3.6.2 Leistungsbeschränkung bei manuellem, schreibenden Zugriff auf den Fileservice des Backendverfahrens .....	15

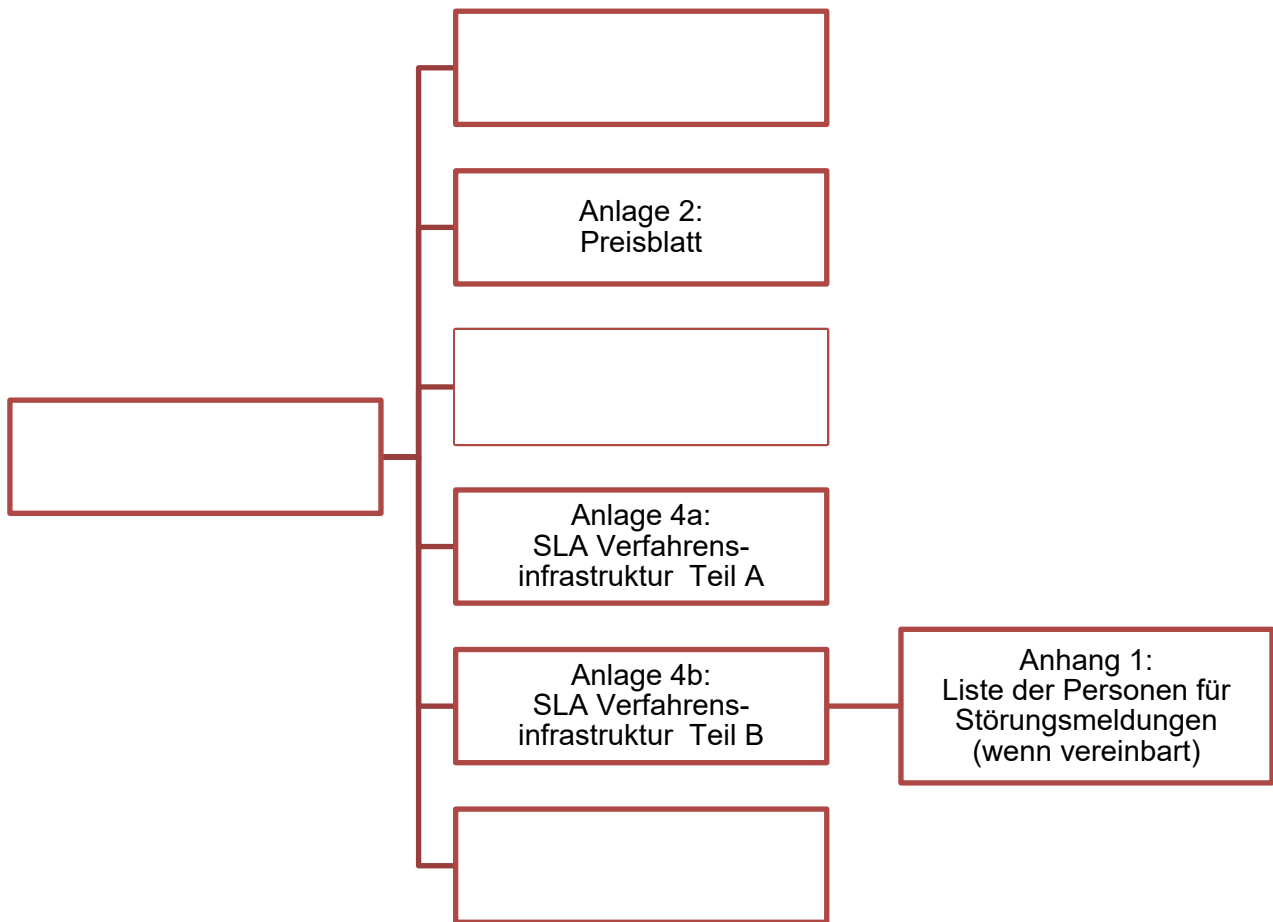


<b>4</b>	<b>Leistungsspezifische KPIs und Reporting .....</b>	<b>15</b>
<b>5</b>	<b>Maßnahmen bei Beendigung der Leistung.....</b>	<b>16</b>

## 1 Einleitung

Dataport stellt Verfahrensinfrastrukturen (Server-Services und Technisches Verfahrensmanagement) im vereinbarten 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:

- Mitwirkungspflichten des Auftraggebers, konkrete Rollenfestlegung
- die Leistungsbeschreibung: Server-Services und TVM
- ggf. Leistungsspezifische KPIs: Ausführungen zu Kennziffern und Reporting
- ggf. Maßnahmen bei Beendigung der Leistung

### 1.3 Rollenzuordnung

Für diesen SLA sind die Rollen wie folgt zugeordnet:

Rolle	Rolleninhaber
Auftraggeber (AG)	Siehe EVB-IT
Auftragsverarbeiter (AV)	Siehe EVB-IT
Zusätzliche Auftragsberechtigte (AB) zur Anlage 1 EVB-IT:	Vom Kunden benannte Personen
Nutzer	Nutzer der Verfahrrensinfrastruktur, 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 stellt gemäß Anlage 1 des EVB-IT eine Liste mit Ansprechpartnern zur Verfügung, welche gleichzeitig Auftragsberechtigte für Serviceabrufe aus dem Vertrag sind und informiert umgehend darüber, wenn sich Änderungen ergeben. Diese Verpflichtung gilt ebenso für den Auftragsverarbeiter.

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.

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.

Ein Sonderfall der Mitwirkung des Auftraggebers ist die geteilte Betriebsverantwortung (siehe Abschnitt 3.4).



## 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.

Mit der Erweiterten Supportzeit 2 kann ein standardisiertes Modell gewählt werden.

Supportzeit	Montag bis Donnerstag	Freitag	Samstag / Sonntag
Erweiterte Supportzeit 2 „7 x 24 h“	00:00 – 24:00 Uhr	00:00 – 24:00 Uhr	00:00 – 24:00 Uhr
<i>(an 365 Tagen im Jahr)</i>			

**Bemerkung:** Die Erweiterte Supportzeit 2 gilt für TVM, Linux Systemtechnik.

Innerhalb der erweiterten Supportzeiten gilt für die Erfüllung der Reaktionszeiten (Teil A; Abschnitt 2.3.1) eine Zielwahrscheinlichkeit von [REDACTED].

Kommt es durch Wartungsarbeiten innerhalb der vereinbarten Erweiterten Supportzeit zu geplanten Verfügbarkeitsbeschränkungen erfolgt regelhaft 14 Tage vorher eine Information an den Auftraggeber. Der Auftraggeber kann der Durchführung widersprechen (Teil A; Abschnitt 2.2.1).

#### 2.1.2 Störungsannahme

##### Erreichbarkeit in Erweiterter Supportzeit

Störungsannahme außerhalb der Supportzeit Standard	[REDACTED]
--	------------

#### 2.1.3 Service Request Management

Sind im vereinbarten Leistungsumfang Service Requests (Serviceabrufe) definiert, können diese durch die Auftragsberechtigten abgerufen werden. (Nummer 5.1 des EVB-IT)

Service Requests werden vom Auftraggeber und den Abrufberechtigten per Mail an das Funktionspostfach [REDACTED] eingestellt.

Die Bearbeitung wird beim Auftragsverarbeiter im Rahmen des Prozesses zum Changemanagement sichergestellt.

### 3 Leistungsbeschreibung Verfahreninfrastruktur

---

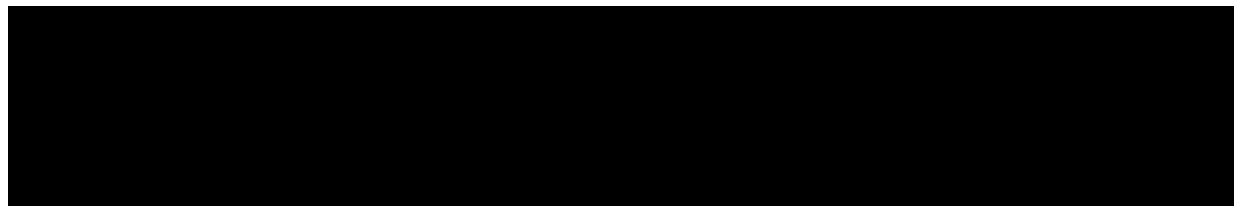
Für das nachfolgend beschriebene Fachverfahren werden eine oder mehrere Verfahrensumgebungen entsprechend den jeweiligen Produktionsstufen im Rechenzentrum von Dataport bereitgestellt. Die jeweilige Verfahrensumgebung nutzt die RZ-Basisdienste entsprechend der ausgewählten SLA-Klasse, dem Sicherheitsbereich, 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

Beim Fachverfahren AFM handelt es sich um eine Plattform für Online-Antragsverfahren die auf der Software intelliForm der Firma [REDACTED] basiert. Das System erlaubt dabei durch Konfiguration unterschiedliche Ausbaustufen vom reiner Formularserver, über Online-Assistenten bis hin zum vorgeschalteten Fallmanagement mit Anbindung an entsprechende Fachverfahren.

#### 3.2 Bereitgestellte Umgebungen

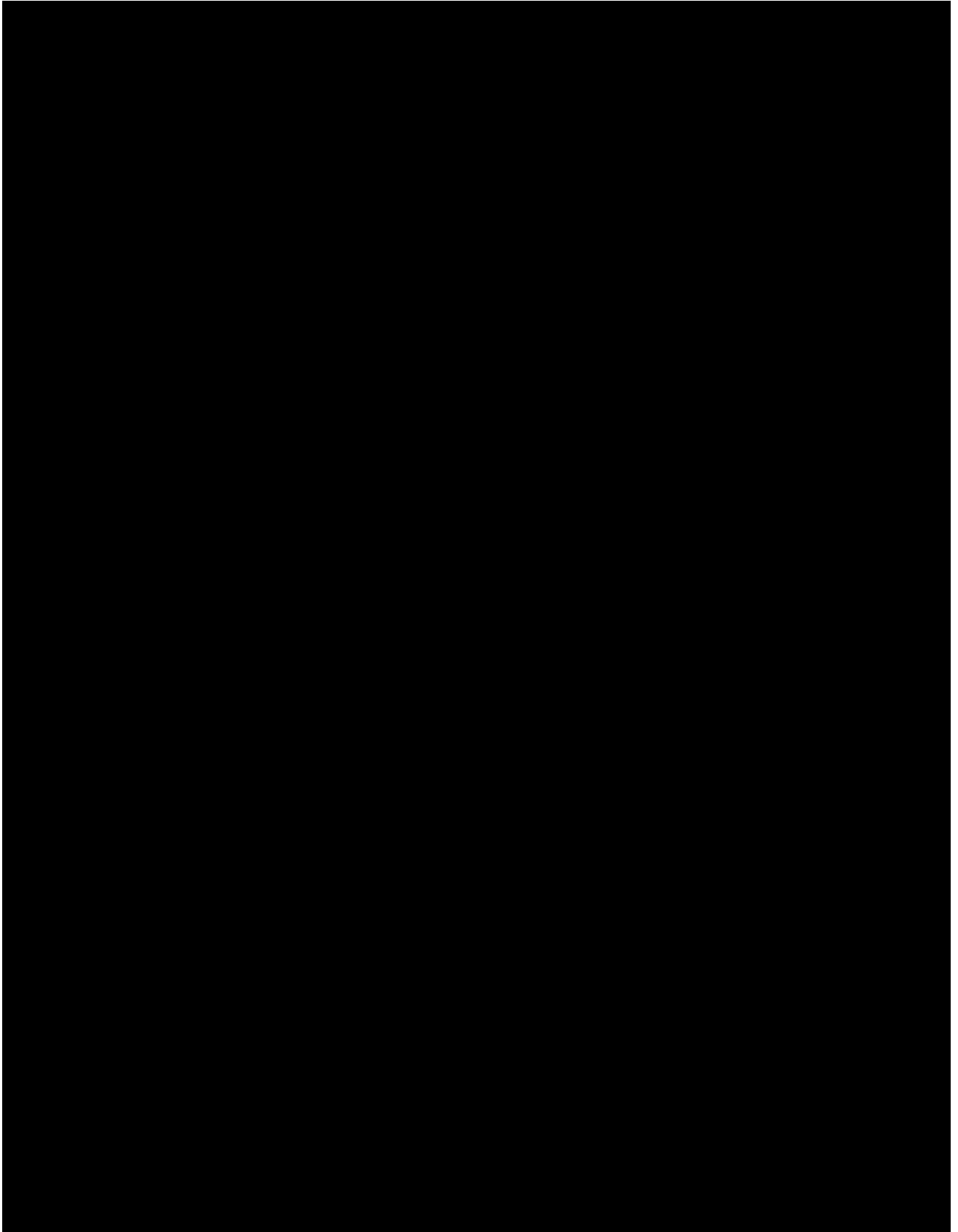


#### 3.3 Details zu Server-Services

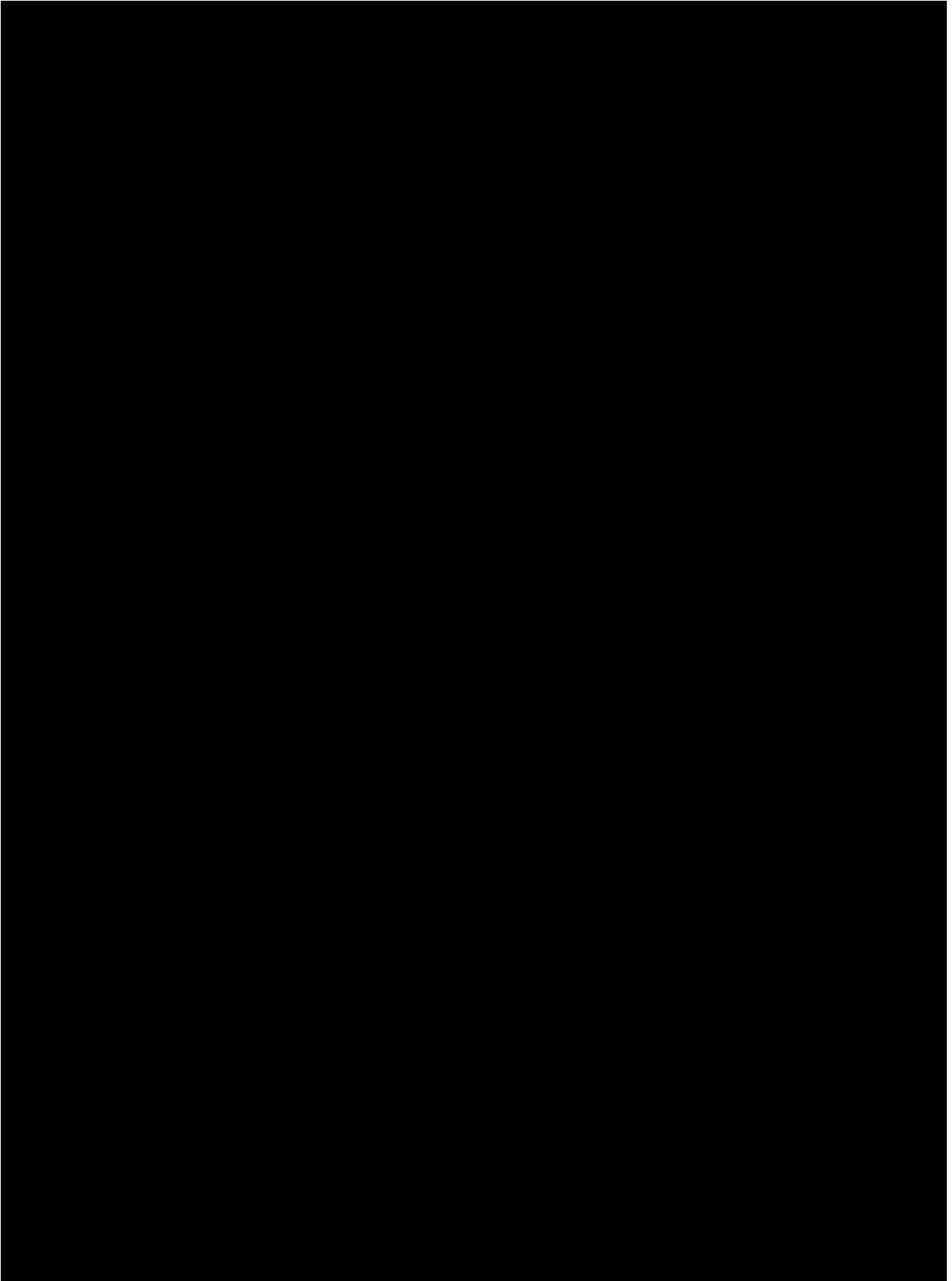
Alle nachfolgenden Server-Services werden nur mit Betriebssystemen und Middleware bereitgestellt, die sich im offiziellen Herstellersupport befindet. Bei absehbarem Auslaufen des Herstellersupports wird der Auftragsverarbeiter rechtzeitig (regelmäßig mit mindestens 24 Monaten Vorlaufzeit) auf den Auftraggeber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

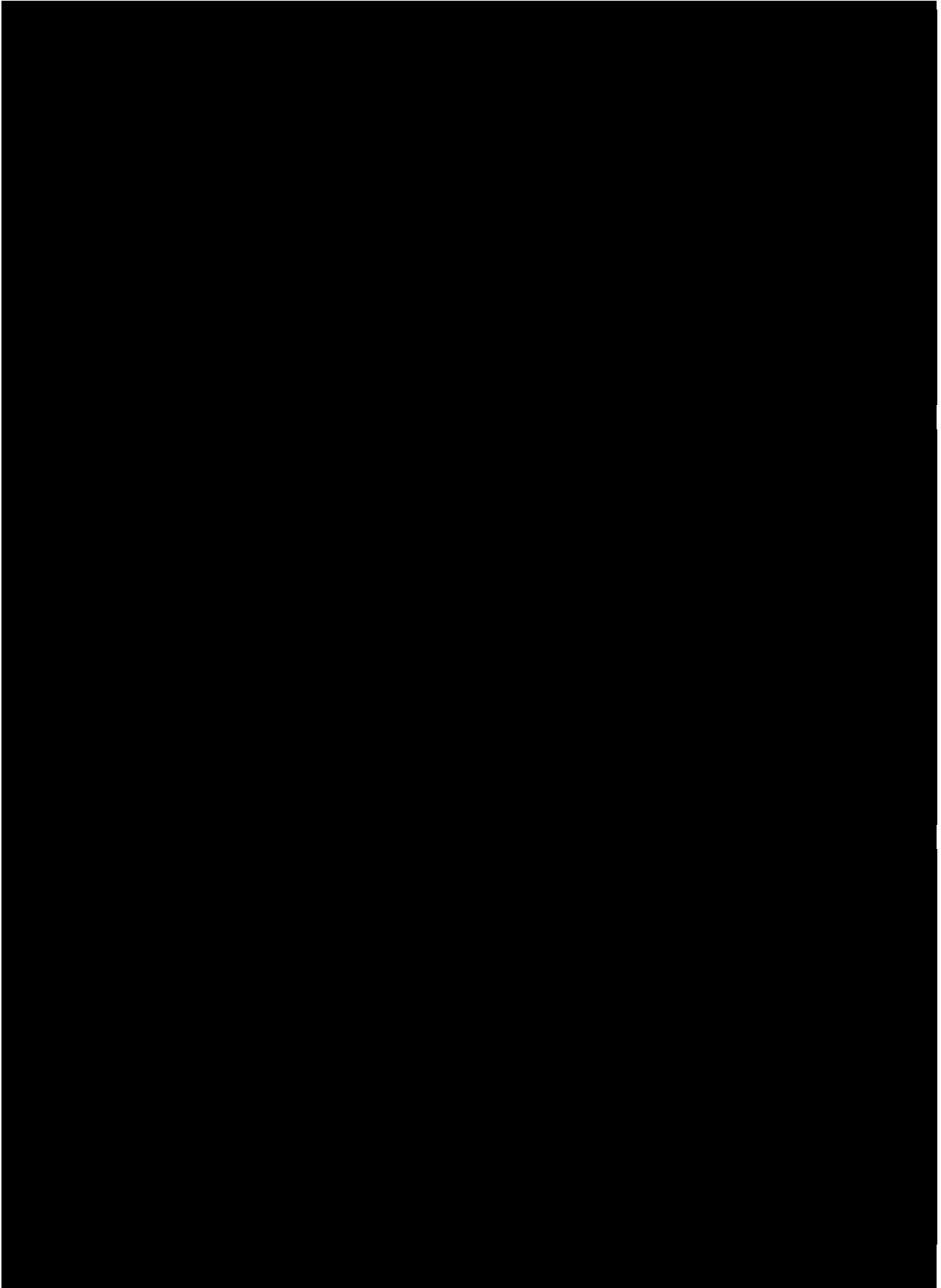
Der Auftraggeber hat keinen Anspruch auf Weiterbetrieb von Verfahreninfrastrukturen mit Betriebssystemen oder Middleware, für die kein Herstellersupport mehr besteht.

