EVB-IT Dienstvertrag

Vertragsnummer/Kennung Auftraggeber _____

Vertragsnummer/Kennung Auftragnehmer: V11661-1/3016010

Vertrag über die Beschaffung von IT-Dienstleistungen

Zwischen

SIS - Senator für Inneres 101
Ref. 10, Organisation, IT, eGovernment,
Verwaltungsmodernisierung
Contrescarpe 22/24
28203 Bremen

– im Folgenden „Auftraggeber" genannt –

und

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

– im Folgenden „Auftragnehmer" genannt –

wird folgender Vertrag geschlossen:

1 Vertragsgegenstand und Vergütung

1.1 Projekt-/Vertragsbezeichnung

Verfahrensinfrastruktur des Verfahrens Führerscheinwesen im Rechenzentrum sowie technisches Verfahrensmanagement und integrierter
Dataport Oracle Service" (IDOS) – zentrale Nutzung
1. Änderung: Erweiterung Applikationsserver in der Produktivumgebung und Beauftragung SSLA

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

1.3 Die Leistungen des Auftragnehmers werden

☒ nach Aufwand gemäß Nummer 5.1

☒ zum Festpreis gemäß Nummer 5.2

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

Die zum Zeitpunkt der Leistungserbringung gültige Umsatzsteuer wird gesondert vergütet.

2 Vertragsbestandteile

2.1 Es gelten nacheinander als Vertragsbestandteile:

- dieses Vertragsformular (Seiten 1 bis 6)
- Allgemeine Vertragsbedingungen von Dataport (Dataport AVB) in der jeweils geltenden Fassung (s. 11.1)
- Vertragsanlage(n) Nr. 1, 2a, 2b, 2c, 2d, 3, 4a, 4b. 5, 6, 7 (die Reihenfolge der Anlagen ergibt sich aus Nr. 3.2.1)
- Ergänzende Vertragsbedingungen für die Erbringung von IT-Dienstleistungen (EVB-IT Dienstleistung, Fassung vom 01. April 2002)
- Vergabe- und Vertragsordnung für Leistungen – ausgenommen Bauleistungen – Teil B (VOL/B) in der bei Vertragsschluss geltenden Fassung

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

3 Art und Umfang der Dienstleistungen

3.1 Art der Dienstleistungen

Der Auftragnehmer erbringt für den Auftraggeber folgende Dienstleistungen:

3.1.1 ☐ Beratung
3.1.2 ☐ Projektleitungsunterstützung
3.1.3 ☐ Schulung
3.1.4 ☐ Einführungsunterstützung
3.1.5 ☐ Betreiberleistungen
3.1.6 ☐ Benutzerunterstützungsleistungen
3.1.7 ☐ Providerleistungen ohne Inhaltsverantwortlichkeit
3.1.8 ☒ sonstige Dienstleistungen:

gemäß Anlage 4a, 4b und 5

3.2 Umfang der Dienstleistungen des Auftragnehmers

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

☐ folgenden Teilen des Angebotes des Auftragnehmers vom

	Anlage(n) Nr.	
☒ der Leistungsbeschreibung des Auftragnehmers		
Service Level Agreement Verfahrensinfrastruktur im Dataport Rechenzentrum Teil A (allgemeiner Teil für Verfahren Führerscheinwesen (FSW_HB001)) (SLA VI RZ TeilA)	Anlage(n) Nr.	4a
Service Level Agreement Verfahrensinfrastruktur im Dataport Rechenzentrum Teil B (spezifischer Teil für Verfahren Führerscheinwesen (FSW_HB001)) (SLA VI RZ TeilB)		4b
Security Service Level Agreement Grundschutzkonformer Verfahrensbetrieb Führerscheinwesen (SSLA TeilA)		5

☒ folgenden weiteren Dokumenten:

Ansprechpartner	Anlage(n) Nr.	1
Preisblatt Aufwand ab 01.09.2019	Anlage(n) Nr.	2a
Preisblatt Festpreis ab 01.09.2019 bis 31.12.2019	Anlage(n) Nr.	2b
Preisblatt Festpreis ab 01.01.2020 bis 31.12.2020	Anlage(n) Nr.	2c
Preisblatt Festpreis ab 01.01.2021	Anlage(n) Nr.	2d
Selbstauskunft Auftraggeber zur Auftragsverarbeitung	Anlage(n) Nr.	3
Clientvereinbarung	Anlage(n) Nr.	6
Muster Leistungsnachweis Dienstleistung	Anlage(n) Nr.	7

Es gelten die Dokumente in

☐ obiger Reihenfolge
☒ folgender Reihenfolge: 1, 2a, 2b, 2c, 2d, 3, 4b, 4a, 5, 6, 7

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 V12909/3011005.

3.3 Vergütungsbestimmende Faktoren aus dem Bereich des Auftraggebers

Vergütungsbestimmende Faktoren aus dem Bereich des Auftraggebers sind

a) die Mitwirkungsleistungen des Auftraggebers gemäß Nummer 8

b) folgende weitere Faktoren:

4 Ort der Dienstleistungen / Leistungszeitraum

4.1 Ort der Dienstleistungen in den Räumlichkeiten des Auftragnehmers

4.2 Zeiträume der Dienstleistungen

Leistungen (gemäß Nummer 3.1)	**Geplanter Leistungszeitraum**		**Verbindlicher Leistungszeitraum**	
	Beginn	**Ende**	**Beginn**	**Ende**
V11661/3016010			01.10.2017	31.08.2019
V11661-1/3016010			01.09.2019	

4.3 Zeiten der Dienstleistungen

Die Leistungen des Auftragnehmers werden erbracht gemäß SLA VI RZ Teil A Pkt. 2.2, SLA VI RZ Teil B Pkt. 2.1

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

_____ bis _____ von _____ bis _____ Uhr
_____ bis _____ von _____ bis _____ Uhr

4.3.2 während sonstiger Zeiten

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

5 Vergütung gem. Preisblatt Anlage 2a-d und Leistungsnachweis Dienstleistung

5.1 ☒ Vergütung nach Aufwand

mit einer Obergrenzenregelung gemäß Anlage 2a

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

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

Reisezeiten

☒ Reisezeiten werden nicht gesondert vergütet.

☐ Reisezeiten werden vergütet gemäß Anlage

Rechnungsstellung
Die Rechnungsstellung erfolgt gemäß Anlage 2a.

Vergütungsvorbehalt

Es wird ein Vergütungsvorbehalt vereinbart

☐ gemäß Ziffer 6.4 EVB-IT Dienstleistung

☒ gemäß Ziffer 3.1 der Dataport AVB

☐ anderweitige Regelung gemäß Anlage Nr. .

5.2 ☒ **Festpreis**

Der der **jährliche Festpreis** setzen sich gemäß Anlage 2b-d zusammen.

Die Rechnungsstellung des jährlichen Festpreises erfolgt gemäß Anlage 2b-d.

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

☐ Es werden folgende Abschlagszahlungen vereinbart: gemäß Anlage

5.3 Reisekosten und Nebenkosten

☒ Reisekosten werden nicht gesondert vergütet

☐ Reisekosten werden vergütet gemäß Anlage

☒ Nebenkosten werden nicht gesondert vergütet

☐ Nebenkosten werden vergütet gemäß Anlage

6 Rechte an den verkörperten Dienstleistungsergebnissen

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

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

_____

_____

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

_____

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

6.4 ☐ Sonstige Nutzungsrechtsvereinbarungen

_____

7 Verantwortlicher Ansprechpartner siehe Anlage 1

des Auftraggebers: _____

des Auftragnehmers: _____

8 Mitwirkungsleistungen 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 [redacted] zu senden.

8.3. gemäß Anlage SLA RZ VI Teil A Pkt. 1.2, SLA VI RZ Teil B Pkt. 1.4 und SSLA TeilA Pkt. 5.2

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, die EVB-IT Dienstleistungs-AGB unter www.cio.bund.de und die VOL/B unter www.bmwi.de zur Einsichtnahme bereit.

11.2 Umsatzsteuer

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

11.3 Verschwiegenheitspflicht

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

11.4 Bremer Informationsfreiheitsgesetz

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

11.4.2 ☐ Optionale Erklärung der Nichtveröffentlichung

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

11.5 Besondere Leistungsmerkmale
Oracle IDOS:

Die Vergütung der in Anlage 2b, 2c und 2d aufgeführten Oracle IDOS Leistungen erfolgt durch den Zentralfinanzierungsvertrag mit dem Auftragnehmer.

11.6 Laufzeit und Kündigung

Dieser Vertrag beginnt am 01.09.2019. 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 Monaten zum 31.12.2021 gekündigt werden. Danach kann er zum Ende eines Kalenderjahres unter Wahrung einer Frist von 6 Monaten gekündigt werden. Die Kündigung bedarf der Textform.

11.7 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.

Bremen	_____	Bremen	09.12.2020
Ort	Datum	Ort	Datum

[redacted]

Ansprechpartner
zum Vertrag über die Beschaffung
von IT-Dienstleistungen
Verfahrensinfrastruktur des Verfahrens Führerscheinwesen im Rechenzentrum sowie technisches Verfahrensmanagement und integrierter Dataport Oracle Service“ (IDOS) – zentrale Nutzung
1. Änderung: Erweiterung Applikationsserver in der Produktivumgebung und Beauftragung SSLA

Vertragsnummer/Kennung Auftraggeber:

Auftraggeber:
SIS - Senator für Inneres 101
Ref. 10, Organisation, IT, eGovernment, Verwaltungsmodernisierung
Contrescarpe 22/24
28203 Bremen

Rechnungsempfänger:
Freie Hansestadt Bremen
- Rechnungseingang FHB -
Senator für Inneres

28026 Bremen

Leitweg-ID: [redacted]

Der Rechnungsempfänger ist immer auch der Mahnungsempfänger.

Zentraler Ansprechpartner des Auftragnehmers:

Vertraglicher Ansprechpartner des Auftraggebers:

Fachliche Ansprechpartner des Auftraggebers:

Technische Ansprechpartner des Auftraggebers:

[redacted]

Herr/Frau
Tel.:
Email:

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

Ort , Datum

Preisblatt (für Aufwände)

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

mit einer jährlichen Obergrenze von 10.000,00 €.

[redacted]

Die Abrechnung erfolgt nach Aufwand.

Die Rechnungsstellung der Position 10 erfolgt kalendermonatlich nachträglich gem. Leistungsnachweis.

Die Rechnungsstellung der Position 20 erfolgt nach Bereitstellung.

Die Rechnungsstellung der Position 30-50 erfolgt ab 01.01.2020 gemäß
Anlage 2c und ab 01.01.2021 gemäß Anlage 2d.

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.

Preisblatt

Für die vom Auftragnehmer zu erbringenden Dienstleistungen
zahlt der Auftraggeber einen **jährlichen Festpreis (nachrichtlich)** bestehend aus

Preise ohne Personalkostenzuschlag:	93.288,53 €
Personalkostenzuschlag gesamt:	807,35 €
Gesamtpreis:	**94.095,88 €**

Der verbindliche **Preis** setzt sich wie folgt zusammen:

verbindliche Leistungen gemäß Dataport-Servicekatalog

[redacted]

[redacted]

Die Rechnungsstellung des Festpreises erfolgt zum 15.06. eines Kalenderjahres.