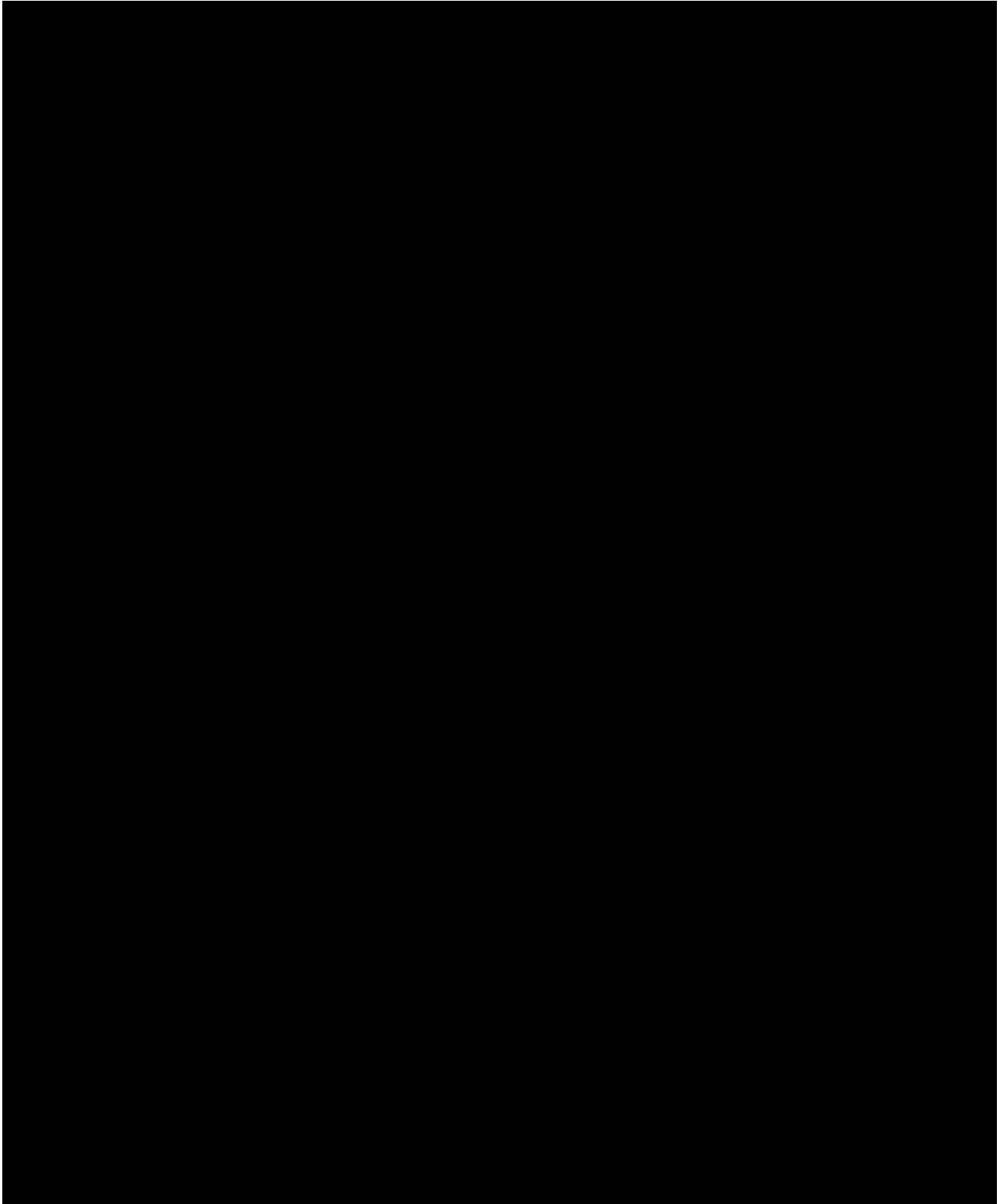
In den Server-Services ist ohne gesonderte Beauftragung durch den Auftraggeber eine systemtechnische Speicherleistung in ausreichender Größe für das Betriebssystem und die Middleware enthalten.



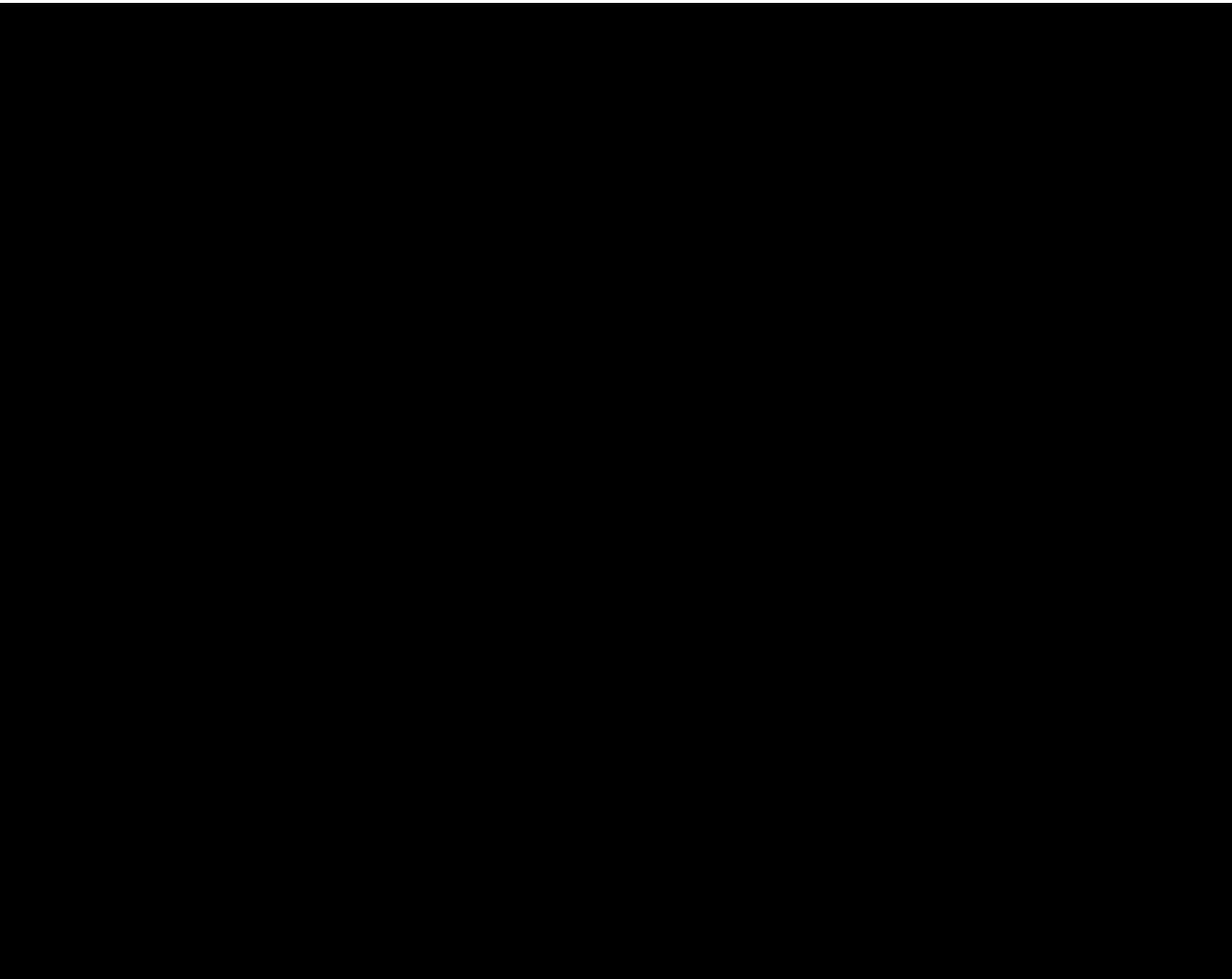












### **3.3.2 Zentraler Fileservice**

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 Auftragsverarbeiter 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.

### **3.3.6 Container**

Nicht Bestandteil des SLAs.

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

Nicht Bestandteil des SLAs.

## **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:

Produktionsstufen	Schnittstellen
Produktion	
Qualitätssicherung	
Test	

### 3.5.3 Benutzerverwaltung

Die Benutzerverwaltung für die Verfahrensinfrastruktur erfolgt:

- über die Benutzerverwaltung der Active Directory des Landes / der Länder: <Land>
- Verfahrensintern
- Sonderlösung: OSI

Die Benutzerverwaltung ist nicht Bestandteil dieser Leistungsvereinbarung.

### 3.5.4 Zeitlich befristeter und überwachter Fernzugriff

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 Auftragsverarbeiter betriebenes Verfahren folgendermaßen eingesetzt:



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.

## **3.6 Leistungseinschränkungen**

### **3.6.1 Leistungsbeschränkung bei geteilter Betriebsverantwortung**

Nicht Bestandteil des SLAs.

### **3.6.2 Leistungsbeschränkung bei manuellem, schreibenden Zugriff auf den Fileservice des Backendverfahrens**

Nicht Bestandteil des SLAs.

## **4 Leistungsspezifische KPIs und Reporting**

---

Es wurden keine weiteren leistungsspezifischen KPIs und Reports vereinbart.

## 5 Maßnahmen bei Beendigung der Leistung

---

Bei Beendigung der Vertragsbeziehung sind vom Auftragnehmer innerhalb von 6 Wochen nach Zustellung der Kündigung dem Auftraggeber die Unterlagen zur Verfügung zu stellen, die erforderlich sind, um den Geschäftsbetrieb unter geänderten Bedingungen fortzusetzen.

Dazu gehören unter anderem:

- Eine aktuelle Darstellung der im Zusammenhang mit diesem Vertrag genutzten Hardware.
- Eine aktuelle Aufstellung der für den Systembetrieb installierten Software.
- Die Übergabe der Lizenzunterlagen, soweit der Auftraggeber Lizenznehmer ist.
- Eine aktuelle Version der eingesetzten Standardkonfigurationen.
- Eine Dokumentation des eingesetzten Datensicherungssystems.
- Ein Exemplar einer aktuellen Datensicherung bzw. eines Datenexportes.
- Die Dokumentation der zu dem Zeitpunkt offenen Problemmeldungen und Aufträge.
- Jeweils eine Kopie der dem AG zuzuordnenden Handbücher, Hand-Outs und Dokumentationen.

Am Ende des letzten Tages des Vertrages bzw. der tatsächlichen Nutzung der Systeme sind vom Auftragnehmer an den Auftraggeber zu übergeben:

- der aktuelle Datenbestand,
- der Bestand der gesicherten Daten,
- alle dem Auftraggeber zuzuordnenden mobilen Datenträger (z. B. Installations-CDs, Sicherungsbänder)

Der Auftragnehmer wirkt auf Wunsch des Auftraggebers an einer durch Vertragsende durchzuführenden Migration mit. Aufwand, der durch eine solche Migration beim Auftragnehmer entsteht, sowie Materialaufwendungen und Aufwandsleistungen für individuelle Abschluss- und Sicherungsarbeiten werden vom Auftraggeber gesondert vergütet.

Der Auftragnehmer verpflichtet sich mit dem Vertragsende alle aus diesem Vertrag bezogenen Dateien und Programme in seiner Systemumgebung zu löschen.



## **Service Level Agreement**

### **Verfahrensinfrastruktur im Dataport Rechenzentrum**

#### **Teil B (spezifischer Teil für Verfahren AFM ML (AFM\_ML002))**

## Inhaltsverzeichnis

---

<b>Inhaltsverzeichnis .....</b>	<b>2</b>
<b>1 Einleitung .....</b>	<b>4</b>
1.1 Einbindung des SLAs in die Vertragsstruktur .....	4
1.2 Aufbau des Dokumentes .....	4
1.3 Rollenzuordnung .....	5
1.4 Mitwirkungsrechte und -pflichten .....	5
<b>2 Rahmen der Leistungserbringung .....</b>	<b>6</b>
2.1 Servicerelevante Regelungen .....	6
2.1.1 Supportzeiten .....	6
2.1.2 Störungsannahme .....	6
2.1.3 Service Request Management .....	6
<b>3 Leistungsbeschreibung Verfahrensinfrastruktur .....</b>	<b>7</b>
3.1 Beschreibung des Fachverfahrens .....	7
3.2 Bereitgestellte Umgebungen .....	7
3.3 Details zu Server-Services .....	7
3.3.1 Bereitgestellte Server-Services .....	7
3.3.2 Zentraler Fileservice .....	11
3.3.3 Fileservice Economy .....	11
3.3.4 Application Level Gateway-Funktionalität (ALG) .....	11
3.3.5 Backup & Recovery .....	11
3.3.6 Container .....	12
3.4 Geteilte Betriebsverantwortung/ Service Fernzugriff Adminplattform (SFA) .....	12
3.5 Details zum Technischen Verfahrensmanagement .....	12
3.5.1 Serviceklassifikation .....	12
3.5.2 Schnittstellen zu anderen Fachverfahren .....	12
3.5.3 Benutzerverwaltung .....	13
3.5.4 Zeitlich befristeter und überwachter Fernzugriff .....	13
3.6 Leistungseinschränkungen .....	14
3.6.1 Leistungsbeschränkung bei geteilter Betriebsverantwortung .....	14
3.6.2 Leistungsbeschränkung bei manuellem, schreibenden Zugriff auf den Fileservice des Backendverfahrens .....	14



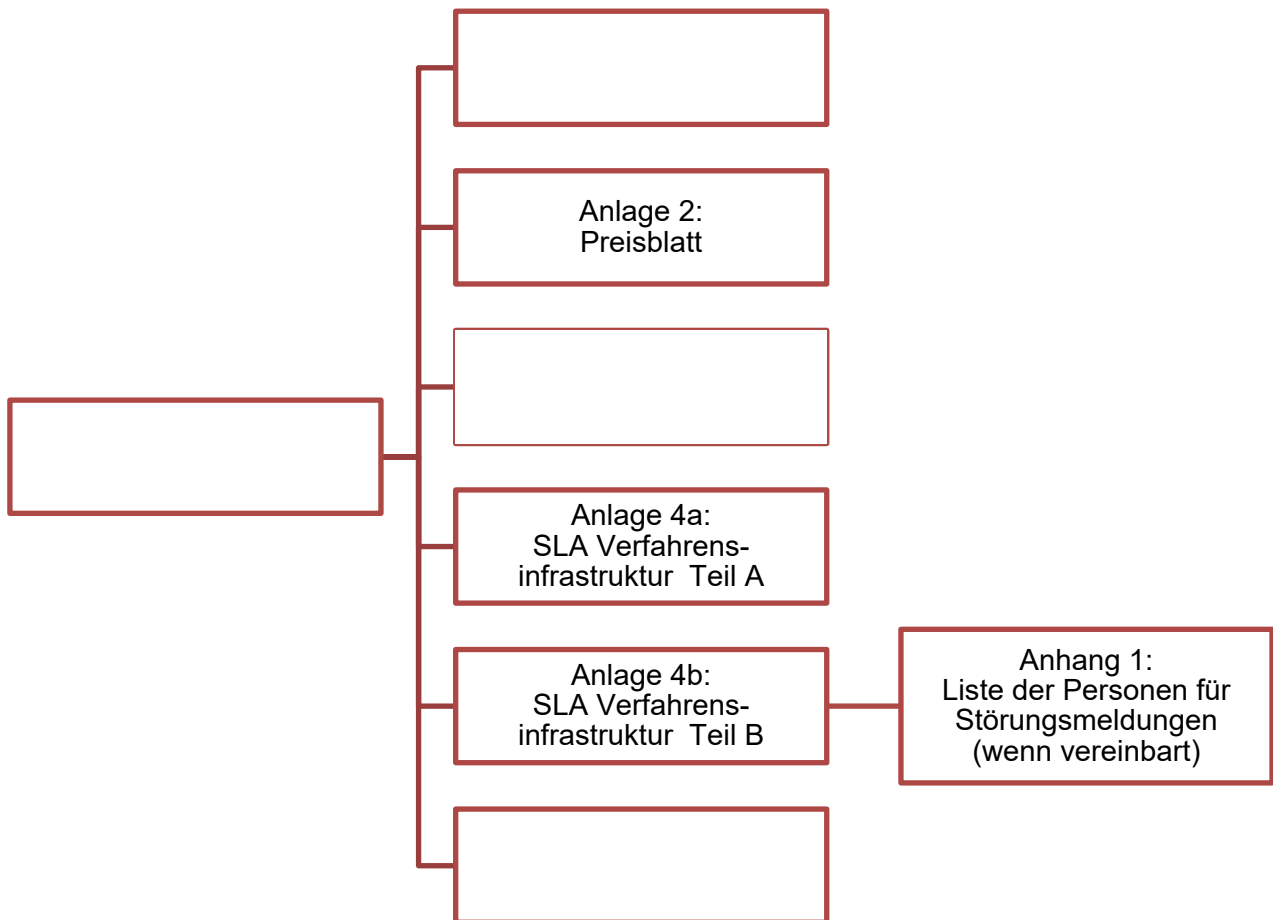


<b>4</b>	<b>Leistungsspezifische KPIs und Reporting .....</b>	<b>14</b>
<b>5</b>	<b>Maßnahmen bei Beendigung der Leistung.....</b>	<b>15</b>

## 1 Einleitung

Dataport stellt Verfahrensinfrastrukturen (Server-Services und Technisches Verfahrensmanagement) im vereinbarten 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:

- Mitwirkungspflichten des Auftraggebers, konkrete Rollenfestlegung
- die Leistungsbeschreibung: Server-Services und TVM
- ggf. Leistungsspezifische KPIs: Ausführungen zu Kennziffern und Reporting
- ggf. Maßnahmen bei Beendigung der Leistung

### 1.3 Rollenzuordnung

Für diesen SLA sind die Rollen wie folgt zugeordnet:

Rolle	Rolleninhaber
Auftraggeber (AG)	Siehe EVB-IT
Auftragsverarbeiter (AV)	Siehe EVB-IT
Zusätzliche Auftragsberechtigte (AB) zur Anlage 1 EVB-IT:	Vom Kunden benannte Personen
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 stellt gemäß Anlage 1 des EVB-IT eine Liste mit Ansprechpartnern zur Verfügung, welche gleichzeitig Auftragsberechtigte für Serviceabrufe aus dem Vertrag sind und informiert umgehend darüber, wenn sich Änderungen ergeben. Diese Verpflichtung gilt ebenso für den Auftragsverarbeiter.

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.

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.

Ein Sonderfall der Mitwirkung des Auftraggebers ist die geteilte Betriebsverantwortung (siehe Abschnitt 3.4).



## 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.

Mit der Erweiterten Supportzeit 2 kann ein standardisiertes Modell gewählt werden.

Supportzeit	Montag bis Donnerstag	Freitag	Samstag / Sonntag
Erweiterte Supportzeit 2 „7 x 24 h“	00:00 – 24:00 Uhr	00:00 – 24:00 Uhr	00:00 – 24:00 Uhr
<i>(an 365 Tagen im Jahr)</i>			

**Bemerkung:** Die Erweiterte Supportzeit 2 gilt für TVM, Linux Systemtechnik, Datenbank.

Innerhalb der erweiterten Supportzeiten gilt für die Erfüllung der Reaktionszeiten (Teil A; Abschnitt 2.3.1) eine Zielwahrscheinlichkeit von ████.

Kommt es durch Wartungsarbeiten innerhalb der vereinbarten Erweiterten Supportzeit zu geplanten Verfügbarkeitsbeschränkungen erfolgt regelhaft 14 Tage vorher eine Information an den Auftraggeber. Der Auftraggeber kann der Durchführung widersprechen (Teil A; Abschnitt 2.2.1).

#### 2.1.2 Störungsannahme

##### Erreichbarkeit in Erweiterter Supportzeit

Störungsannahme außerhalb der Supportzeit Standard	
--	--

#### 2.1.3 Service Request Management

Sind im vereinbarten Leistungsumfang Service Requests (Serviceabrufe) definiert, können diese durch die Auftragsberechtigten abgerufen werden. (Nummer 5.1 des EVB-IT)

Service Requests werden vom Auftraggeber und den Abrufberechtigten per Mail an das Funktionspostfach [dataportantragsundfallmanagement@dataport.de](mailto:dataportantragsundfallmanagement@dataport.de) eingestellt.

Die Bearbeitung wird beim Auftragsverarbeiter im Rahmen des Prozesses zum Changemanagement sichergestellt.



### 3 Leistungsbeschreibung Verfahreninfrastruktur

---

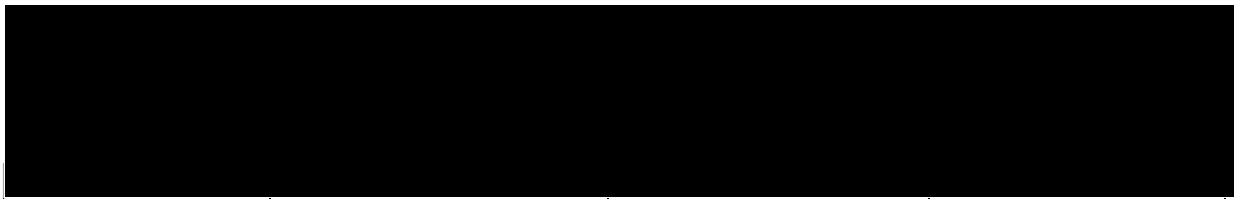
Für das nachfolgend beschriebene Fachverfahren werden eine oder mehrere Verfahrensumgebungen entsprechend den jeweiligen Produktionsstufen im Rechenzentrum von Dataport bereitgestellt. Die jeweilige Verfahrensumgebung nutzt die RZ-Basisdienste entsprechend der ausgewählten SLA-Klasse, dem Sicherheitsbereich, 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

Beim Fachverfahren AFM handelt es sich um eine Plattform für Online-Antragsverfahren die auf der Software intelliForm der Firma [REDACTED] basiert. Das System erlaubt dabei durch Konfiguration unterschiedliche Ausbaustufen vom reiner Formularserver, über Online-Assistenten bis hin zum nachgeschalteten Fallmanagement.

#### 3.2 Bereitgestellte Umgebungen



#### 3.3 Details zu Server-Services

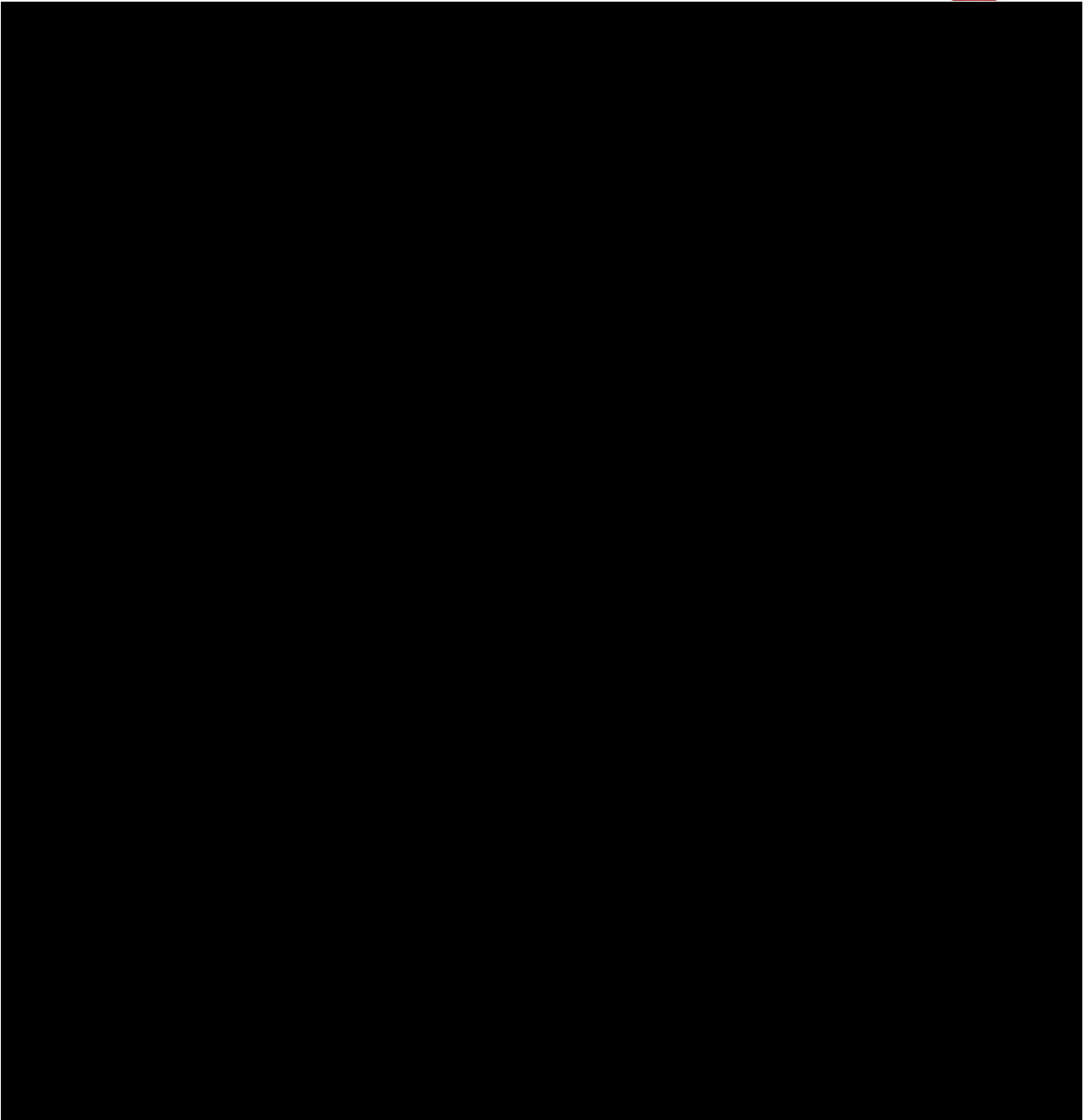
Alle nachfolgenden Server-Services werden nur mit Betriebssystemen und Middleware bereitgestellt, die sich im offiziellen Herstellersupport befindet. Bei absehbarem Auslaufen des Herstellersupports wird der Auftragsverarbeiter rechtzeitig (regelmäßig mit mindestens 24 Monaten Vorlaufzeit) auf den Auftraggeber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

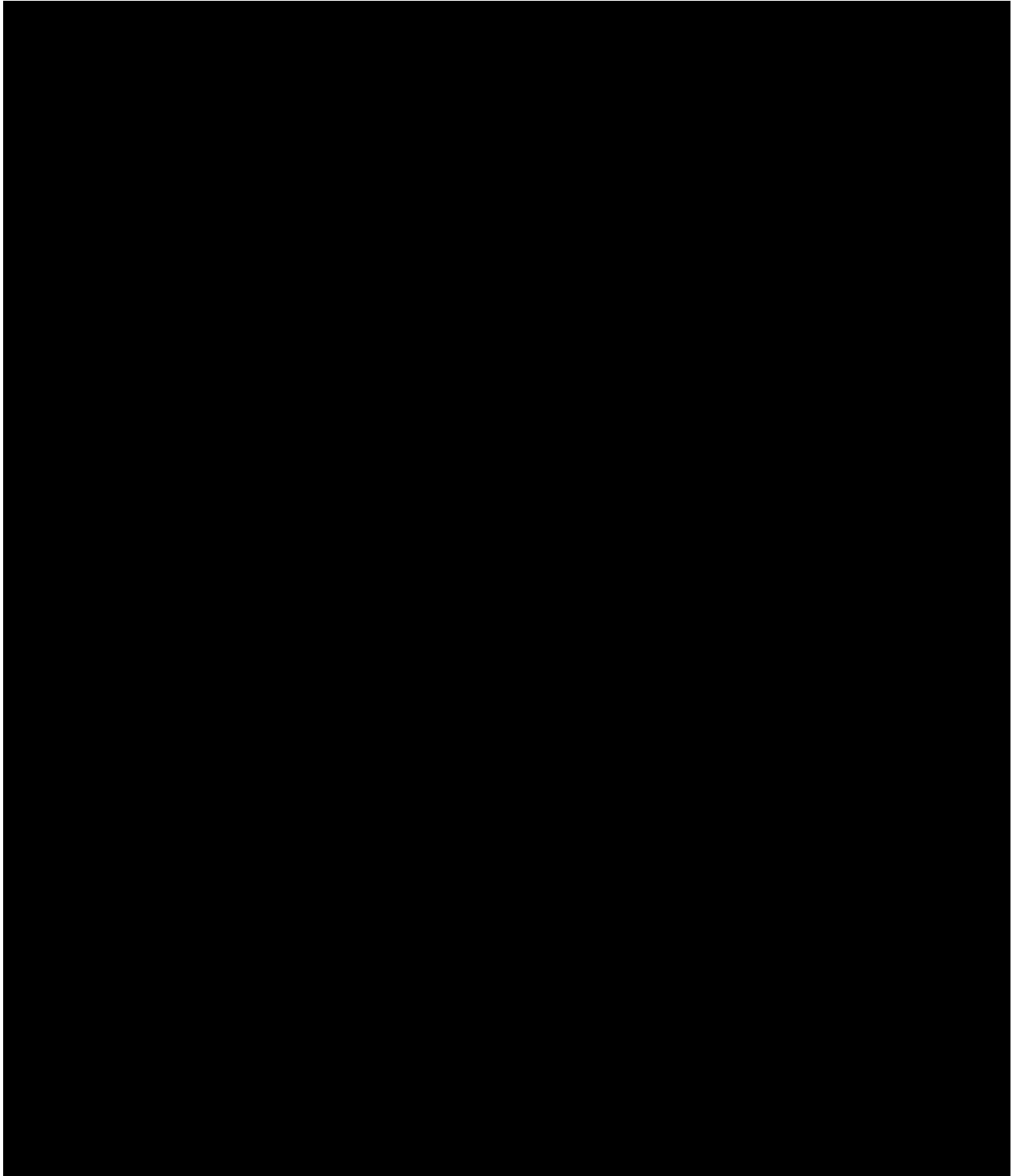
Der Auftraggeber hat keinen Anspruch auf Weiterbetrieb von Verfahreninfrastrukturen mit Betriebssystemen oder Middleware, für die kein Herstellersupport mehr besteht.

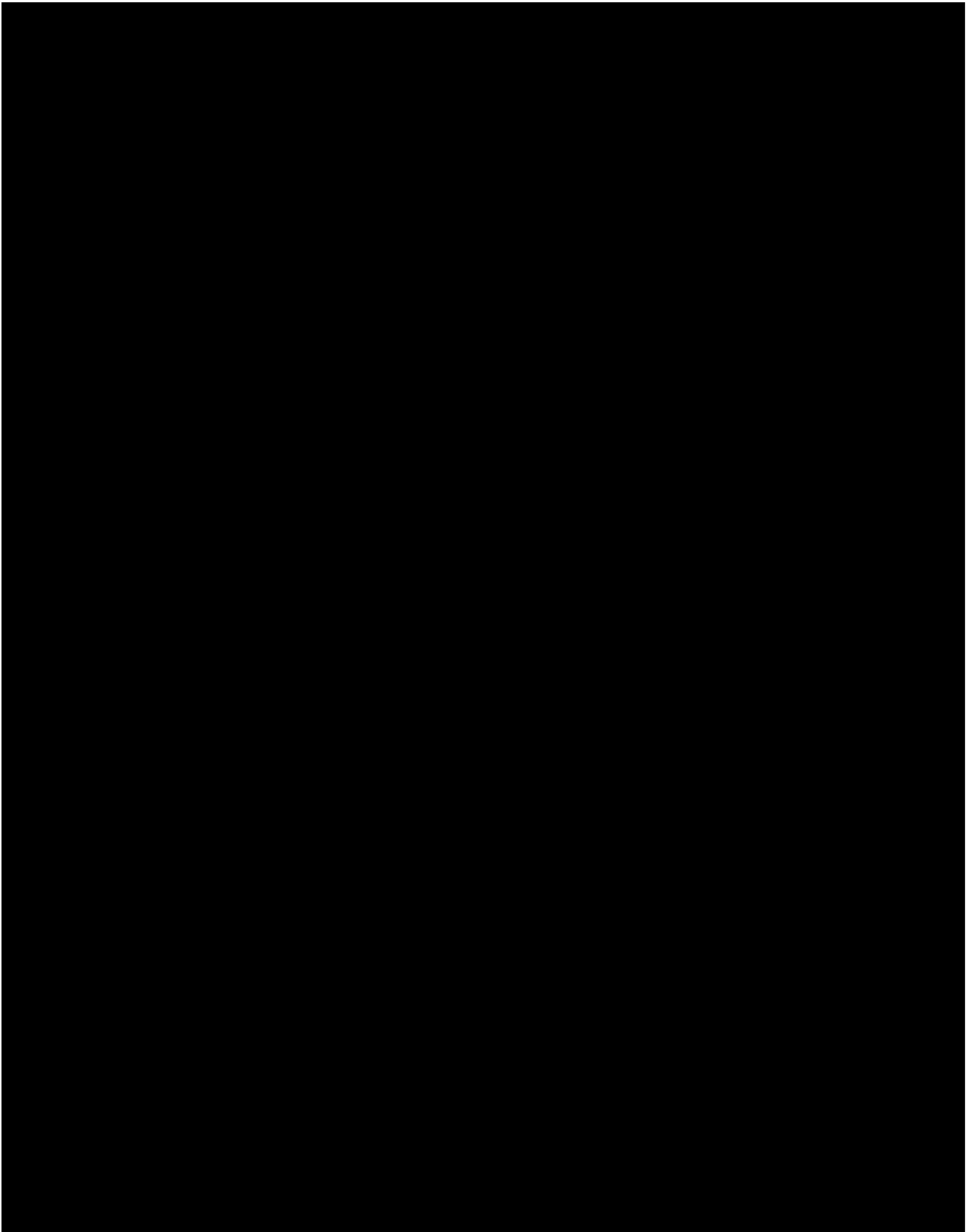
In den Server-Services ist ohne gesonderte Beauftragung durch den Auftraggeber eine systemtechnische Speicherleistung in ausreichender Größe für das Betriebssystem und die Middleware enthalten.

##### 3.3.1 Bereitgestellte Server-Services

Die Lizenzen für das Betriebssystem sind Bestandteil des Server-Services.









### **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.

Zugriff aus dem Internet ins Intranet

### **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 Auftragsverarbeiter 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.

30 Tage

### 3.3.6 Container

Nicht Bestandteil des SLAs.

## 3.4 Geteilte Betriebsverantwortung/ Service Fernzugriff Adminplattform (SFA)

Nicht Bestandteil des SLAs.

## 3.5 Details zum Technischen Verfahrensmanagement

### 3.5.1 Serviceklassifikation

Für das technische Verfahrensmanagement wird folgende Ausprägung vereinbart:

Spezifikation der Leistungsklasse	
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:

Produktionsstufen	Schnittstellen
Produktion	
Qualitätssicherung	
Test	

### 3.5.3 Benutzerverwaltung

Die Benutzerverwaltung für die Verfahrensinfrastruktur erfolgt:

- über die Benutzerverwaltung der Active Directory des Landes / der Länder: <Land>
- Verfahrenintern
- Sonderlösung: Das Verfahren hat keine Benutzerauthentifizierung. Wenn sich der Benutzer zuvor im Serviceportal angemeldet hat, werden die dort hinterlegten Daten automatisch in das Formular übernommen.

Die Benutzerverwaltung ist nicht Bestandteil dieser Leistungsvereinbarung.

### 3.5.4 Zeitlich befristeter und überwachter Fernzugriff

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 Auftragsverarbeiter betriebenes Verfahren folgendermaßen eingesetzt:



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.

## **3.6 Leistungseinschränkungen**

### **3.6.1 Leistungsbeschränkung bei geteilter Betriebsverantwortung**

Nicht Bestandteil des SLAs.

### **3.6.2 Leistungsbeschränkung bei manuellem, schreibenden Zugriff auf den Fileservice des Backendverfahrens**

Nicht Bestandteil des SLAs.

## **4 Leistungsspezifische KPIs und Reporting**

---

Es wurden keine weiteren leistungsspezifischen KPIs und Reports vereinbart.



## 5 Maßnahmen bei Beendigung der Leistung

---

Bei Beendigung der Vertragsbeziehung sind vom Auftragnehmer innerhalb von 6 Wochen nach Zustellung der Kündigung dem Auftraggeber die Unterlagen zur Verfügung zu stellen, die erforderlich sind, um den Geschäftsbetrieb unter geänderten Bedingungen fortzusetzen.

Dazu gehören unter anderem:

- Eine aktuelle Darstellung der im Zusammenhang mit diesem Vertrag genutzten Hardware.
- Eine aktuelle Aufstellung der für den Systembetrieb installierten Software.
- Die Übergabe der Lizenzunterlagen, soweit der Auftraggeber Lizenznehmer ist.
- Eine aktuelle Version der eingesetzten Standardkonfigurationen.
- Eine Dokumentation des eingesetzten Datensicherungssystems.
- Ein Exemplar einer aktuellen Datensicherung bzw. eines Datenexportes.
- Die Dokumentation der zu dem Zeitpunkt offenen Problemmeldungen und Aufträge.
- Jeweils eine Kopie der dem AG zuzuordnenden Handbücher, Hand-Outs und Dokumentationen.

Am Ende des letzten Tages des Vertrages bzw. der tatsächlichen Nutzung der Systeme sind vom Auftragnehmer an den Auftraggeber zu übergeben:

- der aktuelle Datenbestand,
- der Bestand der gesicherten Daten,
- alle dem Auftraggeber zuzuordnenden mobilen Datenträger (z. B. Installations-CDs, Sicherungsbänder)

Der Auftragnehmer wirkt auf Wunsch des Auftraggebers an einer durch Vertragsende durchzuführenden Migration mit. Aufwand, der durch eine solche Migration beim Auftragnehmer entsteht, sowie Materialaufwendungen und Aufwandsleistungen für individuelle Abschluss- und Sicherungsarbeiten werden vom Auftraggeber gesondert vergütet.