Preisblatt

Für die vom Auftragnehmer zu erbringenden Dienstleistungen
zahlt der Auftraggeber einen **jährlichen Festpreis (nachrichtlich)** bestehend aus

Preise ohne Personalkostenzuschlag:	93.763,43 €
Personalkostenzuschlag gesamt:	807,35 €
Gesamtpreis:	**94.570,78 €**

Der verbindliche **Preis** setzt sich wie folgt zusammen:

verbindliche Leistungen gemäß Dataport-Servicekatalog

[redacted]

[redacted]

Die Rechnungsstellung des Festpreises erfolgt zum 15.06. eines Kalenderjahres.

Preisblatt

Für die vom Auftragnehmer zu erbringenden Dienstleistungen
zahlt der Auftraggeber einen **jährlichen Festpreis (nachrichtlich)** bestehend aus

Preise ohne Personalkostenzuschlag:	90.346,68 €
Personalkostenzuschlag gesamt:	0,00 €
Gesamtpreis:	**90.346,68 €**

Der verbindliche **Preis** setzt sich wie folgt zusammen:

verbindliche Leistungen gemäß Dataport-Servicekatalog

[redacted]

Die Rechnungsstellung des Festpreises erfolgt zum 15.06. eines Kalenderjahres.

Vertragsnummer: V11661-1/3016010
Auftraggeber: _____

Selbstauskunft Auftraggeber über Auftragsverarbeitung

Angaben zum Vertrag über Auftragsverarbeitung

Für die Verarbeitung der in Rede stehenden personenbezogenen Daten gelten folgende Datenschutzregelungen:	Zutreffendes ankreuzen
Verordnung (EU) 2016/679 (DSGVO) und gfls. ergänzende landesrechtliche Regelungen	☑
Nationale Regelungen (Landesdatenschutzgesetz bzw. Bundesdatenschutzgesetz) zur Umsetzung der RiLi (EU) 2016/680 (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)	☑
Es findet keine Verarbeitung personenbezogener Daten statt	☐

Angaben zum Gegenstand der Auftragsverarbeitung [1]

Eine Erläuterung zu den nachfolgend zu machenden Angaben findet sich z. B. hier:
https://www.lda.bayern.de/media/dsk_hinweise_vov.pdf

1.	**Art und Zweck der Verarbeitung** (siehe z. B. Art. 28 Abs. 3 S. 1 DSGVO)
	Fahrerlaubnisregister einschl. elektronische Archivierung

2.	**Beschreibung der Kategorien von personenbezogenen Daten** (siehe z. B. Art. 28 Abs. 3 S. 1 DSGVO bzw. Art. 30 Abs. 1 S. 2 lit. c)
	personenbezogene und fahrerlaubnisrechtliche Daten von Fahrerlaubnisbewerber_innen und Fahrerlaubnisinhaber_innen und Personen, denen ein Verbot erteilt wurde, ein Fahrzeug zu führen, soweit dies zur Erfüllung der gesetzlichen Bestimmungen erforderlich ist
	darunter Kategorien besonderer personenbezogener Daten (siehe z. B. Art. 9 Abs.1 DSGVO)
	im Einzelfall Angaben über die Gesundheit einer Person

3.	**Beschreibung der Kategorien betroffener Personen** (siehe z. B. Art. 28 Abs. 3 S. 1 DSGVO)
	Fahrerlaubnisinhaber_innen, Fahrerlaubnisbewerber_innen sowie Personen, denen die Fahrerlaubnis entzogen bzw. ein Verbot erteilt wurde, ein Fahrzeug zu führen.

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

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

Anhang zur Anlage Nr. 3 V11661-1/3016010

Liste der weiteren Auftragsverarbeiter

Anlage 4a zum V11661-1/3016010

Service Level Agreement

Verfahrensinfrastruktur im Dataport Rechenzentrum

Teil A – Allgemeiner Teil - für Verfahren Führerscheinwesen (FSW_HB001)

für

SIS Senator für Inneres
Ref.10 Organisation, IT, e Government
Verwaltungsmodernisierung
Contrescarpe 22/24
28203 Bremen

nachfolgend Auftraggeber

Inhaltsverzeichnis

1 Einleitung

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

1.1 Aufbau des Dokumentes

Diese Anlage enthält nach der Einleitung die folgenden Kapitel:

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

1.2 Allgemeine Mitwirkungsrechte und –pflichten

Die von Dataport zugesagten Leistungen erfordern Mitwirkungs- und Beistellleistungen 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.

- [redacted]

[redacted]

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 [redacted]

Für alle Services gilt einheitlich die Supportzeit [redacted] 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	-
	(ohne die für Schleswig-Holstein gültigen gesetzlichen Feiertage und ohne 24.12., 31.12.)		

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

2.2.3 Störungsannahme

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

[redacted]

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

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

2.2.4 Personendaten der Nutzer für die Störungsannahme

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

2.2.5 Changemanagement und Patchmanagement

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

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

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

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

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

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

2.2.6 Zeitfenster für Sicherheitsupdates

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

2.3 Serviceübergreifende Leistungskennzahlen (KPIs)

2.3.1 Reaktionszeit

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

Störungspriorität[1]	Reaktionszeiten
Kritisch (1)	[redacted]
Hoch (2)	
Mittel (3)	
Niedrig (4)	

Die vereinbarte Zielwahrscheinlichkeit P_{Soll} für die Erreichung der Reaktionszeiten pro Kalendermonat beträgt [redacted]

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 Middelwarekomponenten 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.

[1] Für eine detaillierte Definition siehe Ziffer 4 in diesem Dokument

3 Rollendefinition

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

Rolle	Rollendefinition
Auftraggeber (AG)	Rolle des Auftraggebers im Sinne der DSGVO
Auftragsverabeiter (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 Dienstleitung 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 Verfahrens-management (FVM)	Das fachliche Verfahrensmanagement umfasst administrative Tätigkeiten innerhalb der Verfahrenssoftware (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
Leistungsübergabe-punkt (LÜP)	Bezugspunkt der Definition von Service Leveln. Die Services werden dem Auftraggeber am LÜP zur Verfügung gestellt. Einflüsse auf die Servicequalität ab LÜP sind nicht Bestandteil der vom Auftragsverarbeiter zugesagten Leistungen. Analog sind die Details der Serviceerbringung durch den Auftragsverarbeiters bis zum LÜP alleine unter der Verantwortung des AV.
Operational Level Agreement (OLA)	Dataport-interne Beschreibung von Leistungen nach ihrer Qualität und Ausprägung. Zweck ist die interne Absicherung der nach außen bzw. gegenüber dem Auftraggeber zugesagten Service Levels.
Reaktionszeit	Die Reaktionszeit ist die Zeitspanne zwischen der Meldung einer Störung über den vereinbarten Störmeldeweg und dem Beginn der inhaltlich qualifizierten Bearbeitung durch Dataport. Zur Messung der Reaktionszeit wird der Zeitpunkt der Störungsmeldung und der Status „in Bearbeitung" in der ITSM Suite bei Dataport verwendet. Die Reaktionszeit ist grundsätzlich abhängig von der Priorität der Störung. Je nach SLA-Klasse im Servicekatalog sind die Prioritäten „kritisch" oder „hoch" evtl. nicht verfügbar.
Twin Data Center	Dataport Rechenzentren in Alsterdorf und Norderstedt
Security Service Level Agreement (SSLA)	Ergänzung eines SLA zur Verfahrensinfrastruktur. Mit dem Security Service Level Agreement wird zwischen den Vertragspartnern vereinbart, wie der Betrieb unter Informationssicherheitsgesichtspunkten auf Basis des IT-Grundschutzes des Bundesamtes für Informationssicherheit (BSI) unter Nutzung des Sicherheitsmanagementsystems des Auftragsverarbeiters erfolgt.
Service	Standardisierte Bündelung von Leistungen; aufgeführt im Servicekatalog und relevant für die Preisgestaltung
Service Desk	Das Service Desk ist die Anlaufstelle für die Nutzer, d.h. alle Störungen werden hier zunächst angenommen und bearbeitet. Regelhaft wird diese Aufgabe vom Callcenter übernommen

Begriff	Definition
Service Fernzugriff Administrativ (SFA)	Der Service stellt dem Auftraggeber für administrative Aufgaben personalisierte Accounts zur Verfügung und beinhaltet folgende Leistungen: • Einrichtung von Accounts für Administratoren des Auftraggebers • Bereitstellung der Infrastruktur für den Administrativen Zugang einschließlich der Lizenzkosten für Clientkomponenten • Durchführung der ITIL Prozesse durch Dataport • Technische Beratungsleistung für die Umsetzung der administrativen Aufgaben (z.B. Anmeldung, Administration eines Servers,...) 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.
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. $\text{Verfügbarkeit}_{Ist} \geq \text{Verfügbarkeit}_{Soll}$; $\text{Reaktionszeit}_{Ist} \leq \text{Reaktionszeit}_{Soll}$).
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	Die Supportzeit Standard beschreibt den Zeitraum, in dem Störungen und Anfragen entgegengenommen werden und auf sie reagiert wird. In der erweiterten Supportzeit werden nur Störungen entgegengenommen und bearbeitet. Die Supportzeit liegt innerhalb der Betriebszeit und kann sich auch über das Wartungsfenster erstrecken
Technisches Verfahrens-management (TVM)	Das technische Verfahrensmanagement umfasst administrative Tätigkeiten in systemnaher Software (Middleware ober 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.
User Help Desk (UHD)	Der User Help Desk ist eine besondere Ausprägung des Service Desk bei Dataport bei entsprechender gesonderter vertraglicher Grundlage. 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.
Verfahren	Die IT-Unterstützung für die Durchführung von Fachaufgaben des Auftraggebers

Begriff	Definition
Verfahrens-umgebungen	Verfahrensumgebungen können in folgenden Produktionsstufen bereitgestellt werden: • Schulung: Abbild der Produktivumgebung in einem geringeren Umfang. Ohne Anbindung an produktive Systeme; keine Verarbeitung von Echtdaten • Test: Umgebung für den Test neuer Softwareversionen, die i.d.R. eingekauft werden. keine Verarbeitung von Echtdaten • Entwicklung: Umgebung, auf der Software entwickelt und weiterentwickelt wird. Im Zuge dessen erfolgen auch Softwaretests auf dieser Umgebung. keine Verarbeitung von Echtdaten • Qualitätssicherung: Stellt ein Abbild der Produktivumgebung da; im Regelfall in deutlich reduzierter Skalierung. Updates des Fachverfahrens sowie Patche der Betriebssysteme oder Middelware werden auf dieser Umgebung eingespielt, um vor Produktivsetzung die Funktion zu testen; einschließlich Test der Schnittstellen. Regelhaft keine Verarbeitung von Echtdaten • Produktion: Die Umgebung auf der das Fachverfahren betrieben wird; Verarbeitung der Echtdaten
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	Zeitfenster für Wartungsarbeiten an den Systemen. Es wird zwischen dem Standard-Wartungsfenster (regelmäßig pro Woche) und besonderen Wartungsfenstern (auf gesonderte Vereinbarung) unterschieden. Das Wartungsfenster liegt in der Betriebszeit. Während des Wartungsfensters muss nicht generell von einer Nichtverfügbarkeit der Services ausgegangen werden. Jedoch sind im Wartungsfenster Serviceunterbrechungen möglich. 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.

Begriff	Definition
Zielwahrscheinlich-keit (P_{Soll})	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. Eine Zielwahrscheinlichkeit kann nur für Kennziffern angegeben werden, die in vielen Einzelmessungen oder Einzelereignissen bestimmt werden (z. B. Reaktionen auf einzelne Störungen). 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 ≤ 30 Minuten betragen müssen.

6.1 Definition der Verfügbarkeit

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

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

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 „Ecomomy“ 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 Verfügbarkeistklassen für Verfahrensinfrastrukturen zur Verfügung:

[redacted]

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

Anlage 4b zum V11661-1/3016010

Service Level Agreement

Verfahrensinfrastruktur im Dataport Rechenzentrum

Teil B (spezifischer Teil für Verfahren Führerscheinwesen (FSW_HB001))

für

SIS Senator für Inneres
Ref.10 Organisation, IT, e Government
Verwaltungsmodernisierung
Contrescarpe 22/24
28203 Bremen

nachfolgend Auftraggeber

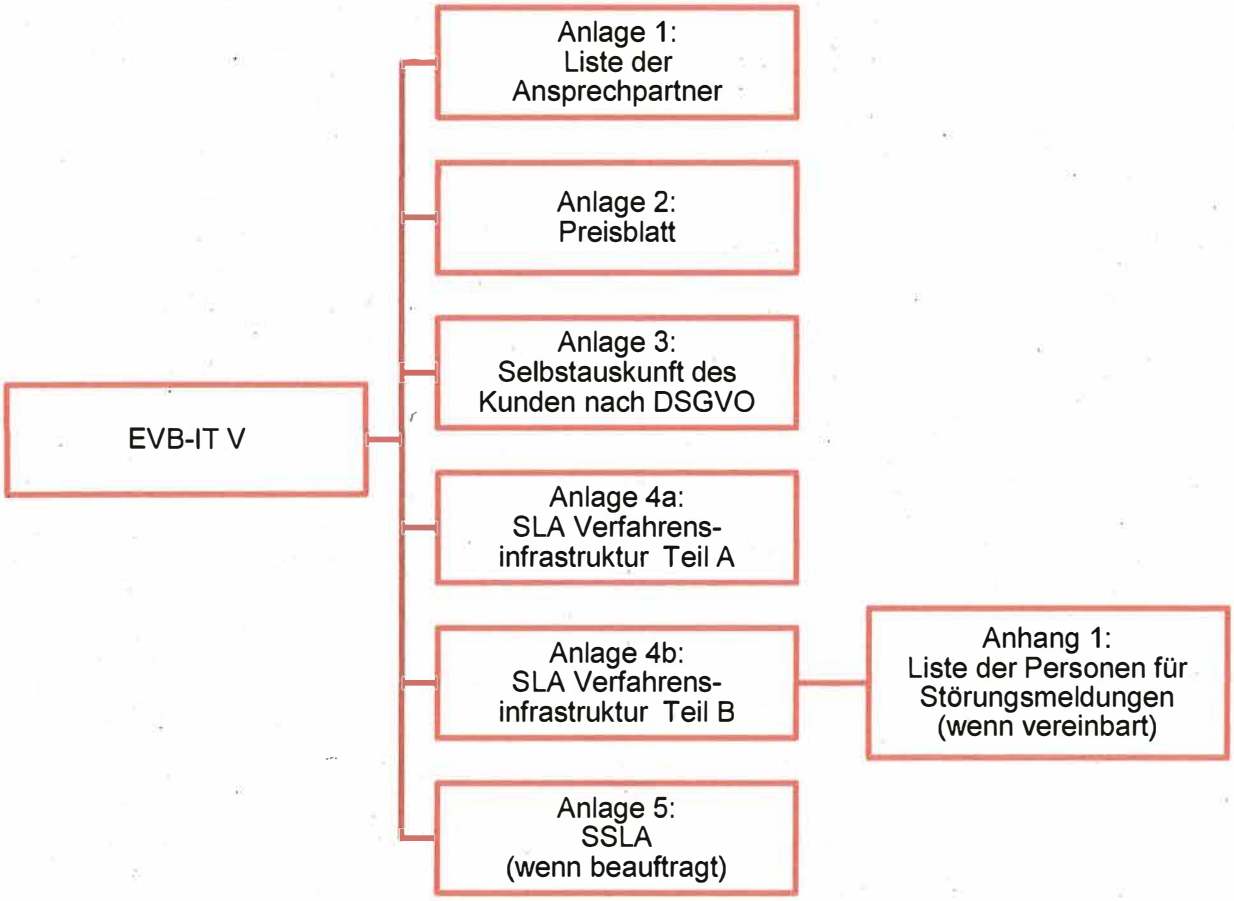
Anlage 4b zum V11661-1/3016010

Inhaltsverzeichnis

1 Einleitung

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

1.1 Einbindung des SLAs in die Vertragsstruktur



1.2 Aufbau des Dokumentes

Diese Anlage enthält nach der Einleitung die folgenden Kapitel:

- Mitwirkungsleistungen des Auftraggebers, konkrete Rollenfestlegung
- die Leistungsbeschreibung: Server-Services und TVM
- Leistungsspezifische KPIs: Ausführungen zu Kennziffern und Reporting

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

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

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

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

2 Rahmen der Leistungserbringung

2.1 Servicerelevante Regelungen

2.1.1 Supportzeiten

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

Es wird keine Erweiterte Supportzeit beauftragt.

2.1.2 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 wie folgt eingestellt:

[redacted]

Formgebundene Service-Request können nur bei vollständigen Informationen bearbeitet werden.

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

3 Leistungsbeschreibung Verfahrensinfrastruktur

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

3.1 Beschreibung des Fachverfahrens

Das Verfahren Führerscheinwesen wird für die Bearbeitung von Fahrerlaubnisdaten in der Führerscheinstelle des Stadtamts Bremen genutzt. So erfolgt beispielsweise die Bearbeitung und Aushändigung von Führerscheinen über dieses Verfahren.
Die Software wird den Anwendern über Citrix-Terminalserver bereitgestellt. In einer gemeinsamen Oracle-Instanz werden zwei Datenbanken zur Verfügung gestellt (Führerscheinwesen und „Führerscheinwesen eAkte").

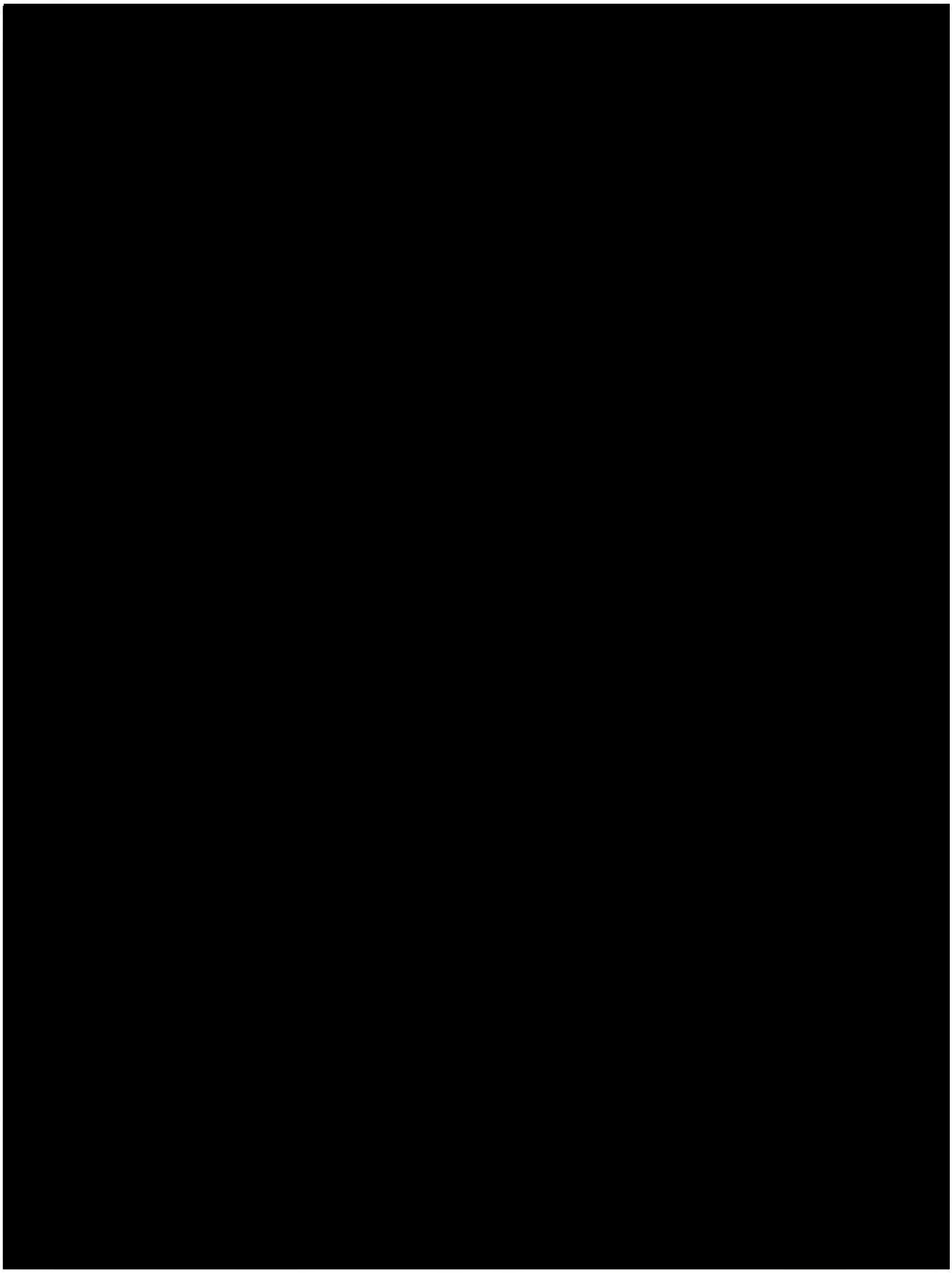
[redacted]