Der Auftragnehmer verpflichtet sich mit dem Vertragsende alle aus diesem Vertrag bezogenen Dateien und Programme in seiner Systemumgebung zu löschen.



## **Service Level Agreement**

### ***Fachliches Verfahrensmanagement***

### ***zum IT-Verfahren Antrags- und Fallmanagement***

Version: 1.5  
Stand: 18.08.2022

## Inhaltsverzeichnis

---

<b>1</b>	<b>Einleitung</b> .....	<b>4</b>
1.1	Leistungsgegenstand .....	4
1.2	Beschreibung des IT-Verfahrens .....	4
1.3	Vereinbarte Leistungen .....	4
<b>2</b>	<b>Leistungsrahmen</b> .....	<b>5</b>
2.1	Bestandteile des IT-Verfahrens .....	5
2.2	Verfahrensinfrastruktur .....	5
2.3	Anwendende Fachbereiche .....	5
<b>3</b>	<b>Rahmenbedingungen</b> .....	<b>6</b>
3.1	Mitwirkungsrechte und –pflichten .....	6
3.2	Fachliche Gesamtverantwortung .....	6
3.3	Ansprechpartner .....	6
3.4	Auftragsverarbeitung .....	6
<b>4</b>	<b>Steuerung und Koordination</b> .....	<b>7</b>
4.1	Produktmanagement .....	7
4.2	Abstimmung mit dem Auftraggeber und weiteren Beteiligten .....	7
4.3	Koordination von Leistungserbringern / Herstellern .....	8
<b>5</b>	<b>Leistungen zu Betriebsprozessen und zur Bereitstellung des IT-Verfahrens</b> .....	<b>8</b>
5.1	Release Management .....	8
5.2	Change Management .....	8
5.3	Incident Management .....	9
5.4	Problem Management .....	10
5.5	Access Management .....	10
5.6	Aktualisierung von Stammdaten .....	11
5.7	Bereitstellung des IT-Verfahrens in anderen Umgebungen .....	11
<b>6</b>	<b>Beratungsleistungen</b> .....	<b>12</b>
6.1	Beratung des Auftraggebers (zu Strategie und Planung) .....	12
6.2	Beratung der anwendenden Fachbereiche des Auftraggebers (zum Einsatz des Verfahrens) .....	12

---

6.3	Mitwirkung an Fachgremien und Arbeitsgruppen des Auftraggebers .....	13
6.4	Information und Austausch .....	13
6.5	Beratung bei Beteiligungen oder auf Anfrage Dritter .....	13
6.6	Beratung zu fachlichen Anforderungen.....	13
<b>7</b>	<b>Unterstützung der Anwender.....</b>	<b>14</b>
7.1	Telefonische Hilfestellung .....	14
7.2	Erstellen und Veröffentlichen von Informationen .....	14
7.3	Durchführen von Informationsveranstaltungen / Anwendergremien.....	15
7.4	Unterstützung bei Einweisungen und Schulungen .....	15
7.5	Besondere Unterstützungsleistungen .....	15
<b>8</b>	<b>Fachliche Verfahrenssteuerung .....</b>	<b>16</b>
8.1	Verfahrensspezifische Kennzahlen / Auswertungen.....	16
8.2	Überwachung von verfahrensinternen Abläufen.....	16
<b>9</b>	<b>Services zur Auftragsverarbeitung .....</b>	<b>17</b>
9.1	Ausführen von Batchprogrammen (Jobs) .....	17
9.2	Manuelle Eingriffe in Produktionsdaten.....	18
<b>10</b>	<b>Service Level .....</b>	<b>18</b>
10.1	Hinweise .....	18
10.2	Servicezeit.....	18
10.3	Reaktionszeit.....	19
10.4	Regelmäßige Gespräche zwischen Auftragnehmer und Auftraggeber .....	19
10.5	Informationsveranstaltungen / Anwendergremien .....	19
10.6	Reporting .....	20
<b>11</b>	<b>Leistungsabgrenzung .....</b>	<b>20</b>
<b>12</b>	<b>Erläuterung VDBI.....</b>	<b>21</b>



## 1 Einleitung

---

### 1.1 Leistungsgegenstand

Gegenstand dieser Leistungsvereinbarung (Service Level Agreement, SLA) zum Fachlichen Verfahrensmanagement sind Dienstleistungen des Auftragnehmers zur fachlichen Betreuung eines IT-Verfahrens sowie zur Unterstützung und Beratung des Auftraggebers und seiner anwendenden Fachbereiche.

Mit dieser Leistungsvereinbarung wird das Ziel verfolgt, qualitativ hochwertige Dienstleistungen zu erbringen, um

- die Anwenderinnen und Anwender bei der Nutzung des IT-Verfahrens zu unterstützen,
- die bestmöglichen Voraussetzungen zu schaffen, damit die Erledigung einer Fachaufgabe mit dem IT-Verfahren zur Zufriedenheit des Auftraggebers erfolgen kann, und
- sicherzustellen, dass die Abläufe im Verfahrensbetrieb im Einklang mit fachlichen Anforderungen des Auftraggebers gesteuert und durchgeführt werden können.

### 1.2 Beschreibung des IT-Verfahrens

Beim IT-Verfahren Antrags- und Fallmanagement handelt es sich um eine Infrastrukturlösung

. Die AFM-Infrastruktur ermöglicht innerhalb von Mandanten fachlich völlig unterschiedliche Antrags- und Fallbearbeitungsverfahren einzurichten, zu konfigurieren und zu betreiben. Die AFM-Verfahren werden dann im Internet oder im Intranet betrieben.

Das AFM bietet je nach Umsetzung des Fachverfahrens die Möglichkeit, folgende Komponenten zu nutzen:

- Über AFM-Modellierungstools (Composer) können fachlich unterschiedlichste Antragsverfahren entwickelt werden.
- Über sogenannte Assistenten können Online-Antragsstellungen oder Verfahrensklä rung für die Kunden der Verwaltung (einzelne Bürger oder Firmen) oder für interne Verwaltungsprozesse realisiert werden.
- Mit der Fallmanagement-Plattform können koordinierende (vermittelnde) Stelle, (z. B. der Einheitliche Ansprechpartner) und zuständige Stellen (z. B. Sachbearbeiter der Bezirke) arbeiten und in einen Dokumenten- und Mailaustausch mit dem Bürger, Unternehmen oder der Verwaltung treten.

Der Auftraggeber setzt das IT-Verfahren Antrags- und Fallmanagement für folgende Aufgaben ein:

- Als Infrastrukturkomponente für den Einsatz von unterschiedlichen Online-Antragsverfahren.

Das IT-Verfahren wird beim Auftragnehmer betrieben.

### 1.3 Vereinbarte Leistungen

In dieser Leistungsvereinbarung sind die möglichen Leistungen des Auftragnehmers zum Fachlichen Verfahrensmanagement beschrieben.

Vereinbart werden die Leistungen, die durch ein Kreuz (☒) ausgewählt worden sind. Zu diesen ausgewählten Leistungen werden die konkreten Ausprägungen und verfahrensspezifischen Merkmale beschrieben.

Leistungen, die nicht markiert wurden (☐), sind auch nicht Bestandteil dieser Leistungsvereinbarung.

Darüber hinaus beschreibt diese Leistungsvereinbarung die Aufgaben und Zuständigkeiten von Auftragnehmer und Auftraggeber. Außerdem werden Leistungskennzahlen und Messgrößen zu einzelnen Service Levels festgelegt.

## 2 Leistungsrahmen

---

### 2.1 Bestandteile des IT-Verfahrens

Die Leistungen des Fachlichen Verfahrensmanagements werden für folgende Komponenten, Module und Schnittstellen zum IT-Verfahren Antrags- und Fallmanagement erbracht:

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

### 2.2 Verfahrensinfrastruktur

Die Leistungen des Fachlichen Verfahrensmanagements werden für die zum IT-Verfahren Antrags- und Fallmanagement bereitgestellten folgenden Umgebungen erbracht:

- Testumgebung RZ<sup>2</sup>
- Qualitätsumgebung RZ<sup>2</sup>
- Produktionsumgebung RZ<sup>2</sup>

### 2.3 Anwendende Fachbereiche

Die Leistungen des Fachlichen Verfahrensmanagements werden für folgende Dienststellen / Fachbereiche des Auftraggebers erbracht:

- 
- Senatskanzlei Hamburg, Amt für IT und Digitalisierung
- MEKUN, Zentrales IT-Management SH
- SF – Der Senator für Finanzen, Abteilung 4, Referat 41 (IT Querschnittslösungen)
- Ministerium für Infrastruktur und Digitales des Landes Sachsen-Anhalt (MID-CIO-ORG)

## 3 Rahmenbedingungen

---

### 3.1 Mitwirkungsrechte und –pflichten

Die vom Auftragnehmer zugesagten Leistungen erfolgen auf Anforderung des Auftraggebers. Es sind Mitwirkungs- und Bereitstellungsleistungen des Auftraggebers erforderlich, die in dieser Leistungsvereinbarung geregelt sind.

### 3.2 Fachliche Gesamtverantwortung

Die Gesamtverantwortung für den Einsatz des IT-Verfahrens liegt beim Auftraggeber. Gleichwohl ist diese Leistungsvereinbarung darauf ausgerichtet, den Auftraggeber und seine Fachbereiche, die das IT-Verfahren nutzen (nachfolgend anwendende Fachbereiche genannt) soweit wie möglich zu entlasten.

### 3.3 Ansprechpartner

Benötigen Anwender des Auftraggebers Unterstützung bei der Bedienung des IT-Verfahrens oder Hilfestellung bei fachlichen Fragen im Zusammenhang mit der Bedienung des IT-Verfahrens, steht beim Auftragnehmer eine zentrale Kontaktstelle für alle Anwender zur Verfügung (User Help Desk oder Call Center).

Für alle Fragen und Angelegenheiten zum IT-Verfahren benennt der Auftragnehmer einen Produktverantwortlichen als Ansprechpartner<sup>1</sup>.

Der Auftraggeber benennt Ansprechpartner, die für folgende Aufgaben befugt und verantwortlich sind:

- Bewertung von Störungs- und Fehlermeldungen
- Beauftragung von Fehlerbehebungen
- Abstimmung mit dem Auftragnehmer zur Planung neuer Releases
- Erteilung von Installationsaufträgen für neue Releases
- Beauftragung des Auftragnehmers mit Leistungen, die in dieser Leistungsvereinbarung zum Fachlichen Verfahrensmanagement vereinbart wurden (Auftragsberechtigte)

### 3.4 Auftragsverarbeitung

Der Auftraggeber benennt die Verantwortlichen gemäß EU-DSGVO und kann den Auftragnehmer mit der technischen Hilfeleistung für die Datenverarbeitung beauftragen.

---

<sup>1</sup> Der Begriff „Ansprechpartner“ wird synonym für die weibliche und männliche Form verwendet.

## 4 Steuerung und Koordination

---

### 4.1 Produktmanagement

Sämtliche Leistungen, die zu dem IT-Verfahren erbracht werden, bündelt der Auftragnehmer im Produktmanagement. Das Produktmanagement beim Auftragnehmer ist zentraler und ganzheitlicher Ansprechpartner und sorgt für verbindliche Vereinbarungen und Absprachen mit dem Auftraggeber.

Das Produktmanagement umfasst insbesondere:

- Zentrale Kommunikation mit dem Auftraggeber
- Steuerung des Technischen Verfahrensmanagements:  
Sofern das SLA Technisches Verfahrensmanagement bereits Bestandteil einer Vereinbarung zwischen Auftraggeber und Auftragnehmer ist, unterstützt das Produktmanagement die reibungslose Durchführung der Betriebsprozesse und nimmt die Rolle des Auftraggebers zum Technischen Verfahrensmanagement wahr.
- Steuerung der hier vereinbarten Leistungen zum Fachlichen Verfahrensmanagement:  
Das Produktmanagement ist für die Durchführung sämtlicher Aufgaben zum Fachlichen Verfahrensmanagement beim Auftragnehmer verantwortlich. Es informiert den Auftraggeber über geplante Maßnahmen seitens des Auftragnehmers und stimmt die Durchführung besonderer Maßnahmen mit dem Auftraggeber ab.

Für vertragliche Angelegenheiten und für gewünschte Anpassungen der Leistungen benennt der Auftragnehmer einen Ansprechpartner zum IT-Verfahren (vgl. Nr. 7 im EVB-IT-Dienstvertragsformular). Dieser Ansprechpartner steht auch zur Verfügung, wenn über das Fachliche Verfahrensmanagement hinaus Leistungen zum IT-Verfahren beauftragt werden sollen. Gegenstand dieser Leistungsvereinbarung sind jedoch nur Leistungen des Produktmanagements, die unmittelbar für das Fachliche Verfahrensmanagement erbracht werden müssen.

Vereinbart wird, dass die Leistungen des Auftragnehmers

- pauschal zum Festpreis erbracht werden.
- nach Aufwand abgerechnet werden.

### 4.2 Abstimmung mit dem Auftraggeber und weiteren Beteiligten

- Im Auftrag des Auftraggebers sorgt der Auftragnehmer bei geplanten Änderungen zum IT-Verfahren für die Kommunikation und Abstimmung zwischen den Beteiligten (z.B. Entscheidungsträgern beim Auftraggeber, IT-Sicherheitsbeauftragten, Fachlichen Leitstellen, anwendenden Fachbereichen, Partnern) im Umfeld des IT-Verfahrens.

Sollen zusätzliche Leistungen durch den Auftragnehmer erbracht werden oder soll die Nutzung des IT-Verfahrens ausgeweitet werden, kann der Auftragnehmer mit der Erstellung von Leistungsbeschreibungen und entsprechenden Angeboten beauftragt werden. Die inhaltliche Ausgestaltung stimmt der Auftragnehmer mit dem Auftraggeber und weiteren Beteiligten ab.

Vereinbart wird, dass die Leistungen des Auftragnehmers

- pauschal zum Festpreis erbracht werden.
- nach Aufwand abgerechnet werden.



### 4.3 Koordination von Leistungserbringern / Herstellern

- Im Rahmen der Verfolgung von Störungen zum IT-Verfahren nimmt der Auftragnehmer Kontakt zu anderen Leistungserbringern bzw. Herstellern des IT-Verfahrens auf. Bei Bedarf koordiniert der Auftragnehmer die erforderlichen Maßnahmen zur Beseitigung der Störung. Hierbei sorgt er für die Information des Auftraggebers und stimmt das weitere Vorgehen mit allen Beteiligten ab.

Bei geplanten Änderungen zum IT-Verfahren kann der Auftragnehmer mit zusätzlichen Leistungen beauftragt werden:

- Beschaffung und Aufbereitung von Informationen von Leistungserbringern oder Hersteller
- Umsetzungsplanung und Abstimmung vorgesehener Maßnahmen
- Koordination der Durchführung.

Vereinbart wird, dass die Leistungen des Auftragnehmers

- pauschal zum Festpreis erbracht werden.  
 nach Aufwand abgerechnet werden.

## 5 Leistungen zu Betriebsprozessen und zur Bereitstellung des IT-Verfahrens

### 5.1 Release Management

- Das Release Management ist verantwortlich für die Planung, den zeitlichen Ablauf und die Steuerung des Übergangs von Releases in Test- und Produktionsumgebungen. Das Release Management soll sicherzustellen, dass die Integrität der Produktionsumgebung aufrechterhalten wird und dass die richtigen Komponenten im Release enthalten sind.

Das Fachliche Verfahrensmanagement unterstützt diesen Prozess mit folgenden Aufgaben:

Aufgaben und Zuständigkeiten	Auftrag-nehmer	Auftrag-geber
Releaseplanung in Abstimmung mit dem Auftraggeber	D	V, B
Fachlicher Test der Releases	V, D	I
Fachliche Abnahme der Releases	B	V, D
Erstellung der Anwenderinformationen	V, D	I

### 5.2 Change Management

- Das Change Management dient dem kontrollierten Umgang mit geplanten Änderungen an der IT-Infrastruktur, sowie Prozessen, Rollen oder Dokumentationen. Es wird dabei der einzuhaltende Rahmen des Vorgehens bei geplanten Veränderungen gesetzt.

Im Rahmen des Fachlichen Verfahrensmanagements erfolgt die Berücksichtigung geplanter oder durchgeführter Veränderungen bei der Abwicklung standardisierter Betriebsprozesse.



Aufgaben und Zuständigkeiten	Auftrag-nehmer	Auftrag-geber
Aufnahme einer fachlichen Anforderung / Anfrage (Request for Change, RFC)	V, D	B
Planung von Change-Durchführungen	V, D	B
Erstellung der Testpläne (fachlich)	D	V
Fachlicher Test	V, D	
Change Abnahme und Review - fachlich	B	V, D

Änderungen zum IT-Verfahren selbst (Customizing, Programmänderungen) sind nicht Bestandteil des fachlichen Verfahrensmanagements und im Rahmen von Wartung, Pflege und Weiterentwicklung des IT-Verfahrens gesondert zu vereinbaren.

### 5.3 Incident Management

- Das Incident Management reagiert auf Störungen und sorgt für die schnellstmögliche Wiederherstellung des Servicebetriebs.

Zusätzlich zu technischen Störungen werden auch Störungen im fachlichen Kontext bzw. Beeinträchtigungen bei der Bedienung des IT-Verfahrens im Rahmen eines standardisierten Incident Management Prozess bearbeitet. Zur Bearbeitung gehören folgende Aufgaben und Zuständigkeiten:

Aufgaben und Zuständigkeiten	Auftrag-nehmer	Auftrag-geber
Störungsannahme	V, D	
Unterstützung bei der Störungsverfolgung (2nd und 3rd Level)	V, D	
Fachliche Bewertung und Klassifizierung einer Störung	D	V, B
Dokumentation der Störung aus fachlicher Sicht	V, D	
ggf. Erarbeiten einer fachlichen Lösung, um die Störung zu umgehen (Workaround) und den Betrieb aus fachlicher Sicht wiederherzustellen	V, D	
Information der anwendenden Fachbereiche über die Störung und deren Beseitigung	V, D	I
ggf. Eskalation beim Hersteller des IT-Verfahrens	V, D	I

Der Auftraggeber definiert in Zusammenarbeit mit dem Auftragnehmer, wie das IT-Verfahren an sich und die Auswirkung und Dringlichkeit bei Auftreten von Störungen bewertet werden müssen.

Die Beseitigung von Störungen, die das IT-Verfahren selbst verursacht (Programmfehler), ist nicht Bestandteil des Fachlichen Verfahrensmanagements und im Rahmen einer Wartung des IT-Verfahrens gesondert zu vereinbaren.



Der Auftraggeber ist grundsätzlich verpflichtet, die Anwender in die Bedienung des IT-Verfahrens schulen bzw. einweisen zu lassen. Der Auftragnehmer ist daher berechtigt, Störungsmeldungen abzuweisen, die darin begründet sind, dass Anwender noch keine Schulung zum IT-Verfahren erhalten haben. In solchen Fällen informiert der Auftragnehmer den Auftraggeber und weist ihn auf seine Mitwirkungspflicht hin.

### 5.4 Problem Management

- Das Problem Management hat die Aufgabe, nachteilige Auswirkungen der durch Fehler in der IT-Infrastruktur oder des IT-Verfahrens verursachten Störungen und Probleme zu minimieren und eine Wiederholung zu verhindern. Hierzu werden im Rahmen des Problem Managements die Ursachen für das Auftreten von Störungen und Problemen nachhaltig untersucht und Maßnahmen für Verbesserungen initiiert.