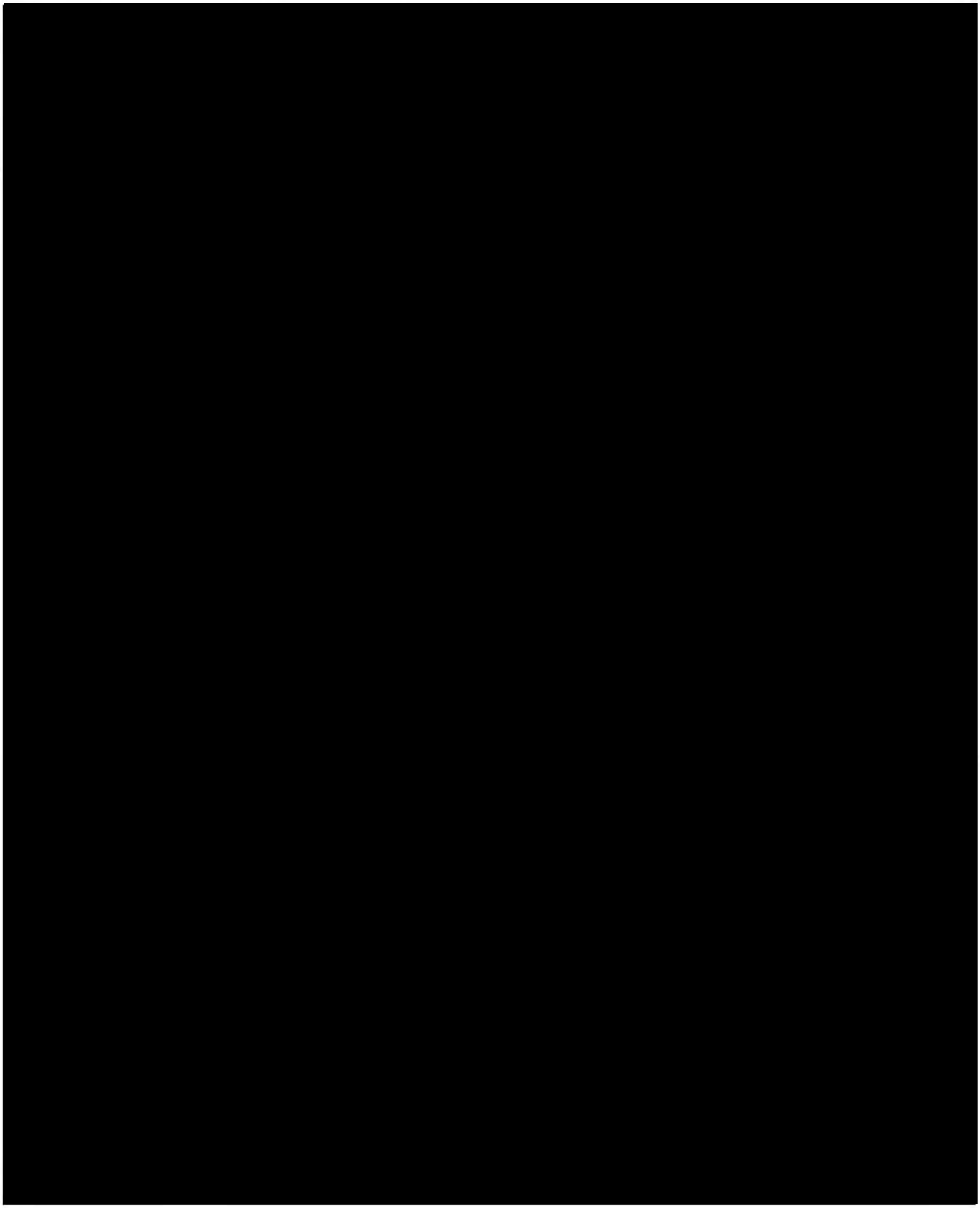
3.2 Bereitgestellte Umgebungen

[redacted]

3.3 Details zu Server-Services

Alle nachfolgenden Server-Services werden nur mit Betriebssystemen und Middleware bereitgestellt, die sich im offiziellen Herstellersupport befindet. Bei absehbarem Auslaufen des Herstellersupports wird der Auftragsverarbeiter rechtzeitig (regelhaft mit mindestens 24 Monaten Vorlaufzeit) auf den Auftraggeber zum Zweck des Updates der Verfahrensinfrastruktur zukommen.
Der Auftraggeber hat keinen Anspruch auf Weiterbetrieb von Verfahrensinfrastrukturen mit Betriebssystemen oder Middleware, für die kein Herstellersupport mehr besteht.
In den Server-Services ist ohne gesonderte Beauftragung durch den Auftraggeber eine systemtechnische Speicherleistung in ausreichender Größe für das Betriebssystem und die Middleware enthalten.





3.3.2 Spezifische Punkte zu Windows- und Citrix Terminal Services

Skalierung und Benutzerverhalten

Die Anzahl der gleichzeitigen Benutzer ergibt sich aus den aktuellen Anforderungen der Applikationskomponenten und dem aktuell angenommenen Benutzerverhalten. Die konkrete Ermittlung erfolgt im Rahmen der Erstmaligen Herstellung der Betriebsbereitschaft (EHdB) und wird in der Verfahrensdokumentation festgeschrieben. Die Ermittlung kann nicht für die gleichbleibende Performance über die Gesamtlaufzeit der Verfahrensnutzung garantieren.

Signifikante Änderungen des Benutzerverhaltens, die Einführung neuer Applikations-Module oder geänderte Systemanforderungen bestehender Applikations-Module (z. B. durch ein individuelles Customizing des Auftraggebers) beeinflussen die Performanz und erfordern ggf. eine Neuskalierung des Systems.

Die benutzerbezogene Rechenleistung (CPU) und der Arbeitsspeicher (RAM) je Benutzer orientieren sich an Durchschnittswerten. Der tatsächliche Bedarf pro Benutzer kann je nach Nutzerverhalten (insbesondere bei Nutzung des Internet Explorers) stark variieren. Auch diese Werte werden im Rahmen des EHdB ermittelt und dokumentiert.

Drucken über Terminalservices

Auf Fat-Clients (Windows) erfolgt das Drucken unter Citrix aktuell mit dem Universal Printer Driver (UPD) und unter Windows Terminalservices derzeit mit Remote Desktop Easy Print.

Für Thin-Clients bzw. Non-Windows Endgeräte erfolgt seitens des Auftragverarbeiters eine Prüfung, welche Drucklösung möglich ist. Der Betrieb ist kostenpflichtig und gesondert zu beauftragen.

Voraussetzungen auf die Clients des Auftraggebers

- **Endgerätekomponenten**

  Für die Nutzung des Dataport-Citrix-Terminal-Services wird auf den Endgeräten der Citrix Receiver, Version 4.2 oder höher, vorausgesetzt. Der Auftragverarbeiter stellt dem Auftraggeber für die Bereitstellung des Citrix-Receivers auf dem Endgerät eine Installations- und Konfigurationsanleitung zur Verfügung.

  Für die Nutzung des Dataport-Windows-Terminal-Services wird auf den Endgeräten der RDP Client, Version 7 oder höher, vorausgesetzt.

  Sofern das Endgerät von Dataport betreut wird, ist die Paketierung und Verteilung des Citrix Receivers / RDP Clients durch den Auftraggeber entsprechend der vereinbarten Prozesse zu beauftragen.

- **Netzanbindung**

  Für die Netzanbindung zum Twin Data Center wird für Citrix Terminal Services eine Bandbreite von mindestens 1,6 Mbit/s, für Windows Terminal Services von mindestens 2,5 Mbit/s je zehn gleichzeitige Nutzer benötigt. Der weitere Datenverkehr (z.B. für Dateitransfer oder zum drucken von Dokumenten) ist gesondert zu berücksichtigen.

- **Audio**

  Eine Audioübertragung bei der Nutzung des Internet Explorers wird standardmäßig nicht bereitgestellt. Sie ist kostenpflichtig und gesondert zu beauftragen.

3.3.3 Zentraler Fileservice

Für die zentrale Dateiablage wird ein zentraler Fileservice in der Größe von **10** GB bereitgestellt.

3.3.4 Fileservice Economy

Nicht Bestandteil des SLAs.

3.3.5 Application Level Gateway-Funktionalität (ALG)

Nicht Bestandteil des SLAs.

3.3.6 Backup & Recovery

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

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

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

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

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

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

3.4 Details zum Technischen Verfahrensmanagement

3.4.1 Serviceklassifikation

Für das technische Verfahrensmanagement wird folgende Ausprägung vereinbart:

Spezifikation der Leistungsklasse	[redacted]
Anzahl Benutzer (named)	
Anzahl Umgebungen	
Anzahl / Art Server	
Anzahl Updates	

Anzahl Schnittstellen	[redacted]

3.4.2 Schnittstellen zu anderen Fachverfahren

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

- **Produktionsumgebung**
  [redacted]
- **Qualitätssicherungsumgebung**
  Es existieren folgende Schnittstellen: [redacted]

3.4.3 Benutzerverwaltung

Die Benutzerverwaltung für die Verfahrensinfrastruktur erfolgt:

- Verfahrensintern

Die Benutzerverwaltung ist nicht Bestandteil dieser Leistungsvereinbarung.

3.4.4 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 Auftragsverabeiters freigeschaltet werden. Der externe Dienstleister muss, bevor er sich an einem System authentisieren kann, Kontakt mit dem Auftragsverarbeiter aufnehmen.

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

[redacted]

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 Auftragverarbeiter einsehen.

3.5 Geteilte Betriebsverantwortung/ Service Fernzugriff Administrativ (SFA)

Nicht Bestandteil des SLAs.

3.5.1 Leistungsbeschränkung bei manuellem, schreibenden Zugriff auf den Fileservice des Backendverfahrens

Wenn der Auftraggeber für Benutzer manuellen, schreibenden Zugriff auf den Fileservice des Backendverfahrens beauftragt, können Verfügbarkeitszusagen nur eingeschränkt umgesetzt werden.
Der zum Backendverfahren zugehörige Fileservice liegt in Bezug auf das technische Verfahrensmanagement in der Verantwortung des Auftraggebers.
Fehler und Produktionsausfälle der Fachapplikation, die auf fehlerhaften Fileservice zurückzuführen sind, werden nicht auf die vereinbarte Zielverfügbarkeit des definierten Services (Servicelevel) angerechnet.

Anlage 5 zum V11661-1/3016010

Security Service Level Agreement

Grundschutzkonformer Verfahrensbetrieb Führerscheinwesen

für

Auftraggeber

SIS Senator für Inneres
Ref.10 Organisation, IT, e Government
Verwaltungsmodernisierung

Contrescarpe 22/24

28203 Bremen

nachfolgend Auftraggeber

Anlage 5 zum V11661-1/3016010

Inhaltsverzeichnis

1. Einleitung

Der Auftragnehmer stellt dem Auftraggeber IT-Ressourcen einschließlich Hardware und systemnaher Software sowie IT-Dienstleistungen in definiertem Leistungsumfang zur Verfügung. Die Leistungen, die der Auftragnehmer im Rahmen dieser Vereinbarung erbringt, folgen der Vorgehensweise, die im BSI-Standard 100-1 (Managementsysteme für Informationssicherheit) sowie im BSI-Standard 100-2 (IT-Grundschutz-Vorgehensweise) beschrieben wird.

1.1 Aufbau des Dokumentes

Diese Anlage enthält die folgenden Kapitel:

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

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

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

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

1.2 Leistungsgegenstand

Mit dem **S**ecurity **S**ervice **L**evel **A**greement (SSLA) wird zwischen den Vertragspartnern ergänzend vereinbart, wie der Betrieb unter Informationssicherheitsgesichtspunkten auf Basis des IT-Grundschutzes des Bundesamtes für Informationssicherheit (BSI) unter Nutzung des Sicherheitsmanagementsystems des Auftragnehmers erfolgt. Ferner wird festgelegt, wie die vom Auftragnehmer in dessen Zuständigkeitsbereich getroffenen Sicherheitsmaßnahmen gegenüber dem Auftraggeber dokumentiert werden.

2. Leistungsumfang und -beschreibung

2.1 Informationssicherheitsmanagementsystem (ISMS)

Der Auftragnehmer betreibt ein Informationssicherheitsmanagementsystem (ISMS) auf Basis des BSI-Standards 100-1[1]. Wesentliche Elemente des ISMS sind:

- die im IT-Sicherheits- und Datenschutzmanagementhandbuch des Auftragnehmers festgelegten und mit denen im Geschäftsverteilungsplan (GVP[2]) 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 100-2
  - 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 100-2 festgelegten Schema die einschlägigen Sicherheitsmaßnahmen der IT-Grundschutz-Kataloge ausgewählt und umgesetzt werden können. Es liefert dem Auftragnehmer die Berücksichtigung relevanter Grundschutzmaßnahmen bei Planung, Errichtung und Betrieb von Verfahren des Auftraggebers sowie die Grundlagen für den Nachweis über die aktuell umgesetzten Sicherheitsmaßnahmen.

2.2 Verfahrensbezogener IT-Sicherheitskoordinator (ITSK)

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

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

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

---

1 https://www.bsi.bund.de/cln_165/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html

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

3 Der Sicherheitsnachweis ist die Dokumentation des Umsetzungsstandes aller relevanten Sicherheitsmaßnahmen.

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[4] vorgegebenen A-, B- und C-Maßnahmen, die in den Zuständigkeitsbereich des Auftragnehmers fallen, für den von dieser Vereinbarung betroffenen Informationsverbund umzusetzen.

Die Maßnahmenermittlung und Umsetzung von Sicherheitsmaßnahmen 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 Sicherheitsmaßnahmen und der jeweilige Umsetzungsstand werden im Sicherheitskonzept dokumentiert. Sofern zusätzliche Maßnahmen umgesetzt werden müssen, sind diese im SSLA Teil B zu benennen und die 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[5] Sicherheitsmaßnahmen im Zuständigkeitsbereich des Auftragnehmers.

Der Auftragnehmer stellt die dauerhafte Umsetzung der Sicherheitsmaßnahmen sicher. Zu diesem Zweck prüft er im Rahmen von Basissicherheitschecks regelmäßig den Umsetzungsstand der Sicherheitsmaßnahmen 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.

---

[4] Die aktuelle Version der IT-Grundschutz-Kataloge des BSI kann unter https://www.bsi.bund.de/DE/Themen/IT-Grundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html abgerufen werden.

[5] Die Festlegung der relevanten Maßnahmen erfolgt auf Grundlage der Modellierungsvorschriften des BSI-Standards 100-2.

2.4.2 Struktur und Standardordner

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 100-2 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 Sicherheitsmaßnahmen.

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

2.4.2.4 A.4 Ergebnis des Basis-Sicherheitschecks (Sicherheitsnachweis)

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

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

Der Report beinhaltet Angaben zur Durchführung der Prüfung (Datum, Personen), eine Beschreibung der Maßnahmenumsetzung, 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.[6]

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 beigefügt.

2.4.2.6 A.D1 Begleitdokumentation

Sofern für das vom Auftragnehmer erstellte Sicherheitskonzept weitere Dokumente zum Verständnis oder zum Nachweis der Maßnahmenumsetzung 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.

---

[6] Für Verfahren, die mindestens in Teilen im Green Twin Data Center (RZ²) 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 100-2 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 Ergänzende Sicherheits- und Risikoanalyse

Bei der ergänzenden Sicherheits- und Risikoanalyse nach BSI-Standard 100-3 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 Maßnahmen (z.B. im Rahmen des SSLA Teil B).

2.4.3.3 A.7 Risikobehandlung

Nicht oder nicht vollständig umgesetzte Maßnahmen des betrachteten Informationsverbundes werden im Rahmen der Basissicherheitschecks dokumentiert und dem Auftraggeber zur Verfügung gestellt. Sofern z.B. für Zwecke der Zertifizierung ein separater Risikobehandlungsplan erforderlich ist, werden nicht vollständig umgesetzte Maßnahmen 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 Basissicherheitschecks für den oder die maßgeblichen Anwendungsbausteine (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 Maßnahmen 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 Maßnahmenumsetzung

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 Maßnahmen 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 Maßnahmenumsetzung 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-Grundschutzkonforme Betrieb behandelt die Grundwerte der Informationssicherheit (Vertraulichkeit, Verfügbarkeit, Integrität).

Der unter Kapitel 2 aufgeführte Leistungsumfang ist grundsätzlich geeignet, die getroffenen Sicherheitsmaßnahmen sowie ihren Umsetzungsstand in geeigneter Form nachzuweisen und damit einen wesentlichen Beitrag zur Erfüllung datenschutzrechtlichen 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 Verantwortung für diese Maßnahmen liegt beim Verantwortlichen und geht im Zuge der Auftragsverarbeitung nicht auf den Auftragsverarbeiter (Auftragnehmer) über. Besondere Maßnahmen- 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-Grundschutz-konformes Sicherheitskonzept des betreffenden Verfahrens dar.

Die Umsetzung von Sicherheitsmaßnahmen kann nur dann zugesichert und geeignet nachgewiesen werden, wenn die jeweilige Maßnahmenverantwortung 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 Sicherheitsmaßnahmen 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 von der dokumentierten Maßnahmenumsetzung

Im laufenden Betrieb können temporäre Abweichungen zwischen der Dokumentation des Umsetzungsstandes und der tatsächlichen Umsetzung einzelner Sicherheitsmaßnahmen auftreten. Die Ursachen für temporäre Abweichungen können in der Änderung der IT-Infrastruktur oder durch neue oder veränderte IT-Grundschutzmaßnahmen verursacht werden.

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

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

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

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

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

3.5 Fortschreibung des IT-Grundschutzes

Der IT-Grundschutz des Bundesamtes für Informationssicherheit unterliegt der ständigen Fortschreibung. Hieraus kann sich z.B. bei wesentlichen Neuerungen oder Änderungen der IT-Grundschutzstandards (z.B. neue oder geänderte Sicherheitsmaßnahmen) eine Veränderung des Leistungsumfangs 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 100-2 vollständiges Sicherheitskonzept erforderliche Leistungen sind nicht Teil der vorliegenden Vereinbarung:

1. Durchführung der Schutzbedarfsfeststellung
2. Durchführung der ergänzenden Sicherheits- und Risikoanalyse nach BSI-Standard 100-3
3. Umsetzung zusätzlicher, über den Schutzbedarf "Normal" hinausgehender, Sicherheitsmaßnahmen
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 Maßnahmen befinden, für die die Umsetzungsverantwortung beim Auftraggeber liegt[7]. Sofern die Umsetzung dieser Maßnahmen beim Auftragnehmer nicht beauftragt wurde, werden diese Maßnahmen als "entbehrlich" dokumentiert. Erfolgt die Prüfung der Maßnahmenumsetzung in einem gemeinsamen Workshop (vgl. Kapitel 2.4.2), wird der Maßnahmenumsetzungsstand 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.

[7] Bausteine die einer "geteilten" Verantwortung unterliegen, finden sich insbesondere auf Schicht der Anwendungen wieder. Hierbei handelt es sich beispielsweise um Maßnahmen wie Freigabeprozesse für Patches der Fachanwendung, Einrichtung eines Internet-Redaktionsteams oder 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 100-3 durchzuführen. Die ergänzende Risikoanalyse dient der Identifikation erhöhter Risiken sowie geeigneter Maßnahmen zur Risikobehandlung.

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

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

Maßnahmen, 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-Grundschutz-konformen Betrieb des gesamten Informationsverbundes ist die Betrachtung aller relevanten Verfahrensteile erforderlich. Der Auftragnehmer kann Grundschutzkonformität jedoch nur für die von ihm verantworteten Komponenten sicherstellen. Maßnahmen, die im Verantwortungsbereich des Auftraggebers liegen, sind durch diesen selbst umzusetzen.

Bei der Planung und Umsetzung von Maßnahmen 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[8] bei der Erweiterung des betrachteten IT-Verbundes um fachliche oder technische Komponenten oder der Erweiterung um Kommunikationsschnittstellen, insbesondere zu Verfahren mit niedrigerem Sicherheitsniveau[9]
3) Bereitstellung von relevanten anwendungs- bzw. verfahrensspezifischen Informationen/Dokumentationen/Konzepten wie beispielsweise:

   a) Berechtigungskonzept (Rollen- und Rechtekonzept)
   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 Verfahrenssoftware). 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 Sicherheitsmaßnahmen 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.

[8] ggf. schließt das auch die Aktualisierung der Risikoanalyse nach BSI-Standard 100-3 mit ein
[9] z.B. zu Verfahren, die nicht IT-Grundschutzkonform betrieben werden

Anlage 6 zum V11661-1/3016010

Clientvereinbarung

Erklärung über Client-Sicherheitsmaßnahmen durch

<Firma>
<Anschrift>
<Anschrift>

Bei Fernzugriffen bestehen direkte Zugriffsmöglichkeiten von außerhalb auf das interne Netz und die darin verarbeiteten Daten. Durch diese Schnittstelle könnten vor allem unbeabsichtigt wirtschaftliche und betriebstechnische Schäden angerichtet werden, beispielsweise durch Schadsoftware. Daher sind besondere Sicherheitsmaßnahmen für die Clients notwendig, mit denen Fernzugriffe durchgeführt werden. Die folgenden Maßnahmen basieren auf dem IT-Grundschutz-Kompendium des BSI[1].

Der Vertragspartner garantiert, dass bei Fernzugriffen die folgenden Maßnahmen erfüllt sind:

1. Der Zugang zum Client muss mit Benutzerkennung und Passwort geschützt werden. Bei Inaktivität muss die Nutzungsmöglichkeit des Endgerätes automatisch gesperrt werden. Die Freigabe nach Inaktivität erfordert eine erneute Authentisierung. Der Startvorgang des Clients muss gegen Manipulationen abgesichert sein.
2. Auf dem Client muss ein aktuelles und aktiviertes Virenschutzprogramm betrieben werden.
3. Betriebssysteme und die auf dem Client installierte Software müssen gemäß den aktuellen Sicherheitsempfehlungen der Hersteller gepflegt sein und stets die Updates mit den aktuellen Security Patches erhalten.
4. Der Client muss so eingerichtet werden, dass normale Tätigkeiten nicht mit Administrationsrechten erfolgen. Administrationsrechte zur Laufzeit sollten vermieden werden. Sicherheitsrelevante Ereignisse müssen Protokolliert werden.
5. Kommunikationsbeziehungen zu Teilnehmern oder Ressourcen außerhalb des Dataport Netzes sowie Verbindungen zum Internet dürfen ausschließlich über die dafür von Dataport bereitgestellten und betriebenen Netzübergänge hergestellt werden. Die ggf. notwendigen Freischaltungen führt Dataport auf Antrag nach Prüfung durch.

   Die Umsetzung dieser Maßnahme ist nicht notwendig, wenn der Fernzugriff über eine durch Dataport zur Verfügung gestellte „Fastviewer" Fernzugriffslösung erfolgt
6. Kopien von Anwendungsdateien, Logfiles und Traces dürfen nicht auf lokalen Rechnern angelegt werden. Gemeint ist hier auch die vorübergehende, nicht über den Auftrag hinausgehende Speicherung dieser Daten. In Ausnahmefällen darf das Speichern der erforderlichen Daten unter ausdrücklichem Genehmigungsvorbehalt durch die verantwortliche Stelle (TVM/FVM) für die Dauer des Auftrags erfolgen.
7. Der Fernzugriff muss so erfolgen, dass Dritte keine Möglichkeit zur Einsichtnahme oder zum Zugriff auf den Client haben. Der Fernzugriff sollte grundsätzlich aus den Geschäftsräumen des Vertragspartners erfolgen. Alle Teilnehmenden sind zur Verschwiegenheit verpflichtet.