Zum Problem Management nimmt das Fachliche Verfahrensmanagement die folgenden Aufgaben wahr:

Aufgaben und Zuständigkeiten	Auftrag-nehmer	Auftrag-geber
Erstellen von Problem Tickets	V, D	
Fachliche Untersuchung und Diagnose eines Problems	V, D	B
Einbeziehung externer Dienstleister des Auftraggebers sowie Herstellern des IT-Verfahrens und Prüfung der Ergebnisse	D	B, V
Erarbeitung einer fachlichen Lösung	D	V
Qualitätssicherung des fachlichen Lösungskonzepts	D	V
Überprüfung Umsetzbarkeit aus Request for Change	V, D	B
Kommunikation und Abschluss Problem Ticket	V, D	

Das Lösungskonzept wird dem Auftraggeber zur weiteren Verwendung zur Verfügung gestellt.

Die Umsetzung der erarbeiteten Lösung gehört nicht zum Leistungsspektrum des Fachlichen Verfahrensmanagements und ist gesondert zu beauftragen bzw. im Rahmen von Wartung, Pflege und Weiterentwicklung des IT-Verfahrens mit zu vereinbaren.

### 5.5 Access Management

- Das Access Management ist verantwortlich für die autorisierte Nutzung von IT-Services und Daten. Das Access Management bietet Unterstützung beim Schutz der Vertraulichkeit, Integrität und Verfügbarkeit, indem sichergestellt wird, dass nur berechtigte Anwender IT-Services nutzen bzw. auf Daten zugreifen oder Änderungen an diesen vornehmen können. Das Access Management kann auch als Berechtigungs-Management oder Identitäts-Management (Identity Management) bezeichnet werden.

Aufgaben und Zuständigkeiten	Auftrag-nehmer	Auftrag-geber
Einrichtung / Aktualisierung der personen-, organisations- und fachspezifischen Berechtigungen und Konten		



Aufgaben und Zuständigkeiten	Auftrag-nehmer	Auftrag-geber
<ul style="list-style-type: none"> <li>als Metadaten</li> </ul>	D	V
<ul style="list-style-type: none"> <li>in Benutzer- / Organisationsverwaltung</li> </ul>	B	V, D

In Abhängigkeit der verfahrensspezifischen Benutzerverwaltung wird festgelegt, welche Berechtigungsarten vom wem eingerichtet werden sollen.

- Die Leistung wurde bereits an anderer Stelle (z.B. Wartung und Pflege zum IT-Verfahren) geregelt.

## 5.6 Aktualisierung von Stammdaten

- Der Auftragnehmer wird mit der laufenden Aktualisierung von Stammdaten zum IT-Verfahren beauftragt. Voraussetzung hierfür ist, dass der Auftragnehmer über entsprechende Berechtigungen und Zugänge zum IT-Verfahren verfügt.

In Abhängigkeit der verfahrensspezifischen Besonderheiten wird festgelegt, welche Stammdaten unter welcher Voraussetzung im Rahmen des Fachlichen Verfahrensmanagements in der Zuständigkeit des Auftragnehmers bearbeitet werden sollen.

- Die Leistung wurde bereits an anderer Stelle (z.B. Wartung und Pflege zum IT-Verfahren) geregelt.

## 5.7 Bereitstellung des IT-Verfahrens in anderen Umgebungen

- Hat der Auftraggeber den Auftragnehmer mit der Bereitstellung einer Infrastruktur für Schulungen und / oder Tests zum IT-Verfahren beauftragt, bietet der Auftragnehmer ergänzende Leistungen für die laufende Bereitstellung des IT-Verfahrens in diesen Umgebungen an.

Folgende Leistungen werden vereinbart:

- Einrichtung und Pflege von Benutzersätzen
- Einrichtung und Pflege von Berechtigungen
- Einrichtung und Pflege von Stammdaten.
- ...

Die Leistungen werden in folgenden Umgebungen erbracht

- Test / QS
- Schulung
- Abnahme / Stage



## 6 Beratungsleistungen

---

### 6.1 Beratung des Auftraggebers (zu Strategie und Planung)

- Der Auftragnehmer berät den Auftraggeber bei allen strategischen Überlegungen und Planungen zum Einsatz des IT-Verfahrens. Der Auftragnehmer informiert sich (bei Bedarf mit Unterstützung des Auftraggebers) über die weitere Produktentwicklung und leitet daraus Handlungsempfehlungen für den Auftraggeber ab.

Sind grundlegende Änderungen zum IT-Verfahren geplant, prüft der Auftragnehmer die möglichen Auswirkungen auf die vorhandene Infrastruktur (Systemvoraussetzungen)

- die vereinbarten Betriebsprozesse
- die Geschäftsprozesse in den anwendenden Fachbereichen

und berät den Auftraggeber hinsichtlich geeigneter Maßnahmen, um den weiteren Einsatz des IT-Verfahrens optimal zu ermöglichen.

Nimmt der Auftragnehmer das Fachliche Verfahrensmanagement zu diesem IT-Verfahren gleichzeitig für mehrere Auftraggeber wahr, zeigt der Auftragnehmer mögliche Synergien auf, um einen Mehrwert für den Auftraggeber zu erzielen.

- Auf Anfrage liefert der Auftragnehmer Informationen für die jährliche Veranschlagung von Investitions- und laufenden Betriebskosten und unterstützt somit die Finanzplanung des Auftraggebers.

### 6.2 Beratung der anwendenden Fachbereiche des Auftraggebers (zum Einsatz des Verfahrens)

- Hinsichtlich der Nutzung des IT-Verfahrens in den Fachbereichen des Auftraggebers berät der Auftragnehmer verantwortliche vom Auftraggeber benannte Ansprechpartner. Im Fokus steht hierbei, Empfehlungen zur Bewältigung von grundlegenden Herausforderungen bei der Bedienung und Nutzung des IT-Verfahrens zu geben und ggf. geeignete Maßnahmen festzulegen, um strukturelle Probleme zu überwinden.
- Ein weiterer Schwerpunkt der Beratung ist die Optimierung des Einsatzes im Hinblick auf die Abläufe und Geschäftsprozesse im Fachbereich. Ziel dieser Beratungstätigkeit ist es, fachliche und organisatorische Rahmenbedingungen in Einklang mit einer effizienten Nutzung und Bedienung des IT-Verfahrens zu bringen.

Vereinbart wird, dass diese Beratungsleistungen zur Optimierung von Geschäftsprozessen

- pauschal zum Festpreis erbracht werden.
- nach Aufwand abgerechnet werden.

### 6.3 Mitwirkung an Fachgremien und Arbeitsgruppen des Auftraggebers

- Nach Auftrag leistet der Auftragnehmer Unterstützung bei der Analyse resultierender Anforderungen aus neuen oder geänderten Rechtsnormen und entwickelt entsprechende Anforderungsspezifikationen für die Weiterentwicklung des IT-Verfahrens. Die Unterstützung kann bei Bedarf und im Auftrag des Auftraggebers auch durch die regelmäßige Teilnahme an Fachgremien oder Arbeitsgruppen erfolgen.

Ebenso berät und unterstützt der Auftragnehmer bei der Durchführung von Entwicklungs- oder Einführungsprojekten sowie vergleichbaren Vorhaben.

- Die Leistungen werden beim Auftraggeber erbracht. Reisezeiten bzw. Fahrtzeiten sind im vereinbarten Preis enthalten.

Vereinbart wird, dass diese Leistungen des Auftragnehmers

- pauschal zum Festpreis erbracht werden.  
 nach Aufwand abgerechnet werden.

### 6.4 Information und Austausch

- Auftragnehmer und Auftraggeber informieren sich gegenseitig über neue Entwicklungen zum IT-Verfahren selbst sowie zu den einschlägigen Fachthemen, die für die Nutzung des IT-Verfahrens relevant sind. Ein regelmäßiger Austausch zu aktuellen Themen und den Erfahrungen mit dem Einsatz des IT-Verfahrens sind Voraussetzung für eine nachhaltig effiziente und sinnvolle Nutzung.

Im Rahmen eines regelmäßigen Informationsaustauschs wird zudem die gemeinsame und abgestimmte Planung neuer Releases oder anderer Aktivitäten zum IT-Verfahren erleichtert.

### 6.5 Beratung bei Beteiligungen oder auf Anfrage Dritter

- Auf Anfrage berät und informiert der Auftragnehmer über die Umsetzung datenschutzrechtlicher Regelungen sowie bei Fragen der Revisionsinstanzen, der Mitbestimmung im Rahmen des Personalvertretungsgesetzes und bei der Beantwortung parlamentarischer Anfragen.

Die Beteiligung von Dritten, die für den Einsatz des IT-Verfahrens erforderlich ist, liegt allein in der Verantwortung des Auftraggebers.

Der Auftraggeber kann den Auftragnehmer bei umfangreichen Veränderungen mit der Erstellung oder Anpassung einer Verfahrensbeschreibung und der Erstellung oder Aktualisierung weiterer Unterlagen (z. B. einer Risikoanalyse) beauftragen. Hierzu bedarf es einer gesonderten Beauftragung.

### 6.6 Beratung zu fachlichen Anforderungen

- Plant der Auftraggeber die Beauftragung von Änderungen, Erweiterungen oder Erneuerungen zum IT-Verfahren, berät der Auftragnehmer über die grundsätzliche Machbarkeit zur Umsetzung fachlicher Anforderungen (soweit er es beurteilen kann) und unterstützt im Rahmen der Auftragsfindung und Auftragsbeschreibung.

Die Spezifizierung und konzeptionelle Aufbereitung fachlicher Anforderungen sind hingegen gesondert zu beauftragen.

## 7 Unterstützung der Anwender

---

### 7.1 Telefonische Hilfestellung

Benötigen Anwender des Auftraggebers Unterstützung bei der Bedienung des IT-Verfahrens steht beim Auftragnehmer folgende Kontaktstelle für alle Anwender des Auftraggebers zur Verfügung:

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

Kann die Anfrage im Erstkontakt nicht beantwortet werden, erfolgt die Weiterleitung an den Fachbereich des Auftragnehmers. Der Fachbereich des Auftragnehmers versucht dann, Kontakt zum Anwender des Auftraggebers aufzunehmen.

Die Hilfestellung erfolgt telefonisch. Im Einzelfall werden vorhandene Bedienungsanleitungen oder andere schriftliche Unterlagen, die für die Beantwortung der Anfrage hilfreich sein können, zur Verfügung gestellt.

Der Auftraggeber ist grundsätzlich verpflichtet, die Anwender des Auftraggebers in der Bedienung des IT-Verfahrens schulen bzw. einweisen zu lassen. Der Auftragnehmer ist daher berechtigt, Anfragen von Anwendern des Auftraggebers abzuweisen, die noch keine Schulung zum IT-Verfahren erhalten haben. In solchen Fällen informiert der Auftragnehmer den Auftraggeber und weist ihn auf das Defizit hin.

Es wird vereinbart, dass vom Auftragnehmer zusätzlich Hilfestellung bei fachlichen Fragen im Zusammenhang mit der Bedienung des IT-Verfahrens geleistet wird.

### 7.2 Erstellen und Veröffentlichen von Informationen

Vor geplanten Änderungen zum IT-Verfahren werden Informationen zu Art und Zeitpunkt der geplanten Maßnahmen erstellt und den anwendenden Fachbereichen bekannt gegeben. Dies betrifft insbesondere die Auslieferung neuer Releases oder Änderungen an der Infrastruktur, die sich auf den Einsatz oder die Verfügbarkeit des IT-Verfahrens auswirken.

Die Anwender des Auftraggebers werden ebenfalls informiert über Störungen (Incidents), deren Beseitigung sowie Hinweisen zur Umgehung von Störungen (vgl. 5.3).

Der Auftraggeber stellt dem Auftragnehmer Verteilerlisten für die Information der Anwender bzw. anwendenden Fachbereiche des Auftraggebers zur Verfügung.

### 7.3 Durchführen von Informationsveranstaltungen / Anwendergremien

- Der Auftragnehmer bietet regelmäßige Veranstaltungen für Anwender des Auftraggebers an, auf der über neue technische und fachliche Entwicklungen zum IT-Verfahren informiert wird. Nach Möglichkeit wird hierbei der Hersteller des IT-Verfahrens einbezogen. Anwender des Auftraggebers sollen in dieser Veranstaltung Gelegenheit erhalten, sich über Erfahrungen im Umgang mit dem IT-Verfahren und auch zu fachlichen Themen auszutauschen.

### 7.4 Unterstützung bei Einweisungen und Schulungen

- Der Auftragnehmer wird zur Unterstützung bei Einweisungen und Schulungen herangezogen. Bestandteile der Leistung sind:
- Beratung des Schulungsdozenten / der Dozentin
  - Unterstützung bei der Erstellung von Schulungsunterlagen
  - Begleitung von Schulungsveranstaltungen, Unterstützung des Dozenten / der Dozentin
  - Unterstützung der Anwender durch praxisorientierte Hinweise während der Schulungsveranstaltungen

Vereinbart wird, dass diese Leistungen des Auftragnehmers

- pauschal zum Festpreis erbracht werden.
- nach Aufwand abgerechnet werden.

Für die Durchführung von Einweisungen und Schulungen ist der Auftraggeber verantwortlich. Gern unterbreitet das Schulungszentrum von Dataport hierzu Angebote.

### 7.5 Besondere Unterstützungsleistungen

- Für spezielle Anwendergruppen oder zu bestimmten Themen werden zusätzliche Unterstützungsleistungen vereinbart:
- Unterstützung der Arbeit von Multiplikatoren (Key-Usern) durch intensivere Beratung und einen verstärkten Informationsaustausch
  - Beratung von Anwendern, die im Zusammenhang mit der Bedienung des IT-Verfahrens besondere Fachkenntnisse benötigen
  - Beratung von Anwendern, die für die Erledigung ihrer Aufgabe besondere Kenntnisse im Umgang mit dem IT-Verfahren benötigen
  - ...

Vereinbart wird, dass diese Leistungen des Auftragnehmers

- pauschal zum Festpreis erbracht werden.
- nach Aufwand abgerechnet werden.



## 8 Fachliche Verfahrenssteuerung

---

### 8.1 Verfahrensspezifische Kennzahlen / Auswertungen

- Die Ermittlung von verfahrensspezifischen Kennzahlen soll dazu dienen, dass der Auftraggeber Steuerungsmöglichkeiten für eine reibungslose Nutzung des IT-Verfahrens und für den eigenen Dienstbetrieb generieren kann.

Sofern zum IT-Verfahren die Voraussetzungen gegeben sind, bietet der Auftragnehmer an, regelmäßige Auswertungen zu Betriebsdaten durchzuführen:

- Anzahl der Anwender
- Anzahl anwendender Fachbereiche oder Dienststellen
- Anzahl von Vorgängen / Fachobjekten
- durchschnittliche Dauer von Bearbeitungs- oder Erledigungszeiten zu bestimmten Vorgängen
- Anzahl übermittelter Datensätze zu Datenübermittlungen
- Anzahl erstellter Dokumente / Bescheide
- ...

Die Auswertungen erfolgen pro

- Monat
- Quartal
- Halbjahr
- Jahr

### 8.2 Überwachung von verfahrensinternen Abläufen

- Der Auftragnehmer kann mit der regelmäßigen Überwachung von verfahrensspezifischen Abläufen beauftragt werden, sofern diese Bestandteile des IT-Verfahrens sind und nicht zum Leistungsspektrum des Technischen Verfahrensmanagements gehören.

Folgende Leistungen werden beauftragt:

- Überwachung von Datenübermittlungen
- Auswertung von Protokollen
- Kontrolle von Import- / Exportfunktionen
- Überwachung von Schnittstellen zwischen Modulen / Komponenten des IT-Verfahrens
- ...

## 9 Services zur Auftragsverarbeitung

---

### 9.1 Ausführen von Batchprogrammen (Jobs)

- Batchprogramme (Jobs) sind Anwendungen zum IT-Verfahren, die speziell auf eine Stapelverarbeitung ausgerichtet sind und nicht interaktiv vom Anwender des Auftraggebers bedient werden. Sofern das Ausführen der Batchprogramme nicht automatisiert wahrgenommen werden kann, bietet der Auftragnehmer an, Batchprogramme manuell zu starten und den Ablauf zu überwachen.

Die Planung von notwendigen Batchverarbeitungen zum IT-Verfahren obliegt dem Auftraggeber. Die Planung beinhaltet die Vereinbarung mit dem Auftragnehmer, zu welchen Zeitpunkten und in welchen Intervallen die einzelnen Batchverarbeitungen erfolgen sollen. Die wiederkehrenden Läufe werden auf Grundlage des Plans pauschal durch den Auftragsberechtigten des Auftraggebers beauftragt. Der Auftragnehmer informiert den Auftraggeber, sofern einzelne Läufe nicht plangemäß ausgeführt werden können. Die Beauftragung gilt bis zu einem Widerruf der Planungen durch den Auftraggeber. Sonderläufe und Läufe, die nicht wiederkehrend sind, müssen gesondert beauftragt werden.

Zu den einzelnen Batchverarbeitungen macht der Auftraggeber Angaben über die gewünschten Intervalle und ggf. die Verwendung von Inputdatenträgern sowie die Erzeugung und den Versand von Output (Form, Empfänger).

Die Steuerung, Durchführung und Überwachung der regelmäßigen Batchverarbeitungen kann vom Auftragnehmer übernommen werden. Die Ergebnisse der Batchverarbeitungen werden dann in beauftragter Form zur Verfügung gestellt. Ebenso wird der Auftragnehmer Auskunft über fehlerhafte und abgebrochene Batchläufe geben.

Ansprechpartner für Störungsmeldungen von Datenübermittlungsempfängern ist der Auftraggeber. Bei Bedarf findet eine direkte Kontaktaufnahme zwischen Auftragnehmer und den Datenübermittlungsempfängern statt. Sollte eine erneute Datenübermittlung mit dem ursprünglich vorgesehenen Inhalt und dem gleichen Übertragungsweg erforderlich sein, führt der Auftragnehmer die Übermittlung ohne erneuten Auftrag durch, dokumentiert den Vorgang und informiert den Auftraggeber und den Datenübermittlungsempfänger über die erneute Übermittlung. Falls die Übereinstimmung von Inhalt und Übermittlungsweg nicht garantiert sind, bedarf es eines erneuten Auftrags.

Der Auftragnehmer wird mit der Ausführung folgender Batchprogramme / Jobs in folgendem Intervall beauftragt:

- ...
- ...

## 9.2 Manuelle Eingriffe in Produktionsdaten

- Verfügt der Auftragnehmer über die erforderlichen Berechtigungen und technischen Voraussetzungen, kann er damit beauftragt werden, zur Bereinigung von Inkonsistenzen im Datenbestand Eingriffe in (ggf. auch personenbezogene) Produktionsdaten vorzunehmen. Jeder einzelne Eingriff muss durch eine für diese Auftragsart berechnigte Person des Auftraggebers beauftragt und im Auftrag detailliert beschrieben werden. Sofern der Auftraggeber dies bei Erkennen einer Störung nicht leisten kann, leistet der Auftragnehmer bei der Analyse und Formulierung des Auftrags Hilfestellung.