[1] Siehe www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html

8. Der Vertragspartner ermöglicht dem Sicherheitsmanagement von Dataport in Abstimmung mit dem Vertragspartner eine stichprobenartige Prüfung der Umsetzung der vereinbarten Maßnahmen auf für Fernzugriffe genutzte Clients.
   Alternativ kann der Vertragspartner einen gültigen, geeigneten und einschlägigen Nachweis (z.B. ein Zertifikat nach ISO 27001 auf Basis von IT-Grundschutz) eines unabhängigen Prüfers für die Umsetzung dieser Maßnahmen vorlegen.

_____ _____

(Datum) (Klarname &Unterschrift/Stempel Unternehmens)

EVB-IT Dienstvertrag

Leistungsnachweis Dienstleistung (Seite 1 von 1)

dataport

Leistungsnachweis

zum Vertrag über die Beschaffung von Dienstleistungen

Auftraggeber:
Vertragsnummer Dataport:
Vorhabennummer 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.

Position:			
Datum	**Aufwand in Stunden**	**Kommentar**	**Name der / des Leistenden**
		Gesamtzahl geleistete Stunden für Position	

Position			
Datum	**Aufwand in Stunden**	**Kommentar**	**Name der / des Leistenden**
		Gesamtzahl geleistete Stunden für Position	

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.

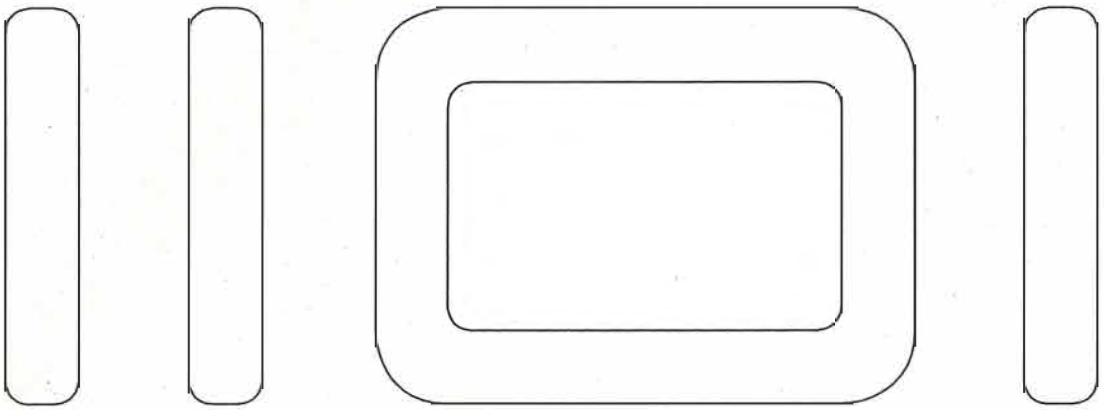
dataport

„Integrierter Dataport Oracle Service“

- IDOS -

Leistungsbeschreibung

Stand 28.02.2018



Für den Auftraggeber: <Behördenbezeichnung> im folgenden IDOS-Nutzungsberechtigter genannt

Inhaltsverzeichnis

1. Einleitung

Dataport hat mit der Firma Oracle Deutschland B.V. & Co. KG einen Vertrag geschlossen, der das Ziel hat, seinen Trägern Nutzung und Support von Oracle Produkten zu ermöglichen.

Dieser Lieferantenvertrag enthält für einen definierten Produktumfang (Produktset) eine unlimitierte Nutzungsmöglichkeit (**ULA** - **U**nlimited **L**icense **A**greement) sowie eine Produktliste, nach der bedarfsorientiert zu festgeschriebenen Konditionen Nutzungsrechte und Support beschafft werden können. Dieser Lieferantenvertrag endet am 31.12.2022.

Dataport bietet basierend auf den Lieferantenvertrag seinen Trägern an, einen umfangreichen

„Integrierten **D**ataport **O**racle **S**ervice“ (**IDOS**)

zu nutzen, der bei der Erfüllung fachspezifischer Anforderungen mit der Zielsetzung unterstützt, die IT effizienter zu gestalten und skalierbare, flexible und zuverlässige Oracle-Leistungen im Dataport – Rechenzentrum (zentrale Nutzung) und in kundeneigenen Betriebsstätten (dezentrale Nutzung) einzusetzen.

Durch die unlimitierte Nutzungsmöglichkeit des Produktsets ergeben sich besondere Vorteile während der Vertragslaufzeit, u.a.:

- **Unlimitierte Nutzungsmöglichkeit** des kompletten ULA Produktsets ohne Mehrkosten
- **Keine Mehrkosten für Lizenznutzungsrechte aus dem ULA Produktset** bei Wachstum der Infrastruktur
- **Grundlage für eine ordnungsgemäße Nutzung** der Produkte (Compliance) sowohl bei zentraler Nutzung als auch bei dezentraler Nutzung
- **Rückübertragung der Nutzungsrechte** im Rahmen der dezentralen Nutzung nach Vertragsende

Der detaillierte Leistungsumfang des „Integrierten Dataport Oracle Service“ (IDOS) ergibt sich aus den folgenden Abschnitten dieser Leistungsbeschreibung.

2. Leistungsumfang

Der „Integrierte Dataport Oracle Service“ (IDOS) besteht aus den folgenden einzelnen Leistungen:

- **Nutzung** der Produkte des ULA – Produktsets gemäß Abschnitt 2.1
- **Support** der Produkte des ULA – Produktsets gemäß Abschnitt 2.2
- **Vertrags-** und **Lizenzmanagement** gemäß Abschnitt 2.3

2.1 Produktset

Der Integrierte Dataport Oracle Service“ (IDOS) enthält für einen definierten Produktumfang (Produktset) eine unlimitierte Nutzungsmöglichkeit (**ULA - U**nlimited **L**icense **A**greement) sowie eine Produktliste, nach der bedarfsorientiert zu festgeschriebenen Konditionen Nutzungsrechte und Support nach Auftrag durch den Kunden beschafft werden.

2.1.1 Unlimitiertes Produktset

Das **unlimitierte ULA - Produktset** besteht aus folgenden Oracle – Produkten:

2.1.2 Produktliste mit Preisfestschreibung

Die Produktliste, nach der bedarfsorientiert zu festgeschriebenen Konditionen Nutzungsrechte und Support beschafft werden können, stellt ein optionales Produktset dar und besteht u.a. neben der Datenbankproduktkategorie aus weiteren ausgewählten Oracle Produktkategorien wie z.B. der Business Intelligence Produkte.

Die Produkte des optionalen Produktsets sind gesondert anzufragen und auf Basis von Einzelangeboten gegen Entgelt zu beauftragen.

2.2 Support

Der Integrierte Dataport Oracle Service" (IDOS) enthält für den unter Abschnitt 2.1.1 definierten Produktumfang (Produktset) Supportleistungen.

Die Supportleistungen werden ausschließlich direkt durch Oracle Deutschland B.V. & Co.KG in eigener Verantwortung erbracht. Es gelten die jeweils aktuellen Oracle Software Technical Support Policies unter http://www.oracle.com/us/support/policies/index.html.

Die für die Registrierung erforderliche Customer Support Identifier–Nummer (CSI–Nr.) lautet:

[redacted]

Die Support - Leistungen der Oracle Deutschland B.V. & Co.KG umfassen:

a) Pflegeleistungen

- Die Bereitstellung verfügbarer Umgehungen, Patches und Updates erfolgt unverzüglich, sobald verfügbar und ist im Internet zum Download verfügbar
  (Adresse: http://support.oracle.com)
- Die Bereitstellung verfügbarer Upgrades, Releases/Versionen ohne Verpflichtung bezüglich Häufigkeit und Umfang erfolgt unverzüglich, sobald verfügbar und ist im Internet zum Download verfügbar
  (Adresse: http://support.oracle.com)

b) Informationsservice

Die unverzügliche Bereitstellung verfügbarer Informationen über bekannt gemachte Programmkorrekturen erfolgt durch Bereitstellung im Internet zum Download
(Adresse: http://support.oracle.com)

c) Servicezeiten

- Montag bis Freitag von 8.30 bis 17.30 Uhr. Diese Zeiten gelten nicht an gesetzlichen Feiertagen am Erfüllungsort.

- Englischsprachiger Support (24x7) über elektronische Services.

d) Störungsmeldungen

Die Störungsmeldung erfolgt auf einem Formular entsprechend Anhang 2 zu EVB-IT Pflege S (Störungsmeldeformular) an:

[redacted]

Web-Adresse: www.oracle.com

Die Störungsmeldung wird während der vorstehend unter c) genannten Zeiten angenommen.

2.3 Vertrags- und Lizenzmanagement

Der Integrierte Dataport Oracle Service" (IDOS) enthält neben der eigentlichen Nutzungsmöglich der Produkte des Produktsets ein für die ordnungsgemäße Nutzung erforderliches Vertrags- und Lizenzmanagement, das von Dataport übernommen wird.

Dataport ist damit der zentrale Ansprechpartner gegenüber Oracle und klärt direkt alle Fragen im Zusammenhang mit der vertragskonformen Nutzung, die sich aus dem zwischen Dataport und der Firma Oracle Deutschland B.V. & Co. KG geschlossenen Vertrages ergeben. Dies trifft nicht auf Supportleistungen zu.

Für die Erstellung von regelmäßigen internen Lizenzbilanzen setzt Dataport ein Lizenzmanagementwerkzeug ein und teilt die Ergebnisse regelmäßig den IDOS – Nutzungsberechtigten mit. Die Erstellung der internen Lizenzbilanzen erfolgt jeweils jährlich, der IDOS- Nutzungsberechtigte bekommt bei Bedarf eine zusätzliche Erstellung pro Jahr auf Anfrage.

Sofern im Rahmen der Erstellung von regelmäßigen internen Lizenzbilanzen Fehlmengen identifiziert werden, z.B. durch die Nutzung von Produkten, die nicht vom unlimitierten Produktset umfasst sind, wird Dataport die betroffenen IDOS-Nutzungsberechtigten informieren und die notwendigen Schritte zur Sicherstellung der Compliance abstimmen und verfolgen. Zum Ausgleich von Fehlmengen kann bei Bedarf ein Lizenzpooling (dynamische Verwendung freiwerdender Lizenzen) in Abstimmung mit den IDOS – Nutzungsberechtigten etabliert werden.

Im letzten Vertragsjahr erstellt Dataport eine abschließende konsolidierte externe Lizenzbilanz zum Stichtag 31.12.2022 und teilt das Ergebnis nach Abstimmung mit den IDOS-Nutzungsberechtigten

Oracle (Herausgabe der Lizenzbilanz) mit dem Ziel der Mengenfestschreibung gemäß dem im Vertrag zwischen Dataport und der Firma Oracle Deutschland B.V. & Co. KG vereinbarten Bestätigungsprozess mit.

2.4 Leistungsabgrenzung

Die nachstehend aufgeführten Leistungen sind nicht Bestandteil des **I**ntegrierten **D**ataport **O**racle **S**ervices" (**IDOS**) und werden hier nur beispielhaft aus Gründen der Klarstellung aufgeführt:

- Technische Beratung im Zusammenhang mit dem Einsatz des Produktsets in der jeweiligen Infrastruktur (Architekturberatung)
- Produktspezifische Beratungsleistungen (Fachberatung)
- Externe Beratungsleistungen
- Schulungsleistungen
- Aufwendungen des IDOS – Nutzungsberechtigten zur Erbringung der unter Abschnitt 3 aufgeführten Mitwirkungen

Im Bedarfsfall können die aufgeführten Leistungen gesondert angefragt und angeboten werden.

3. Mitwirkungen und Beistellungen

Für die vollständige Erbringung des unter Abschnitt 2 beschriebenen Integrierten Dataport Oracle Service" (IDOS) bestehen seitens des IDOS–Nutzungsberechtitgen Mitwirkungsplichten u.a. hinsichtlich des Einrollens von bestehenden Supportverträgen und der Durchführung von Verbrauchsmessungen.

3.1 Einrollen bestehender Supportverträge (Beistellung)

Die Dataport zum Zeitpunkt des Vertragsabschlusses bekannten bestehenden Supportverträge wurden zum Vertragsbeginn in den mit der Firma Oracle Deutschland B.V. & Co. KG geschlossenen Vertrag überführt und sind damit entsprechend vom Integrierten Dataport Oracle Service umfasst. Ggf. noch weiterhin direkt mit Oracle oder einem Handelspartner eigenständig bestehende Supportverträge eines IDOS - Nutzungsberechtigten müssen als Voraussetzung für eine IDOS – Nutzung ebenfalls in diesen Vertrag überführt werden. Dafür erhält Dataport vom jeweiligen IDOS – Nutzungsberechtigten die Kenntnis über einen ggf. noch eigenständig bestehenden Supportvertrag und die Zustimmung zu dessen Überführung. Hierfür liefert der IDOS-Nutzungsberechtigte alle notwendigen Informationen (z.B. Vertragsnummer). Anderenfalls sind die Voraussetzungen für die Nutzung des Integrierten Dataport Oracle Service nicht gegeben und die IDOS - Nutzungsberechtigung entfällt.
Soweit es sich nicht um FullUse Supportverträge handelt, , z.B. ASFU – Nutzungen, entfällt die Pflicht zum Einrollen unter der Voraussetzung, dass die betroffenen Supportverträge eigenständig bis zum 31.12.2022 (Ende des Lieferantenvertrages) fortgeführt werden.

3.2 Verbrauchsmessung – zentrale Nutzung

Für eine Verbrauchsmessung und Erkennung von Oracle – Produkten im Rahmen des Bestätigungsprozesses sind die vom Hersteller vorgegebenen komplexen Lizensierungsmetriken zugrunde zu legen. Dazu wird die vom Hersteller Oracle anerkannte Appliance eRunbook Plattform als Bestandteil des bei Dataport eingesetzten Lizenzmanagementwerkzeugs verwendet. Für die Verbrauchsmessung werden neben Datenbank- und Systeminformationen auch Informationen der Virtualisierungsumgebungen verarbeitet, die zur Ermittlung der Nutzung von Oracle – Produkten (u.a. auch Oracle Datenbankoptionen und Oracle Management Packs) erforderlich sind. Das Ergebnis der Verbrauchsmessung ist eine entsprechend aussagefähige Oracle – Lizenzbilanz (Best-Practice). Für eine automatisierte Verbrauchsmessung ist der Einsatz von zur Verfügung stehenden Skripten erforderlich. Nur Scan – Methoden liefern nachvollziehbare und vom Hersteller anerkannte Ergebnisse.

Die Durchführung der Vermessung im Rahmen **der zentralen Nutzung** wird Dataport eigenständig vornehmen.

3.3 Verbrauchsmessung – dezentrale Nutzung

An der Durchführung der Vermessung im Rahmen der **dezentralen Nutzung** hat der IDOS – Nutzungsberechtigte durch Einsatz bzw. Verwendung der Skripte entsprechend mitzuwirken. Sollte der IDOS – Nutzungsberechtigte die Vermessung nicht automatisiert durchführen können, muss er seine IDOS – Nutzungsmengen manuell ermitteln und nach Aufforderung innerhalb von vier Wochen liefern. Die Verantwortung für die Richtigkeit von manuellen Vermessungsergebnissen trägt der IDOS – Nutzungsberechtigte, insbesondere für sich daraus ergebende Fehllizenzierungen.

An der Aufklärung von festgestellten Fehlmengen im Rahmen der **dezentralen Nutzung** wird der IDOS – Nutzungsberechtigte mitwirken. Für den Ausgleich von Fehlmengen wird der IDOS - Nutzungsberechtigte entsprechende Maßnahmen zum Ausgleich (z.B. Deinstallation, Abbau von Infrastruktur, Nachkäufe) umsetzen, insbesondere wenn diese im Rahmen der Erstellung und Abstimmung der abschließenden externen Lizenzbilanz (Bestätigungsprozess) festgestellt werden.

3.4 Sonstiges – dezentrale Nutzung

Dataport erhält vom jeweiligen IDOS – Nutzungsberechtigten die Kenntnis, inwieweit das IDOS – Produktset in kundenfremden Betriebsstätten genutzt werden soll und teilt entsprechende Veränderungen mit. Die Nutzung ist in einer zusätzlichen Vereinbarung gemäß Abschnitt 4.2 zu regeln.

Ggf. von Oracle direkt an den IDOS – Nutzungsberechtigten im Zusammenhang mit der Nutzung des Produktsets adressierte Anfragen sind entsprechend an Dataport weiterzugeben. Das betrifft insbesondere mögliche Auditanfragen oder Anfragen zu Lizenzplausibilisierungen von Oracle oder von ihr beauftragter Prüfungsgesellschaften.

Für die Rückübertragung von dezentral genutzten Mengengerüsten ist das unter Anhang 1 aufgeführte Formular anzuwenden.

4. Nutzungsbedingungen

Der „Integrierte Dataport Oracle Service“ (IDOS) ist ausschließlich zur Verwendung in Deutschland bestimmt.

Die Leistungen können für den Betrieb im **Dataport – Rechenzentrum (zentrale Nutzung)** und für den Betrieb in **kundeneigenen Betriebsstätten (dezentrale Nutzung)** genutzt werden.

Ausgenommen von der Nutzung ist der IT-Betrieb für das KonsensVerfahren (sowie eines etwaigen Nachfolgeverfahrens) innerhalb der Steuerverwaltung (IDOS – Steuer).

Für eine Nutzung des „Integrierten Dataport Oracle Service“ (IDOS) über den 31.12.2022 hinaus sind entsprechende Vertragserneuerungen (Preisblatt und Anpassung Leistungsbeschreibung) gemäß Abschnitt 6 erforderlich.

4.1 Bedingungen für die zentrale Nutzung

Die Leistungen des „Integrierten Dataport Oracle Service“ (IDOS) können für den Betrieb im **Dataport – Rechenzentrum (zentrale Nutzung)** genutzt werden.

Die Leistungen des „Integrierten Dataport Oracle Service“ (IDOS) dürfen nur für die Zwecke des IDOS – Nutzungsberechtigten selber verwendet werden. Eine Weitergabe oder Übertragung ist während der Vertragslaufzeit nicht gestattet.

4.2 Bedingungen für die dezentrale Nutzung

Die Leistungen des „Integrierten Dataport Oracle Service“ (IDOS) können für den Betrieb in kundeneigenen Betriebsstätten (dezentrale Nutzung) genutzt werden.

Für die dezentrale Nutzung des unlimitierten Produktsets ist eine Lizenzbilanzierung jeweils zum Vertragsbeginn Voraussetzung, sofern Dataport nicht bereits die Ergebnisse der in 2017 durchgeführten Vermessung vorliegen.

Für den Betrieb in kundeneigenen Betriebsstätten (dezentrale Nutzung) gelten die nachstehend aufgeführten Bedingungen:

zur Programmauslieferung: Die Programmauslieferung erfolgt bei Bedarf über die von Oracle dafür eingerichtete elektronische Website unter http://edelivery.oracle.com; Datenträger werden nicht gesondert bereitgestellt. Es ist zu beachten, dass nicht alle Programme auf allen Hardware-/Betriebssystem-Kombinationen verfügbar sind. Der IDOS – Nutzungsberechtigte hat das Recht, die zum IDOS – Produktset korrespondierenden Produkte auf seiner Hardware/Betriebssystem-Kombination zu installieren bzw. zu deinstallieren. Für die Installation bzw. Deinstallation der Produkte ist der IDOS - Nutzungsberechtigte selber verantwortlich.

zur Weitergabe der Leistung: Die Leistungen des „Integrierten Dataport Oracle Service" (IDOS) dürfen nur für die Zwecke des IDOS – Nutzungsberechtigten selber verwendet werden. Eine Weitergabe oder Übertragung ist während der Vertragslaufzeit nicht gestattet.

zur Nutzung in kundenfremden Betriebsstätten: Die dezentrale Nutzung ist beschränkt auf Nutzungen in den kundeneigenen Betriebsstätten des IDOS - Nutzungsberechtigten. Eine Nutzung in kundenfremden Betriebsstätten (z.B. private oder öffentlich rechtliche Rechenzentren) ist grundsätzlich möglich, bedarf aber einer zusätzlichen Vereinbarung zwischen Dataport und dem IDOS Nutzungsberechtigten.

6. Fortsetzung des Gesamtsupports nach Vertragsende

Oracle Deutschland B.V. & Co.KG wird für die im Rahmen der Erstellung einer Lizenzbilanz zum Stichtag 31.12.2022 ermittelten und festgeschrieben Mengen den für eine ordnungsgemäße weitere Nutzung anfallenden Gesamtsupport nach Vertragsende jeweils für weitere 12 Monate anbieten.

Ausgangspunkt für die Berechnung der Höhe des Gesamtsupports durch Oracle Deutschland B.V. & Co.KG für den Zeitraum direkt nach Vertragsende des Lieferantenvertrages (01.01.2023 bis 31.12.2023) sind lediglich die jeweiligen Gesamtsupportkosten des letzten Vertragsjahres zuzüglich ggf. einer allgemeinen Preissteigerungsrate. Damit entfällt eine üblicherweise in solchen Fällen von Oracle Deutschland B.V. & Co.KG geforderte Neuberechnung (Repricing) des Vertragswertes und ist damit unabhängig vom ermittelten Mengengerüst des Bestätigungsprozesses.

6.1 Support für die zentrale und dezentrale Nutzung

Dataport wird sich rechtzeitig im letzten Vertragsjahr mit den IDOS – Nutzungsberechtigten abstimmen, ob und in welchem Umfang der auf die ordnungsgemäße **zentrale** Nutzung entfallende Gesamtsupport für den Zeitraum direkt nach Vertragsende (01.01.2023 bis 31.12.2023) fortgesetzt werden soll bzw. muss. In Abhängigkeit der Summe aller zu diesem Zeitpunkt vorliegenden Beauftragungen der IDOS – Nutzungsberechtigten ergeben sich die dann tatsächlichen anteiligen Kosten der zentralen Nutzung je Nutzungsberechtigten für den Verlängerungszeitraum (01.01.2023 bis 31.12.2023). Der Vertrag für den Integrierten Dataport Oracle Service (IDOS) wird entsprechend durch ein neues Preisblatt und eine aktualisierte Leistungsbeschreibung angepasst.