Der Auftragnehmer dokumentiert die Umsetzung des Auftrags und informiert über:

- Person, die den Eingriff beauftragt hat, und zugehörige Dienststelle
- Datum der Auftragserteilung
- Datum der Auftragserledigung
- Inhalt des Auftrags

Jede Notwendigkeit, unregelmäßige Zustände durch einen Eingriff in Produktionsdaten zu beheben, ist ein Hinweis auf die mangelnde Robustheit des Verfahrens. Die fehlerhafte Bearbeitung ergibt sich aus dem Ausschluss nicht definierter Konstellationen. Insofern ergeben sich aus der Darstellung und Analyse wichtige Hinweise auf Fehlerursachen. Eine entsprechende Aufbereitung wird vom Auftragnehmer zur weiteren Verwendung dem Auftraggeber zur Verfügung gestellt.

## 10 Service Level

---

### 10.1 Hinweise

Zu den beschriebenen Dienstleistungen werden nachfolgende Service Levels vereinbart.

Vereinbart werden die Service Levels, die durch ein Kreuz (☒) ausgewählt worden sind. Zu diesen ausgewählten Service Levels werden die konkreten Ausprägungen und verfahrensspezifischen Merkmale beschrieben.

Service Levels, die nicht markiert wurden (☐), sind auch nicht Bestandteil dieser Leistungsvereinbarung.

### 10.2 Servicezeit

- Zum Fachlichen Verfahrensmanagement werden folgende Servicezeiten vereinbart, in denen die Ressourcen vom Auftragnehmer bedient und Störungen und Anfragen bearbeitet werden:

Wochentage	Uhrzeit von	Uhrzeit bis
Montag bis Donnerstag	09:00 Uhr	15:00 Uhr
Freitag	09:00 Uhr	14:00 Uhr

Gesetzliche Feiertage (so wie der 24.12. und 31.12.) sind von dieser Regelung ausgenommen.



### 10.3 Reaktionszeit

- Die Reaktionszeit ist der Zeitraum zwischen der Erfassung einer Anfrage bzw. eines Auftrags und dem Bearbeitungsbeginn. Bei der Bearbeitung von Anfragen des Auftraggebers bzw. der Fachbereiche oder Anwender erfolgt der erste Versuch einer Kontaktaufnahme innerhalb der Reaktionszeit.

Innerhalb der vereinbarten Servicezeiten gelten für das Fachliche Verfahrensmanagement folgende Reaktionszeiten:

Leistungsart	Reaktionszeit
Hilfestellung für Anwender (Kap. 7.1)	
Anfragen des Auftraggebers (Kap. 6.1)	
Anfragen der Fachbereiche (Kap. 6.2)	

### 10.4 Regelmäßige Gespräche zwischen Auftragnehmer und Auftraggeber

- Auftragnehmer und Auftraggeber tauschen sich regelmäßig über relevante Inhalte und geplante Maßnahmen zum IT-Verfahren miteinander aus (vgl. 6.4).

Die Gesprächsrunden finden statt

- beim Auftraggeber  
 beim Auftragnehmer  
 wechselnd  
 telefonisch

in folgendem Intervall:

- wöchentlich  
 14tägig  
 monatlich  
 einmal im Quartal  
 einmal im Halbjahr  
 einmal im Jahr

### 10.5 Informationsveranstaltungen / Anwendergremien

- Der Auftragnehmer bietet regelmäßig eine Veranstaltung für Anwender des Auftraggebers an, auf der über neue Entwicklungen zum IT-Verfahren informiert wird und Anwender Gelegenheit zu einem Erfahrungsaustausch erhalten (vgl. 7.3).

Der Auftragnehmer führt einmal im

- Quartal  
 Halbjahr



Jahr

Informationsveranstaltungen / Anwendergremien in den Räumen

des Auftragnehmers

des Auftraggebers

durch.

## 10.6 Reporting

Die Einhaltung der Service Level wertet der Auftragnehmer aus und weist diese auf Anfrage nach.

## 11 Leistungsabgrenzung

---

Ausdrücklich nicht Gegenstand dieser Leistungsvereinbarung sind folgende Leistungen:

- **Bereitstellung und Wartung der IT-Infrastruktur**  
Die Bereitstellung aller Komponenten und die Sicherstellung aller technischen Voraussetzungen, die für den Betrieb des IT-Verfahrens erforderlich sind, müssen gesondert vereinbart werden.
- **Technisches Verfahrensmanagement**  
Leistungen zum Technischen Verfahrensmanagement, die über die fachliche Beratung und Betreuung hinausgehen, sind nicht Bestandteil dieser Leistungsvereinbarung. Für das technische Verfahrensmanagement bietet der Auftragnehmer eine gesonderte Leistungsvereinbarung an.
- **Produktmanagement**  
Leistungen des Produktmanagements sind nur in dem Umfang abgedeckt, der für das Fachliche Verfahrensmanagement erforderlich ist bzw. explizit vereinbart wurde (vgl. 4.1).
- **Sicherheitsmanagement**  
Für die Nutzung des Dataport Informationssicherheitsmanagementsystems (ISMS) und die Dokumentation des Umsetzungsstandes der Sicherheitsmaßnahmen im IT-Verfahren auf Basis von IT-Grundschutz bietet der Auftragnehmer eine gesonderte Leistungsvereinbarung (SLA Security Management, SSLA) an.
- **Durchführung von Projekten**  
Projektleistungen zur Einführung neuer IT-Verfahren oder ihrer Module sind in dieser Leistungsvereinbarung nicht enthalten.
- **Modellierung neuer AFM-Verfahren**  
Die Erstellung neuer AFM-Verfahren gehört nicht zu den Leistungsvereinbarungen und ist gegebenenfalls gesondert zu beauftragen.
- **Softwarewartung und -pflege von AFM-Verfahren**  
Die Bereinigung von Programmfehlern in einzelnen AFM-Verfahren, sowie das Planen und Durchführen von Änderungen an einzelnen AFM-Verfahren gehören nicht zum Leistungsspektrum und sind an anderer Stelle zu regeln und zu vereinbaren.
- **Aufwände für Erweiterungen der AFM-Infrastruktur**  
Die technische Beratung, Steuerung und Umsetzung von Erweiterungen und Änderungen der AFM-Infrastruktur hinsichtlich neuer Funktionalitäten, Komponenten und Schnittstellen sind in dieser Leistungsvereinbarung nicht enthalten und gegebenenfalls gesondert zu beauftragen.
- **Schulungen**  
Die Planung und Durchführung von Schulungen gehören nicht zum Leistungsspektrum.

- **Benutzerverwaltung**

Die Benutzerverwaltung ist nicht Bestandteil dieser Leistungsvereinbarung.

Sämtliche Leistungen, die in diesem Dokument zur Auswahl angeboten, jedoch nicht ausgewählt worden sind, gehören ebenfalls nicht zur Leistungsvereinbarung.

## 12 Erläuterung VDBI

---

<b>V</b> = Verantwortlich	„V“ bezeichnet denjenigen, der für den Gesamtprozess verantwortlich ist. „V“ ist dafür verantwortlich, dass „D“ die Umsetzung des Prozessschritts auch tatsächlich erfolgreich durchführt.
<b>D</b> = Durchführung	„D“ bezeichnet denjenigen, der für die technische Durchführung verantwortlich ist.
<b>B</b> = Beratung und Mitwirkung	„B“ bedeutet, dass die Partei zu konsultieren ist und z.B. Vorgaben für Umsetzungsparameter setzen oder Vorbehalte formulieren kann. „B“ bezeichnet somit ein Mitwirkungsrecht bzw. eine Mitwirkungspflicht.
<b>I</b> = Information	„I“ bedeutet, dass die Partei über die Durchführung und/oder die Ergebnisse des Prozessschritts zu informieren ist. „I“ ist rein passiv.

## **Leistungsbeschreibung**

- Migration der Online-Dienste auf die neue AFM Infrastruktur -**

Version: 1.0  
Stand: 25.08.2022



## Inhalt

<b>1</b>	<b>Leistungsbeschreibung .....</b>	<b>3</b>
1.1	Leistungsumfang .....	3
1.2	Unterstützungsleistungen durch den Hersteller .....	3
<b>2</b>	<b>Aufwandsschätzung.....</b>	<b>3</b>
<b>3</b>	<b>Rahmenbedingungen .....</b>	<b>3</b>
3.1	Mitwirkungspflichten des Auftraggebers.....	3



## 1 Leistungsbeschreibung

---

### 1.1 Leistungsumfang

Die AFM Infrastruktur wird im Rahmen eines EHdB in 2022 neu aufgebaut. Die neue Infrastruktur wird modularisiert (Antragsmanagement, Fallmanagement, Interface Manager) und in ihren Funktionen und Schnittstellen standardisiert.

Nach Beendigung des EHdB müssen alle produktiven und zum Zeitpunkt des EHdB in Entwicklung befindlichen Online-Dienste (Antragsmanagement) auf die neue Infrastruktur migriert werden. Hierfür muss jeder Online-Dienst analysiert und der individuelle Anpassungsbedarf ermittelt werden. Im Anschluss müssen alle Online-Dienste auf den Standard der neuen Infrastruktur angepasst werden. Sobald der Online-Dienst dem Standard entspricht, kann er auf die neue Infrastruktur migriert werden. Die Migration auf die neue Infrastruktur erfolgt über alle drei Umgebungen (Test, Stage, Produktion). Vor der Produktivsetzung ist eine fachliche Abnahme des Online-Dienstes durch den Auftraggeber bzw den jeweils zuständigen Online-Dienst Verantwortlichen durchzuführen.

Die Leistungen erfolgen in Form einer Dienstleistung.

### 1.2 Unterstützungsleistungen durch den Hersteller

Im Rahmen der Leistungserbringung sind eventuell Unterstützungsleistungen der Firma [REDACTED] notwendig.

## 2 Aufwandsschätzung

---

Im Rahmen der Erstellung des Grobkonzeptes zur neuen Infrastruktur erfolgte eine grobe Aufwandsschätzung für die Migration der Online-Dienste. Die Schätzung ergab, dass pro anzupassendem Online-Dienst (produktiv oder zum Zeitpunkt des EHdB in Entwicklung) mit einem mittleren Aufwand von 1,5 PT zu rechnen ist. Der tatsächliche Aufwand kann erst nach einer tiefergehenden Analyse ermittelt werden. Die Obergrenze bemisst sich anhand der Anzahl der zu migrierenden Online-Dienste und wurde anhand der aktuell produktiven und in Entwicklung befindlichen Online-Dienste ermittelt (Stand: 21.07.2022).

## 3 Rahmenbedingungen

---

### 3.1 Mitwirkungspflichten des Auftraggebers

Der Auftraggeber unterstützt bei der Information der Online-Dienst Verantwortlichen, sowie bei der Koordination der für die Produktivsetzung notwendigen fachlichen Abnahmen der einzelnen Online-Dienste.

Der Auftraggeber benennt einen fachlichen Ansprechpartner, der für Rückfragen und Absprachen zur Verfügung steht.

## **Service Level Agreement**

### **Bereitstellung von Systemen in der dSecureCloud - IaaS**

Version: 1.5  
Stand: 30.08.2022

## Inhaltsverzeichnis

---

<b>1</b>	<b>Einleitung .....</b>	<b>4</b>
<b>2</b>	<b>Allgemeine Leistungen .....</b>	<b>5</b>
2.1	Basisleistungen.....	5
2.1.1	Grundschutzkonformer Betrieb.....	5
2.1.2	Datenschutz.....	6
2.1.3	Virenschutz .....	6
2.1.4	Monitoring .....	7
2.1.5	Verfügbarkeit .....	7
2.1.6	Zugang.....	7
2.1.7	Netzkommunikation .....	7
2.1.8	Verschlüsselung .....	8
2.1.9	Authentisierung.....	8
2.1.10	Löschung von Daten.....	8
2.1.11	Offenlegung von Daten des Auftraggebers .....	8
2.1.12	Berichtswesen und Rechnungsstellung.....	8
2.1.13	Protokollierung.....	9
2.2	Leistungsgegenstand.....	9
2.2.1	Leistungsmerkmale eines virtuellen Servers in der dSecureCloud.....	9
2.2.2	Betriebssysteme in der dSecureCloud .....	9
2.3	Mitwirkungsleistungen und Pflichten des Auftraggebers.....	9
<b>3</b>	<b>Leistungsbeschreibung .....</b>	<b>10</b>
3.1	Anforderungen an die Infrastruktur des Auftraggeber .....	10
3.1.1	Netzwerk-Anbindung und Firewall.....	10
3.2	Lizenzleistungen .....	10
3.3	Leistungsabgrenzung .....	10
3.4	Optionale Leistungen.....	11
3.4.1	Datensicherung.....	11
3.4.2	Erweiterte Netzkommunikation.....	11
3.4.3	Zusatzservice Erreichbarkeit über öffentliche Netzwerke .....	11
3.4.4	Virenschutz .....	12
<b>4</b>	<b>Leistungskennzahlen .....</b>	<b>12</b>
4.1	Leistungsausprägung .....	12
4.1.1	Betriebszeiten .....	12
4.1.1.1	Onlineverfügbarkeit.....	12



4.1.1.2	Servicezeit - Betreuer Betrieb.....	12
4.1.1.3	Servicezeit - Überwacher Betrieb .....	12
4.1.2	Wartungsarbeiten .....	13
4.1.3	Support .....	13
4.1.4	Störungsannahme .....	13
4.1.5	Incident-Management.....	13
<b>5</b>	<b>Erläuterungen .....</b>	<b>15</b>
5.1	Begriffsfestlegungen.....	15
5.2	Erläuterung VDBI.....	16



## 1 Einleitung

---

Dataport (nachfolgend Auftragnehmer) stellt mit dem Infrastructure-as-a-Service (IaaS) in der dSecureCloud eine „On Demand“ Lösung für die Bereitstellung von Servern für Trägerländer (nachfolgend Auftraggeber) bereit. IaaS in der Dataport Cloud wurde entwickelt, um eine wirtschaftliche und zugleich flexible Bereitstellungsform für virtuelle Server anzubieten. Sie unterscheidet sich in ihrem Leistungsumfang stark vom „Full Service Support“.

Mittels eines Self-Service-Portals kann ein Anwender virtuelle Systeme (VM) nach seinem eigenen Bedarf bereitstellen. Hierbei ist es ihm möglich, Ressourcen seinen benötigten Servern zuzuweisen, als auch aus einer vorgegebenen Auswahl ein Betriebssystem auszuwählen. Die Bereitstellung des virtuellen Servers erfolgt vollautomatisiert, jedoch ohne Konfiguration des Betriebssystems oder betriebssystemnaher Komponenten.

Über einen Proxy Zugang wird die Erreichbarkeit des virtuellen Servers ins Internet hergestellt. Aus dem jeweiligen Clientnetz sind die Server direkt per RDP (Microsoft Windows) oder SSH (Linux), ohne einen eToken oder den Zugang zu einer Adminplattform, zu erreichen. Die Erreichbarkeit der virtuellen Server ist nur untereinander möglich. Zusätzliche Freischaltungen müssen beim Dataport Policymanagement eingereicht werden und unterliegen einem Genehmigungsvorbehalt. Freischaltungen in weitere RZ-Bereiche sind nicht möglich.

Der IT-Grundschutzkonforme Betrieb der Virtualisierungsinfrastruktur wird vom Auftragnehmer für die Verarbeitung von Daten mit dem Schutzbedarf „normal“ gewährleistet. Die virtuellen Systeme selbst, sind im Gegensatz zum „Full Service Support“, ungehärtet und werden vom Auftragnehmer nicht betreut. Sicherheitspatches von Betriebssystem und betriebssystemnaher Software müssen vom Anwender selbstständig installiert werden. Ein Virenschutz für die VMs wird bereitgestellt. Ein Monitoring findet nur für die zugrunde liegende Virtualisierungsinfrastruktur statt, nicht jedoch für die vom Anwender betreuten Server. Es bestehen jedoch keinerlei Verfügungsansprüche für die vom Anwender betriebenen virtuellen Server.

Störungen des Self-Service-Portals können über den User-Help-Desk eröffnet werden, während die Anwender-VMs keinem Support durch den Auftragnehmer unterliegen. Die Option auf eine vollständige Datensicherung und Wiederherstellung der Systeme ist möglich.

## 2 Allgemeine Leistungen

### 2.1 Basisleistungen

Die Basisleistungen stellen die Grundlage des Infrastructure-as-a-Service (IaaS) innerhalb der dSecureCloud dar. Mit dem Self-Service-Portal stellt sich der Auftraggeber seine benötigten virtuellen Server mit den von ihm benötigten Ressourcen flexibel selbst bereit. Zu den Ressourcen, die vom Auftraggeber wählbar sind, gehören RAM, CPU Cores, Kapazität sowie Partitionierung von Storage als auch die Wahl der Betriebssystemplattform.

Die Bereitstellung des virtuellen Servers erfolgt vollautomatisiert über die vom Auftragnehmer bereitgestellten Server-Templates. Es findet keine Konfiguration des Betriebssystems oder möglicher betriebssystemnaher Komponenten durch den Auftragnehmer statt. Der Server wird eigenverantwortlich vom Auftraggeber betreut.

Aufgaben und Zuständigkeiten	Auftragnehmer	Auftraggeber
Bereitstellung der Server-Templates zur Erstellung von virtuellen Servern in der Cloud	V, D, B	I
Erstellung eines virtuellen Servers über das Self-Service-Portal	I	V, D, B
Konfiguration des virtuellen Servers nach Erstellung über das Self-Service-Portal	I	V, D, B
Ressourcenerweiterung des virtuellen Servers (RAM, Cores, Festplatten)	I	V, D, B

#### 2.1.1 Grundschutzkonformer Betrieb

Die zum Betrieb der dSecureCloud erforderliche Infrastruktur erfüllt die Anforderungen des grundschutzkonformen Betriebs des BSI bis zur Schutzstufe „normal“ und wird vom Auftragnehmer gewährleistet.

Der sichere Betrieb für die vom Auftraggeber eigenadministrierten virtuellen Server in der dSecureCloud wird nicht vom Auftragnehmer gewährleistet.

Für das Update- und Patchmanagement der Infrastruktur der dSecureCloud ist der Auftragnehmer verantwortlich.

Die Servertemplates für Neubereitstellungen werden regelmäßig für die vom Auftraggeber nutzbaren Betriebssysteme vom Auftragnehmer auf ein aktuelles Patch- und Updatelevel gehoben.

Ab dem Zeitpunkt der Bereitstellung der virtuellen Systeme verpflichtet sich der Auftraggeber aktuelle Sicherheitspatches und Updates für das Betriebssystem und installierte Software auf seinen betreuten virtuellen Servern innerhalb der dSecureCloud selbstständig zu beziehen und zu installieren.

Der Auftragnehmer behält sich das Recht vor, kundenbetreute Maschinen stillzulegen, wenn diese ein Sicherheitsrisiko (zum Beispiel Teil eines Bot-Netzes, Viren- oder Malwarebefall) darstellen oder nach wiederholter Aufforderung keine sicherheitsrelevanten Patches eingespielt werden.

Aufgaben und Zuständigkeiten	Auftragnehmer	Auftraggeber
Grundschutzkonformer Betrieb der dSecureCloud Infrastruktur	V, D, B	I
Sicherer Betrieb der virtuellen Server innerhalb der dSecureCloud ab Bereitstellung, inkl. Einspielung von Patches und Updates	I	V, D
Anpassung der Templates für Neubereitstellungen auf aktuelles Patch- & Updatelevel	V, D, B	
Planung von systemspezifischen Wartungsarbeiten an der dSecureCloud Infrastruktur	V, D	I



### 2.1.2 Datenschutz

Der Auftraggeber ist allein verantwortlich für die Art der Nutzung der bereitgestellten virtuellen Systeme inklusive der verwendeten Daten. Verarbeitet der Auftraggeber auf den bereitgestellten virtuellen Systemen des Auftragnehmers personenbezogene Daten, so ist der Auftraggeber bezüglich der Verarbeitung dieser personenbezogenen Daten Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO. Der Auftraggeber ist ebenfalls für die Einhaltung der in Kapitel IV der DSGVO und ggfs. ergänzend geltender nationaler Datenschutzvorschriften verantwortlich, insbesondere für

- die Rechtmäßigkeit der Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten,
- sofern die Verarbeitung auf der Grundlage einer Einwilligung erfolgt, die Einholung und Dokumentation von Einwilligungserklärungen, die Dokumentation von Widerrufserklärungen und die Umsetzung der im Falle eines Widerrufs erforderlichen Maßnahmen,
- die Prüfung, ob gemäß Art. 35 DSGVO eine Datenschutz-Folgeabschätzung durchzuführen ist, und falls ja, für die Durchführung derselben,
- die Dokumentation der zum Schutz der Daten getroffenen Maßnahmen, soweit diese in nicht von dem Auftragnehmer im Rahmen der in diesem SLA geregelten Leistungen umzusetzen sind,
- die Prüfung auf Notwendigkeit zur Erstellung eines Datenschutzkonzepts und ggfs. Erstellung desselben,
- die Wahrung der Rechte der Betroffenen insbes. des Rechts auf Berichtigung, Löschung, Einschränkung,
- die Einhaltung von Löschfristen und zulässiger Speicherdauer.

Die datenschutzrechtliche Verantwortung des Auftragnehmers zur Umsetzung der Maßnahmen gemäß Art. 32 und 28 DSGVO ist auf den in diesem SLA geregelten Leistungsumfang beschränkt.

### 2.1.3 Virenschutz

Der Auftragnehmer gewährleistet für die dSecureCloud Infrastruktur einen Virenschutz.

Für die vom Auftraggeber betreuten virtuellen Server ist der Virenschutz innerhalb der dSecureCloud optional.

Aufgaben und Zuständigkeiten	Auftrag-nehmer	Auftrag-geber
Virenschutz der dSecureCloud Infrastruktur	V, D, B	I
Bereitstellung des Virenschutzagenten der virtuellen Server innerhalb der dSecureCloud	V, I, B	D
Betrieb und Betreuung des Virenschutzagenten auf virtuellen Server innerhalb der dSecureCloud		V,D,B

### 2.1.4 Monitoring

Die virtuellen Server des Auftraggebers innerhalb der dSecureCloud unterliegen nicht dem Monitoring des Auftragnehmers. Der Auftraggeber ist eigenverantwortlich für den Zustand und den störungsfreien Betrieb seiner Server.

Die Überwachung für die dSecureCloud Infrastruktur werden vom Auftragnehmer betreut und gewährleistet.

Aufgaben und Zuständigkeiten	Auftrag-nehmer	Auftrag-geber
Monitoring der dSecureCloud Infrastruktur	V, D, B	I
Steuerung und Überwachung der virtuellen Systeme. Proaktives Erkennen und Vermeiden von Störungen	I	V, D

### 2.1.5 Verfügbarkeit

Der Auftraggeber hat gegenüber dem Auftragnehmer keinerlei Verfügbarkeitsansprüche auf seine in der dSecureCloud eigenadministrierten Server.

Die Verfügbarkeit der dSecureCloud Infrastruktur wird analog zum Standard des Dataport Servicekatalogs zugesichert.

### 2.1.6 Zugang

Für die eigenadministrierten Server des Auftraggebers können ab Bereitstellung vom Auftraggeber Netz-Freischaltungen vorgenommen werden.

Es wird kein Zugang zu einer Administrationsplattform benötigt.

### 2.1.7 Netzkommunikation

Die Erreichbarkeit für die vom Auftraggeber in der dSecureCloud betreuten virtuellen Server ist ab Bereitstellung initial nur untereinander möglich.

Zusätzliche Freischaltungen müssen beim Dataport Policymanagement eingereicht werden und unterliegen einem Genehmigungsvorbehalt (siehe 3.4.2).

Aufgaben und Zuständigkeiten	Auftrag-nehmer	Auftrag-geber
Erreichbarkeit der virtuellen Server innerhalb der dSecureCloud Infrastruktur	V, I	D
Beantragung zusätzlicher Freischaltungen	I	V, D
Umsetzung zusätzlicher Freischaltung nach erfolgter Prüfung	V, D	I



### **2.1.8 Verschlüsselung**

Für die Wahrung der Vertraulichkeit der vom Auftraggeber in der dSecureCloud verarbeiteten Daten ist ausschließlich der Auftraggeber verantwortlich; dieser hat eine ggfs. erforderliche Verschlüsselung eigenverantwortlich vorzunehmen. Sofern die vom Auftraggeber in der dSecureCloud verarbeiteten Daten aus Gründen der Sicherheit oder des Geheimschutzes eine Verschlüsselung erfordern, ist der Auftraggeber hierfür verantwortlich.

### **2.1.9 Authentisierung**

Die Authentisierung der vom Auftraggeber betriebenen virtuellen Server innerhalb der dSecureCloud erfolgt mittels lokaler Benutzer-Accounts. Weitere Authentisierungsdienste werden nicht angeboten.

### **2.1.10 Löschung von Daten**

Im Falle einer Vertragskündigung ist der Auftraggeber dafür verantwortlich, die von ihm in der dSecureCloud gespeicherten Daten rechtzeitig vor Beendigung des Vertrages zu sichern. Unabhängig vom Kündigungsgrund und von der Vertragspartei, welche die Kündigung ausgesprochen hat, löscht der Auftragnehmer unverzüglich alle Daten des Auftraggebers, einschließlich der eventuell noch gemäß Tz 3.4.1 vorhandenen Datensicherungen..

Eine Wiederherstellung von Daten ist nach dieser Löschung ausgeschlossen.

Ausgenommen von der Löschung sind Daten, die vom Auftragnehmer zu Abrechnungszwecken über diese Frist hinaus benötigt werden oder soweit sie einer gesetzlichen Aufbewahrungspflicht unterliegen.

Für die Löschung der betriebenen virtuellen Server innerhalb der dSecureCloud während der Vertragslaufzeit ist der Auftraggeber verantwortlich.

### **2.1.11 Offenlegung von Daten des Auftraggebers**

Der Auftragnehmer wird Daten, die der Kunde in der dSecureCloud gespeichert hat, Dritten (insbesondere Strafverfolgungsbehörden) nur offenlegen, sofern der Auftragnehmer hierzu gesetzlich verpflichtet ist. Ist der Auftragnehmer gesetzlich zur Offenlegung verpflichtet, wird er den Auftraggeber unverzüglich darüber informieren und ihm eine Kopie der Verfügung (z.B. Anordnung zur Beschlagnahme oder Durchsuchung) zukommen lassen, sofern dies nicht gesetzlich verboten ist. Der Auftragnehmer ist gegenüber dem Auftraggeber nicht zur Einlegung von Rechtsbehelfen oder Rechtsmitteln gegen solche Verfügungen verpflichtet.

### **2.1.12 Berichtswesen und Rechnungsstellung**

Der Auftragnehmer stellt über das Self-Service-Portal ein automatisiertes Berichtswesen dem Auftraggeber zur Verfügung. Der aktuelle Ressourcenverbrauch und die entstandenen Aufwände sind jederzeit einsehbar.

Die Rechnungsstellung erfolgt kalendermonatlich nachträglich. Auf der Rechnung werden nur die im Leistungszeitraum entstandenen Gesamtaufwände je im Preisblatt (Anlage 2) angegebener Position ausgewiesen.

### **2.1.13 Protokollierung**

Innerhalb des Self-Service-Portals findet eine Protokollierung statt. Durch Firewalls geblockte Netzwerkkommunikation wird ebenfalls protokolliert.

Eine regelmäßige Auswertung erfolgt nicht, sondern nur im Bedarfsfall, wie zum Beispiel dem Verdacht, dass ein Sicherheitsrisiko (s. 2.1.1) vorliegt.

## **2.2 Leistungsgegenstand**

### **2.2.1 Leistungsmerkmale eines virtuellen Servers in der dSecureCloud**

Die Leistungsmerkmale der virtuellen Server in der dSecureCloud können im Benutzerhandbuch auf der Kundenportalseite eingesehen werden.

### **2.2.2 Betriebssysteme in der dSecureCloud**

Die verfügbaren Betriebssysteme der virtuellen Server in der dSecureCloud können im Benutzerhandbuch auf der Kundenportalseite eingesehen werden.

Es werden nur Betriebssysteme bereitgestellt, die sich im regelhaften Support durch den Hersteller befinden. Die Versionen werden vom Auftragnehmer regelmäßig aktualisiert und sind im Self-Service-Portal einsehbar. Bereits bereitgestellte Betriebssysteme können auch nach Entfernung aus dem Self-Service-Portal weiterbetrieben werden, sofern sie keine Gefahr für andere Systeme darstellen (s. 2.1.1).

## **2.3 Mitwirkungsleistungen und Pflichten des Auftraggebers**

Die Mitwirkungsleistungen, Beistelleleistungen und Pflichten des Auftraggebers sind in den jeweiligen Abschnitten der Leistungsbeschreibung und optionalen Leistungen ausgewiesen.

Der Auftragnehmer weist darauf hin, dass das BSI die Erstellung einer Cloud-Sicherheitsrichtlinie für Cloud-Nutzer durch den Auftraggeber empfiehlt.

Zusätzlich gelten für den Auftraggeber folgende Pflichten:

- a) Der Auftraggeber versichert, dass er und diejenigen, die über ihn, in seinem Auftrag, mit seinem Wissen oder seiner Duldung die dSecureCloud nutzen oder auf diese zugreifen können, keine Inhalte auf dem vertragsgegenständlichen Speicherplatz speichern und in das Internet einstellen werden, deren Bereitstellung, Veröffentlichung oder Nutzung gegen geltendes Recht oder Rechte Dritter oder behördliche Anordnungen verstößt; dies gilt insbesondere für ehrverletzende, volksverhetzende oder rechtsradikale Inhalte sowie für die Verbreitung von Spam oder Malware.
- b) Der Auftraggeber prüft eigenverantwortlich die Einhaltung aller für ihn im Zusammenhang mit der Nutzung der Leistung relevanten und anwendbaren rechtlichen Vorschriften, Gesetze und Verordnungen und stellt deren Einhaltung sicher.
- c) Der Auftraggeber ist verpflichtet die Betriebssysteme und Applikationen innerhalb seiner virtuellen Maschinen gegen Angriffe Dritter und Missbrauch zu schützen, sowie frei von Schadsoftware zu halten.

- d) Der Auftraggeber ist verpflichtet innerhalb seiner virtuellen Maschinen die VMwareTools oder openVMTools für die Gastbetriebssystemunterstützung nur nach Aufforderung oder nach Zustimmung durch den Auftragnehmer zu deinstallieren.
- e) Der Auftraggeber ist für die Einhaltung von Lizenzanforderungen hinsichtlich der von ihm oder auf seine Veranlassung in der dSecureCloud installierten Software verantwortlich. Er hält Dataport diesbezüglich von jeglichen Ansprüchen Dritter frei.
- f) Der Auftraggeber verpflichtet sich, zu prüfen, ob für die von ihm auf dem dSecureCloud-Server gespeicherten Daten, ein Datenschutzkonzept notwendig ist und bei Bedarf ein solches zu erstellen.

Ein Verstoß des Auftraggebers gegen die in diesem SLA geregelten Pflichten berechtigt Dataport, den Vertrag mit sofortiger Wirkung zu kündigen und die vom Kunden in der dSecureCloud gespeicherten Daten nach Maßgabe von Tz 2.1.10 zu löschen.

### 3 Leistungsbeschreibung

---

#### 3.1 Anforderungen an die Infrastruktur des Auftraggebers

Für den Fall, dass sich die Anforderungen an die dezentrale Infrastruktur ändern, gehen die dadurch erforderlich werdenden Anpassungen zu Lasten des Auftraggebers. Der Auftraggeber stellt sicher, dass seine dezentrale Infrastruktur den laufenden Betrieb ermöglicht.

##### 3.1.1 Netzwerk-Anbindung und Firewall

Für Dienststellen der Verwaltung der Dataport-Träger wird ein Zugang zum jeweiligen Landesnetz vorausgesetzt.

#### 3.2 Lizenzleistungen

Der Auftragnehmer gewährleistet die Lizenzleistung für die jeweilig zur Verfügung stehenden Betriebssysteme (s.2.2.2). Für alle weiteren Lizenzleistungen ist der Auftraggeber verantwortlich.

Aufgaben und Zuständigkeiten	Auftrag-nehmer	Auftrag-geber
Betriebssystemlizenzen	V,D	
Lizenzen für optional angebotene Dienste Datensicherung und Virenschutz, sofern genutzt	V,D	
Fachanwendung		V, D
Middleware		V, D
Zusätzliche Lizenzen		V, D

#### 3.3 Leistungsabgrenzung

Der Zugang zu den Dataport Basisdiensten für die virtuellen Server des Auftragsgebers innerhalb der dSecureCloud sowie die Administration dieser virtuellen Server durch den Auftragnehmer sind nicht Bestandteil dieser Leistungsbeschreibung.

Seitens des Auftragnehmers werden keine weiteren Serverrollen (z.B. Datenbanken, Webservices etc.) bereitgestellt und/oder betreut.



Störungen innerhalb der automatisiert erstellten Anwender-VMs unterliegen nicht dem Support von Dataport. Störungsmeldungen für die dSecureCloud Infrastruktur, inkl. des Self-Service-Portals, können über den User Help Desk eröffnet werden. Siehe hierzu Punkt 4.

### 3.4 Optionale Leistungen

Die nachfolgenden Leistungen können von allen Auftraggebern zusätzlich zu den Basisleistungen gebucht werden:

#### 3.4.1 Datensicherung

Als optionale und zusätzlich zu berechnende Leistung bietet der Auftragnehmer innerhalb der dSecureCloud eine Datensicherung für die vom Auftraggeber eigenadministrierten Server an.

Die Option der Datensicherung kann bei der Neuerstellung eines vom Auftraggeber betreuten Servers oder auch bei einem in der dSecureCloud bestehenden System aktiviert werden.

Die Aufbewahrungszeit der Datensicherung beträgt 30 Tage. Ein Restore kann nur für den gesamten virtuellen Server angewendet werden, nicht jedoch auf Fileebene.

Eine Serverwiederherstellung kann der Auftraggeber über das Self-Service-Portal eigenständig durchführen.

Aufgaben und Zuständigkeiten	Auftragnehmer	Auftraggeber
Definition von Backup Anforderungen und Aufbewahrungszeiträumen	V, D	I
Definition von Backup mit Zeitplänen, Vorgehensweisen, Parametern	V, D	I
Aktivierung der Full-VM Sicherung		V, D
Durchführung der Datensicherung	V, D	I
Durchführung von Recovery Maßnahmen entsprechend der bestehenden Richtlinien		V, D

#### 3.4.2 Erweiterte Netzkommunikation

Die selbstadministrierten Server des Auftraggebers innerhalb der dSecureCloud sind untereinander erreichbar. Für den Fall, dass die einfache Netzkommunikation nicht ausreicht und eine Kommunikation in erweiterte Bereiche notwendig wird, steht dem Auftraggeber die optionale Möglichkeit einer erweiterten Netzkommunikation zur Verfügung.

Die erweiterte Netzkommunikation muss über zusätzliche Freischaltungen beim Dataport Policymanagement eingereicht werden und unterliegt einem Genehmigungsvorbehalt. Für die Beantragung einer erweiterten Netzkommunikation entstehen keine weiteren Aufwände. Für umzusetzende Maßnahmen können zusätzliche Aufwände entstehen, die nicht Bestandteil dieser Vereinbarung sind.

#### 3.4.3 Zusatzservice Erreichbarkeit über öffentliche Netzwerke

Die Server der dSecureCloud sind in ihrer Standard-Konfiguration nur über die Landesnetze erreichbar. Für Zugriffe von außerhalb der Landesnetze kann für jede virtuelle Maschine zusätzlich ein erweiterter Service, der die Erreichbarkeit über öffentliche Netzwerke sowie die Filterung mittels virtueller Firewalls



sicherstellt, bestellt werden. In diesem ist weiterhin die optionale Buchung eines öffentlichen DNS-Eintrags enthalten.

Es kann zu einer Änderung der öffentlichen IP-Adressen kommen. In dem Fall wird der Auftragnehmer den Auftraggeber rechtzeitig informieren. Alle hieraus in der dSecureCloud Infrastruktur entstehenden Aufwände sind vom Auftragnehmer selbstständig durchzuführen. Notwendige Massnahmen im Betriebssystem des virtuellen Servers obliegen dem Auftraggeber.

### 3.4.4 Virenschutz

Für die vom Auftraggeber betreuten virtuellen Server ist der Virenschutz innerhalb der dSecureCloud optional. Der Auftraggeber entscheidet eigenverantwortlich, ob er den Service vom Auftragnehmer nutzen möchte.

Die Installationsquellen für den Virenschutzclient werden jedem Auftraggeber auf ihren eigen-administrierten Servern zur Installation bereitgestellt. Das Angebot ist im Service enthalten und unterliegt keiner gesonderten Berechnung.

## 4 Leistungskennzahlen

---

### 4.1 Leistungsausprägung

#### 4.1.1 Betriebszeiten

##### 4.1.1.1 Onlineverfügbarkeit

Die zentrale Infrastruktur steht ganztägig zur Verfügung, d.h. an sieben Tagen in der Woche, 24 Stunden pro Tag – ausgenommen der unten angegebenen Einschränkungen (z.B. Wartungsfenster).

##### 4.1.1.2 Servicezeit - Betreuter Betrieb<sup>1</sup>

- Montag bis Donnerstag 08.00 Uhr bis 17.00 Uhr
- Freitag 08.00 Uhr bis 15.00 Uhr

In diesen Zeiten erfolgt die Überwachung und Betreuung der dSecureCloud Infrastruktur durch Administratoren des Auftragnehmers. Es stehen Ansprechpartner mit systemtechnischen Kenntnissen für den Betrieb und zur Störungsbehebung zur Verfügung. Im Problem- und Störfall wird das entsprechende Personal des Auftragnehmers über das Call-Center des Auftragnehmers informiert.

##### 4.1.1.3 Servicezeit - Überwachter Betrieb

- alle Zeiten außerhalb des betreuten Betriebes

Auch außerhalb des betreuten Betriebes stehen die Systeme den Anwendern grundsätzlich zur Verfügung. Die dSecureCloud Infrastruktur wird automatisiert überwacht. Festgestellte Fehler werden automatisch in

---

<sup>1</sup> Gilt nicht für gesetzliche Feiertage, sowie 24.12. und 31.12.

einem Trouble-Ticket-System hinterlegt. Ansprechpartner stehen während des überwachten Betriebes nicht zur Verfügung.

#### 4.1.2 Wartungsarbeiten

Die regelmäßigen, periodisch wiederkehrenden Wartungs- und Installationsarbeiten erfolgen i. d. R. außerhalb der definierten Servicezeiten des betreuten Betriebes. Derzeit ist ein Wartungsfenster in der Zeit von Dienstag 19:00 Uhr bis Mittwoch 06:00 Uhr definiert. In dieser Zeit werden Wartungsarbeiten durchgeführt und das Arbeiten ist nur sehr eingeschränkt möglich. In Ausnahmefällen (z.B. wenn eine größere Installation erforderlich ist) werden diese Arbeiten nach vorheriger Ankündigung zu einem anderen Zeitpunkt vorgenommen.

#### 4.1.3 Support

Der Auftragnehmer übernimmt den Support für die dSecureCloud Infrastruktur und das Self-Service-Portal.

Die automatisch durch den Auftraggeber erstellten VMs unterliegen nicht dem Support des Auftragnehmers. Der Auftragnehmer übernimmt des Weiteren keine verfahrensbezogenen fachlichen Supportleistungen.

#### 4.1.4 Störungsannahme<sup>2</sup>

Die Störungsannahme erfolgt grundsätzlich über das Call-Center/den User-Help-Desk des Auftragnehmers.

Im Rahmen der Störungsannahme werden grundsätzlich Melderdaten sowie die Störungsbeschreibung erfasst und ausschließlich für die Störungsbehebung gespeichert. Der Störungsabschluss wird dem meldenden Anwender bekannt gemacht.

#### 4.1.5 Incident-Management

Betriebsstörungen werden als Incidents im zentralen Trouble Ticket System (TTS) aufgenommen. Jeder Incident und dessen Bearbeitungsverlauf werden im TTS dokumentiert. Aus dem TTS lässt sich die Zeit der Störungsbearbeitung von der Aufnahme bis zum Schließen des Tickets mit der Störungsbehebung bestimmen.

Generell unterbrechen die Zeiten außerhalb des betreuten Betriebes die Bearbeitungszeit. Ebenso wird die Störungsbearbeitung unterbrochen durch höhere Gewalt oder durch Ereignisse, die durch den Auftraggeber oder den Nutzer zu verantworten sind (z.B. Warten auf Zusatzinformationen durch den Nutzer, Unterbrechung auf Nutzerwunsch, etc.).

Folgende Prioritäten werden für die Störungsbearbeitung im Rahmen der beauftragten Leistungen definiert:

Priorität	Auswirkung	Dringlichkeit	Bearbeitung
Niedrig (bisher 4)	Incident betrifft einzelne Benutzer. Die Geschäftstätigkeit ist nicht eingeschränkt.	Ersatz steht zur Verfügung und kann genutzt werden, oder das betroffene System muss aktuell nicht genutzt werden. Tätigkeiten, deren Durchführung durch den Incident behindert wird, können später erfolgen.	Priorität Niedrig führt zur Bearbeitung durch den Auftragnehmer und unterliegt der Überwachung des Lösungsfortschritts. Die Reaktionszeit (Beginn der Bearbeitung oder qualifizierter Rückruf) ergibt sich aus der Serviceklasse.

<sup>2</sup> Gilt nicht für gesetzliche Feiertage, sowie 24.12. und 31.12.

Mittel (bisher 3)	Wenige Anwender sind von dem Incident betroffen. Geschäftskritische Systeme sind nicht betroffen. Die Geschäftstätigkeit kann mit leichten Einschränkungen aufrechterhalten werden.	Ersatz steht nicht für alle betroffenen Nutzer zur Verfügung. Die Tätigkeit, bei der der Incident auftrat, kann später oder auf anderem Wege evtl. mit mehr Aufwand durchgeführt werden.	Priorität Mittel führt zur standardmäßigen Bearbeitung durch den Auftragnehmer und unterliegt der Überwachung des Lösungsfortschritts. Die Reaktionszeit (Beginn der Bearbeitung oder qualifizierter Rückruf) ergibt sich aus der Serviceklasse.
Hoch (bisher 2)	Viele Anwender sind betroffen. Geschäftskritische Systeme sind betroffen. Die Geschäftstätigkeit kann eingeschränkt aufrechterhalten werden.	Ersatz steht kurzfristig nicht zur Verfügung. Die Tätigkeit, bei der der Incident auftrat, muss kurzfristig durchgeführt werden.	Priorität Hoch führt zur bevorzugten Bearbeitung durch den Auftragnehmer und unterliegt besonderer Überwachung des Lösungsfortschritts. Die Reaktionszeit (Beginn der Bearbeitung oder qualifizierter Rückruf) ergibt sich aus der Serviceklasse.
Kritisch (bisher 1)	Viele Anwender sind betroffen. Geschäftskritische Systeme sind betroffen. Die Geschäftstätigkeit kann nicht aufrechterhalten werden.	Ersatz steht nicht zur Verfügung. Die Tätigkeit, bei der der Incident auftrat, kann nicht verschoben oder anders durchgeführt werden.	Priorität Kritisch führt zur umgehenden Bearbeitung durch den Auftragnehmer und unterliegt intensiver Überwachung des Lösungsfortschritts. Die Reaktionszeit (Beginn der Bearbeitung oder qualifizierter Rückruf) ergibt sich aus der Serviceklasse.

## 5 Erläuterungen

### 5.1 Begriffsfestlegungen

Begriff	Begriffsdefinition
Betriebszeit (unbetreuter Betrieb)	Die Betriebszeit ist der Zeitraum, in der die vereinbarten Ressourcen vom Auftragnehmer zur Verfügung gestellt und automatisiert überwacht werden.
Servicezeit	Servicezeiten beschreiben Zeiträume, in denen definierte Services zur Verfügung stehen.
Supportzeit (betreuter Betrieb)	Die Servicezeit „Supportzeit (betreuter Betrieb)“ beschreibt die Zeiträume, in denen die Ressourcen vom Auftragnehmer bedient und Störungen und Anfragen bearbeitet werden.
Wartungsfenster	Regelmäßiges Zeitfenster für Wartungsarbeiten an den Systemen, in dem die Systeme nicht oder nur eingeschränkt für den Auftraggeber nutzbar sind. Sollte in Sonderfällen ein größeres oder weiteres Wartungszeitfenster beansprucht werden, so erfolgt dies in direkter Absprache mit dem Auftraggeber. Der Auftraggeber wird nur in begründeten Fällen die Durchführung von Wartungsmaßnahmen einschränken. Der Auftragnehmer wird in diesen Fällen unverzüglich über sich ggf. daraus ergebenden Mehraufwand und Folgen informieren.
Ausfallzeit	Die Ausfallzeit ist die Zeitspanne, die nach Eintritt der Nichtverfügbarkeit während der zugesagten Servicezeit vergeht, bis ein System (bzw. Systemcluster) mit allen Komponenten wieder für den Regelbetrieb zur Verfügung steht. Gemessen wird die Ausfallzeit in Stunden innerhalb der vereinbarten Servicezeiten.
Reaktionszeit	Die Reaktionszeit ist die Zeitspanne innerhalb der vereinbarten Servicezeiten zwischen der Feststellung einer Störung durch den Dienstleister bzw. Meldung einer Störung durch den Auftraggeber über den vereinbarten Weg (Service Desk) bis zum Beginn der Störungsbeseitigung. Die Reaktionszeit beginnt mit der Aufnahme der Störung in das Ticketsystem des Auftragnehmers.
Messzeitraum	Der Zeitraum, auf den sich eine Leistungskennzahl bezieht und in dem die tatsächlich erbrachte Qualität der Leistung gemessen wird. Sofern nicht anders angegeben beziehen sich alle angegebenen Metriken jeweils auf einen Messzeitraum von einem Kalenderjahr.
dSecureCloud Infrastruktur	Die für den Betrieb der dSecureCloud notwendige technische Infrastruktur inkl. Self-Service-Portal.



## 5.2 Erläuterung VDBI

<b>V</b> = Verantwortlich	„V“ bezeichnet denjenigen, der für den Gesamtprozess verantwortlich ist. „V“ ist dafür verantwortlich, dass „D“ die Umsetzung des Prozessschritts auch tatsächlich erfolgreich durchführt.
<b>D</b> = Durchführung	„D“ bezeichnet denjenigen, der für die technische Durchführung verantwortlich ist.
<b>B</b> = Beratung	„B“ bedeutet, dass die Partei zu konsultieren ist und z.B. Vorgaben für Umsetzungsparameter setzen oder Vorbehalte formulieren kann. „B“ bezeichnet somit ein Mitwirkungsrecht bzw. eine Mitwirkungspflicht.
<b>I</b> = Information	„I“ bedeutet, dass die Partei über die Durchführung und/oder die Ergebnisse des Prozessschritts zu informieren ist. „I“ ist rein passiv.



# **Security Service Level Agreement**

## **für Verfahrensbetrieb Antrags- und Fallmanagement**

## 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

---

### 1.1 Leistungsgegenstand

Mit der Anlage **Security Service Level Agreement (SSLA)** wird zwischen den Vertragspartnern ergänzend vereinbart, wie die Leistungserbringung des zugrundeliegendem Betriebs- oder Servicevertrages unter Informationssicherheitsgesichtspunkten erfolgt.

Die nachfolgend beschriebenen Leistungen folgen dabei dem IT-Grundschutzstandard des Bundesamtes für Sicherheit in der Informationstechnik (BSI) unter Nutzung des Sicherheitsmanagementsystems des Auftragnehmers. Maßgeblich sind dabei die im BSI-Standard 200-1 (Managementsysteme für Informationssicherheit) sowie dem 200-2 „IT-Grundschutz-Vorgehensweise“ festgelegten Rahmenbedingungen und Anforderungen.

Ferner wird festgelegt, wie die vom Auftragnehmer in dessen Zuständigkeitsbereich getroffenen Sicherheitsanforderungen gegenüber dem Auftraggeber dokumentiert und nachgewiesen werden.

### 1.2 Aufbau des Dokumentes

**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.



## 2. Leistungsumfang und -beschreibung

---

### 2.1 Informationssicherheitsmanagementsystem (ISMS)

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

- die im IT-Sicherheits- und Datenschutzmanagementhandbuch des Auftragnehmers festgelegten und mit denen im Geschäftsverteilungsplan (GVP<sup>1</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 oder Services und stellt so die Grundlagen für den Nachweis der aktuell umgesetzten Sicherheitsanforderungen sicher.

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

<sup>2</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 Grundschutzkonformer Betrieb

Der Auftragnehmer verpflichtet sich, die vom BSI in den IT-Grundschutzkatalogen<sup>3</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-Grundschutzkataloge 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, grundschutzkonformes Sicherheitskonzept und weist dem Auftraggeber auf dieser Basis den grundschutzkonformen Betrieb nach (Sicherheitsnachweis).

Das Sicherheitskonzept beschreibt die nach IT-Grundschutz-Methodik zusammengefasste Struktur des betrachteten Informationsverbundes sowie die maßgeblichen<sup>4</sup> Sicherheitsanforderungen im Zuständigkeitsbereich des Auftragnehmers.

Der Auftragnehmer stellt die dauerhafte Umsetzung der Sicherheitsanforderungen sicher. Zu diesem Zweck prüft er 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>3</sup> Die aktuelle Version der IT-Grundschutz-Kataloge kann beim BSI abgerufen werden ([www.bsi.bund.de](http://www.bsi.bund.de)).

<sup>4</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 sind 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>5</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>5</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-Grundschatzanforderungen (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-Grundschatzes

Der IT-Grundschatz des Bundesamtes für Sicherheit in der Informationstechnik unterliegt der ständigen Fortschreibung. Hieraus kann sich z.B. bei wesentlichen Neuerungen oder Änderungen der IT-Grundschatzstandards (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>6</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>6</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>7</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>8</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>7</sup> ggf. schließt das auch die Aktualisierung der Risikoanalyse nach BSI-Standard 200-3 mit ein

<sup>8</sup> z.B. zu Verfahren, die nicht IT-Grundschutzkonform betrieben werden



## **Security Service Level Agreement - Teil B**

### **Verfahrensbetrieb Antrags- und Fallmanagement (AFM\_ML001)**

Version: 2.0.12  
Stand: 04.05.2018





## Inhaltsverzeichnis

---

<b>1.</b>	<b>Einleitung</b> .....	<b>3</b>
1.1	Gegenstand .....	3
1.2	Aufbau des Dokumentes .....	3
<b>2.</b>	<b>Leistungsumfang und -beschreibung</b> .....	<b>4</b>
<b>3.</b>	<b>Zusätzliche Maßnahmen</b> .....	<b>5</b>
3.1	Maßnahmen.....	5
<b>4.</b>	<b>Mitwirkungen</b> .....	<b>6</b>

## 1. Einleitung

---

### 1.1 Gegenstand

Gegenstand des Security Service Level Agreements (SSLA) Teil B ist die Festlegung von zusätzlichen Sicherheitsmaßnahmen, die über den im SSLA Teil A vereinbarten Maßnahmenumfang, bestehend aus A-, B- und C-Maßnahmen der IT-Grundschutzkataloge, hinausgehen.

### 1.2 Aufbau des Dokumentes

Diese Anlage enthält die folgenden Kapitel:

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

**Auflistung der ergänzenden Sicherheitsmaßnahmen (Kapitel 0):** Liste der zusätzlichen Sicherheitsmaßnahmen einschl. Kurzbeschreibung.



## **2. Leistungsumfang und -beschreibung**

---

Der Auftragnehmer verpflichtet sich, die unter Kapitel 3 aufgeführten zusätzlichen Sicherheitsmaßnahmen zusätzlich zu den im SSLA Teil A vereinbarten A-, B- und C-Maßnahmen umzusetzen, sowie die Maßnahmen im Sicherheitskonzept zu dokumentieren (Modellierung) und regelmäßig im Rahmen der Grundschutzerhebung zu prüfen.

Sofern Maßnahmen aufgeführt werden, die nicht im Verantwortungsbereich des Auftragnehmers liegen, werden diese entsprechend ausgewiesen. Die Umsetzung, Dokumentation und regelmäßige Überprüfung dieser Maßnahmen erfolgt in durch den Auftragnehmer.

Die im SSLA Teil A festgelegten Rahmenbedingungen (Dokumentation, Leistungserbringung, Leistungsvoraussetzungen, etc.) gelten analog.

### **3. Zusätzliche Maßnahmen**

---

#### **3.1 Maßnahmen**

Für das Verfahren Antrags- und Fallmanagement existiert ein Sicherheitskonzept. Die zusätzlichen Maßnahmen aufgrund des Schutzbedarfes „hoch“ können dem dazugehörigen Dokument „Risikoanalyse\_AFM (AFM\_ML001)“ entnommen werden.





## **4. Mitwirkungen**

---

Der Auftraggeber stellt dem Auftragnehmer eine aussagekräftige Beschreibung der zusätzlichen Maßnahmen bereit, die vom Auftragnehmer umzusetzenden sind. Der Auftraggeber unterstützt bei der Klärung von Fragen bzgl. der entsprechenden Maßnahmen die sich im Rahmen der Umsetzung ergeben. Sofern Maßnahmen Kooperativ umgesetzt werden müssen, unterstützt der Auftraggeber den Auftragnehmer bei der Maßnahmenumsetzung.

Es gelten ferner die im SSLA Teil A genannten Mitwirkungspflichten.



## **Security Service Level Agreement - Teil B**

### **Verfahrensbetrieb Antrags- und Fallmanagement (AFM\_ML002)**

Version: 2.0.12  
Stand: 04.05.2018



## Inhaltsverzeichnis

---

<b>1.</b>	<b>Einleitung</b> .....	<b>3</b>
1.1	Gegenstand .....	3
1.2	Aufbau des Dokumentes .....	3
<b>2.</b>	<b>Leistungsumfang und -beschreibung</b> .....	<b>4</b>
<b>3.</b>	<b>Zusätzliche Maßnahmen</b> .....	<b>5</b>
3.1	Maßnahmen.....	5
<b>4.</b>	<b>Mitwirkungen</b> .....	<b>6</b>

## 1. Einleitung

---

### 1.1 Gegenstand

Gegenstand des Security Service Level Agreements (SSLA) Teil B ist die Festlegung von zusätzlichen Sicherheitsmaßnahmen, die über den im SSLA Teil A vereinbarten Maßnahmenumfang, bestehend aus A-, B- und C-Maßnahmen der IT-Grundschutzkataloge, hinausgehen.

### 1.2 Aufbau des Dokumentes

Diese Anlage enthält die folgenden Kapitel:

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

**Auflistung der ergänzenden Sicherheitsmaßnahmen (Kapitel 0):** Liste der zusätzlichen Sicherheitsmaßnahmen einschl. Kurzbeschreibung.





## **2. Leistungsumfang und -beschreibung**

---

Der Auftragnehmer verpflichtet sich, die unter Kapitel 3 aufgeführten zusätzlichen Sicherheitsmaßnahmen zusätzlich zu den im SSLA Teil A vereinbarten A-, B- und C-Maßnahmen umzusetzen, sowie die Maßnahmen im Sicherheitskonzept zu dokumentieren (Modellierung) und regelmäßig im Rahmen der Grundschutzerhebung zu prüfen.

Sofern Maßnahmen aufgeführt werden, die nicht im Verantwortungsbereich des Auftragnehmers liegen, werden diese entsprechend ausgewiesen. Die Umsetzung, Dokumentation und regelmäßige Überprüfung dieser Maßnahmen erfolgt in durch den Auftragnehmer.

Die im SSLA Teil A festgelegten Rahmenbedingungen (Dokumentation, Leistungserbringung, Leistungsvoraussetzungen, etc.) gelten analog.

### **3. Zusätzliche Maßnahmen**

---

#### **3.1 Maßnahmen**

Für das Verfahren Antrags- und Fallmanagement existiert ein Sicherheitskonzept. Die zusätzlichen Maßnahmen aufgrund des Schutzbedarfes „hoch“ können dem dazugehörigen Dokument „Risikoanalyse\_AFM (AFM\_ML002)“ entnommen werden.



## **4. Mitwirkungen**

---

Der Auftraggeber stellt dem Auftragnehmer eine aussagekräftige Beschreibung der zusätzlichen Maßnahmen bereit, die vom Auftragnehmer umzusetzenden sind. Der Auftraggeber unterstützt bei der Klärung von Fragen bzgl. der entsprechenden Maßnahmen die sich im Rahmen der Umsetzung ergeben. Sofern Maßnahmen Kooperativ umgesetzt werden müssen, unterstützt der Auftraggeber den Auftragnehmer bei der Maßnahmenumsetzung.

Es gelten ferner die im SSLA Teil A genannten Mitwirkungspflichten.

**EVB-IT Dienstvertrag Vxxxxx/xxxxxxx**  
**Leistungsnachweis Dienstleistung (Seite 1 von 2)**



## Leistungsnachweis

zum Vertrag über die Beschaffung von Dienstleistungen

**Auftraggeber:**  
**Dataport Auftragsnummer:**  
**Vorhabensnummer des Kunden:**  
**Abrechnungszeitraum:**  
**Produktverantwortung Dataport:**  
**Nachweis erstellt am / um:**  
**Gesamtzahl geleistete Stunden:**

Über die Auflistung hinaus können sich noch Stunden in Klärung befinden. Diese werden mit dem nächstmöglichen Leistungsnachweis ausgewiesen.

<b>Position</b>		<b>Materialtext</b>	
Datum	Aufwand in Stunden	Kommentar	Name der / des Leistenden
		<b>Gesamtzahl geleistete Stunden für Position</b>	

**EVB-IT Dienstvertrag Vxxxxx/xxxxxxx**

**Leistungsnachweis Dienstleistung (Seite 2 von 2)**



Positionsübersicht		
Position	Positionsbezeichnung	Stunden gesamt
	<b>Gesamt</b>	

Der Leistungsnachweis ist maschinell erstellt und ohne Unterschrift gültig. Einwände richten Sie bitte per Weiterleitungs-E-Mail an die oder den zuständigen Produktverantwortliche(n) bei Dataport.

Der Leistungsnachweis gilt auch als genehmigt, wenn und soweit der Auftraggeber nicht innerhalb von 14 Kalendertagen nach Erhalt Einwände geltend macht.

Diese Daten sind nur zum Zweck der Rechnungskontrolle zu verwenden.  
**Bitte beachten: in Blau dargestellte Zeilen enthalten Umbuchungen.**