Dataport wird sich rechtzeitig im letzten Vertragsjahr mit den IDOS – Nutzungsberechtigten auch zur Verlängerung des Supports für die **dezentral** genutzten Mengen abstimmen. Dabei ist der Support für die an den IDOS – Nutzungsberechtigten rückübertragene Menge für weitere 12 Monate (01.01.2023 bis 31.12.2023) fortzusetzen. Eine Fortsetzung erfolgt auf Basis von Einzelaufträgen zwischen dem Kunden und Oracle.

Für die Folgejahre (2024 ff.) erfolgt eine Verlängerung jeweils optional auf Basis der durch Oracle Deutschland B.V. & Co.KG zu diesem Zeitpunkt vorgelegten Supportverlängerungsangebote.

6.2 Umwandlung in Named User Plus bei dezentraler Nutzung

Nach den Dataport zum Zeitpunkt des Vertragsabschlusses mit der Firma Oracle Deutschland B.V. & Co. KG vorliegenden Informationen kann auf Wunsch des IDOS – Nutzungsberechtigten auf Anfrage gegenüber Oracle im Rahmen der Festlegungen zur Fortsetzung des Supports für die dezentrale Nutzung eine Wandlung der Mengen an Prozessoren nach einem festgelegten Umrechnungsschlüssel (Ratio-Migration) in Named – User Plus (NUP) vorgenommen werden. Aktuell beträgt der Umrechnungsfaktor (Ratio) 1:50. Eine Umwandlung kann damit nur durch die Firma Oracle Deutschland B.V. & Co. KG nach dessen zu diesem Zeitpunkt gültigen Regeln erfolgen.

6.3 Fortsetzung oder Erneuerung des bestehenden Lieferantenvertrages

Dataport wird mit Oracle ab 2021 eine Klärung herbeiführen, ob ein erneutes Unlimited Licence Agreement zu wirtschaflichen Konditionen möglich ist.

Sollte es ab 01.01.2023 erneut zu einem entsprechenden Lieferantenvertrag kommen, wird der zentrale und dezentrale Support (vg. 5.2 und 5.3) darüber abgebildet, Einzelverträge zwischen Kunde und Oracle bzgl. des dezentralen Supports wird es dann nicht geben. Der IDOS Vertrag wird dann entsprechend mit Preisblatt und Leistungsbeschreibung aktualisiert.

7. Mitgeltende Regelungen

Es gelten die gemäß zwischen Dataport und der Firma Oracle Deutschland B.V. & Co. KG abgeschlossenen Vertrag geltenden nachstehenden Regelungen mit.

7.1 Oracle Definitionen und allgemeine Lizenzvorschriften gem. Lieferantenvertrag

Die für die Nutzung von Oracle - Produkten geltenden Definitionen und allgemeinen Lizenzvorschriften sind entsprechend zu beachten und nachstehend zur Information aufgeführt.

Oracle Definitionen und allgemeine Lizenzvorschriften

Prozessor bezeichnet alle Prozessoren, auf denen die Oracle Programme installiert sind und/oder ablaufen. Auf Programme, die auf Prozessor-Basis lizenziert sind, dürfen Ihre internen Benutzer (inkl. Beauftragte und Auftragnehmer) und Ihre externen dritten Benutzer zugreifen. Zur Ermittlung der erforderlichen Anzahl an Lizenzen wird die Gesamtanzahl der Kerne des Prozessors mit einem Prozessorkern-Lizenzfaktor multipliziert; dieser Faktor ist in der Oracle Processor Core Factor-Tabelle definiert, die unter http://oracle.com/contracts abgerufen werden kann. Alle Kerne auf allen Multicore Chips für jedes Lizenzprogramm müssen zunächst addiert werden, bevor sie mit dem jeweiligen Prozessorkern-Lizenzfaktor multipliziert werden, und alle Bruchteile einer Zahl sind auf die nächsthöhere Zahl aufzurunden. Bei der Lizenzierung von Oracle Programmen mit Standard Edition 2, Standard Edition One oder Standard Edition im Produktnamen (hiervon ausgenommen sind Java SE Support, Java SE Advanced and Java SE Suite) wird ein Prozessor mit einem belegten Socket gleichgesetzt; bei Modulen mit mehreren Chips hingegen wird jeder Chip mit einem belegten Socket gleichgesetzt.

Würde das Programm (ausgenommen sind Standard Edition One- bzw. Standard Edition-Programme) beispielsweise auf einem Multicore Chip-basierten Server mit einem Oracle Prozessorkern-Faktor von 0,25 auf 6 Prozessorkernen installiert und/oder ablaufen, wären zwei Prozessorlizenzen erforderlich (6 multipliziert mit dem Prozessorkern-Lizenzfaktor 0,25 entspricht 1,50, welches dann auf die nächste ganze Zahl, nämlich 2, aufgerundet wird). Würde das Programm hingegen auf einem Multicore-Server für eine in der Oracle Processor Core FactorTabelle nicht angegebene Hardware-Plattform auf 1 O Prozessorkernen installiert und/oder ablaufen, wären zehn Prozessorlizenzen erforderlich (10 multipliziert mit dem Prozessorkern-Lizenzfaktor 1,0 für „Alle anderen Multicore Chips (All other multicore chips)" entspricht 10).

Bei dem Programm Healthcare Transaction Base werden zur Ermittlung der Anzahl an benötigten Lizenzen nur die Prozessoren gezählt, auf denen Internet Application Server Enterprise Edition und Healthcare Transaction Base installiert sind und/oder ablaufen. Bei den Programmen iSupport, iStore und Configurator werden zur Ermittlung der Anzahl an für das lizenzierte Programm benötigten Lizenzen nur die Prozessoren gezählt, auf denen Internet Application Server (Standard Edition und/oder Enterprise Edition) und das lizenzierte Programm (d. h. iSupport, iStore und/oder Configurator) ablaufen; bei diesen Lizenzen dürfen Sie das lizenzierte Programm auch auf den Prozessoren installieren und/oder ablaufen lassen, auf· denen eine lizenzierte Oracle Database (Standard Edition und/oder Enterprise Edition) installiert ist und/oder abläuft.

Bei den folgenden Programmen werden zur Ermittlung der Anzahl an benötigten Lizenzen nur die Prozessoren gezählt, auf denen das verwaltete/überwachte Programm ausgeführt wird: Configuration Management Pack for Applications, System Monitoring Plug-in for Non Oracle Databases, System Monitoring Plug-in for Non Oracle Middleware, Management Pack for Non-Oracle Middleware, Management Pack for WebCenter Suite.

Bei den folgenden Programmen werden nur die Prozessoren zur Ermittlung der Anzahl an benötigten Lizenzen gezählt, (a) die die Datenbankserver ausführen, von denen verfremdete Daten oder Datenteilmengen stammen, und (b) die Prozessoren, die die

Datenbankserver ausführen, auf denen eine Verfremdung oder Teilmengenerstellung erfolgt (per GUI oder Befehlszeile): Data Masking and Subsetting Pack.

Bei den folgenden Programmen werden zur Ermittlung der Anzahl an benötigten Lizenzen alle Prozessoren gezählt, auf denen die Middleware und/oder Datenbank-Software für das entsprechende, verwaltete Anwendungsprogramm ausgeführt wird: Applicatibn Management Suite for Oracle E-Business Suite, Application Management Suite for PeopleSoft, Application Management Suite for Siebe!, Application Management Suite for JD Edwards EnterpriseOne, Application Management Pack for Utilities und Application Pack for Taxation and Policy Management.

Bei den Programmen Application Replay Pack und Real User Experience Insight werden zur Ermittlung der Anzahl an benötigten Lizenzen alle Prozessoren gezählt, auf denen die Middleware-Software für das entsprechende, verwaltete Anwendungsprogramm ausgeführt wird.

Bei den folgenden Programmen werden zur Ermittlung der Anzahl an benötigten Lizenzen nur die Prozessoren gezählt, auf denen die Zieldatenbank ausgeführt wird: Informatica PowerCenter and PowerConnect Adapters sowie Application Adapter for Warehouse Builder for PeopleSoft, Oracle E-Business Suite, Siebe! und SAP.

Bei den folgenden Programmen werden zur Ermittlung der Anzahl an benötigten Lizenzen nur die Prozessoren gezählt, auf denen die Datentransformationen ausgeführt werden: Data Integrator Enterprise Edition, Data Integrator Enterprise Edition for Oracle Applications, Data Integrator und Application Adapter for Data Integration und Application Adapters for Data Integration.

Bei dem folgenden Programm werden zur Ermittlung der Anzahl an benötigten Lizenzen nur die Prozessoren gezählt, auf denen die Komponente Times Ten In-Memory Database des Programms In-Memory Database Cache installiert ist und/oder ausgeführt wird: Oracle In-Memory Database Cache.

Bei dem folgenden Programm werden zur Ermittlung der Anzahl an benötigten Lizenzen nur (a) die Prozessoren zur Ausführung der Oracle Datenbank gezählt, von der Sie Daten erfassen, und (b) die Prozessoren zur Ausführung der Oracle Datenbank, auf die die Daten angewendet werden sollen: Oracle GoldenGate.

Bei den folgenden Programmen werden zur Ermittlung der Anzahl an benötigten Lizenzen nur (a) die Prozessoren zur Ausführung der Datenbank gezählt, von der Sie Daten erfassen, und (b) die Prozessoren zur Ausführung der Datenbank, auf die die Daten angewendet werden sollen: Oracle GoldenGate for Mainframe und Oracle GoldenGate for Teradata Replication Services.

Bei dem folgenden Programm werden zur Ermittlung der Anzahl an benötigten Lizenzen nur (a) die Prozessoren der Nicht-Qracle-Datenbank gezählt, von der Sie Daten erfassen, und (b) die Prozessoren der Nicht-Oracle-Datenbank, auf die die Daten angewendet werden sollen: Oracle GoldenGate for Non Oracle Database.

Bei den folgenden Programmen werden zur Ermittlung der Anzahl an benötigten Lizenzen nur (a) die Prozessoren der Nicht-OracleDatenbank oder Oracle Datenbank gezählt, von der Sie Daten erfassen. Fürmultiple Quelldatenbanken müssen alle Prozessoren für alle Quellen gezählt werden: Oracle GoldenGate Application Adapters und Oracle GoldenGate for Big Data.

Bei den folgenden Programmen werden zur Ermittlung der Anzahl an benötigten Lizenzen nur die Prozessoren der Quellen gezählt, die geschützt, überwacht oder geprüft sind: Audit Vault und Database Firewall.

Bei dem Programm Oracle ATG Web Commerce Search müssen nur die Prozessoren gezählt werden, auf denen Abfragen verarbeitet werden. Nicht erfasst werden müssen Prozessoren, auf denen das Programm für Zwecke der Inhaltsindizierung in konfigurierten Content – Quellen ausgeführt wird, vorausgesetzt, das Programm wird auf allen in einem gegebenen Server installierten Prozessoren nicht noch für weitere Zwecke ausgeführt.

Lizenzvorschriften zu Oracle Technology-Programmen und Oracle Business Intelligence-Anwendungen
Failover: Vorbehaltlich der nachstehenden Bedingungen beinhaltet Ihre Lizenz für die Programme, die in .der US Oracle Technology- Preisliste aufgeführt sind, und welche unter http://www.oracle.com/us/corporate/pricinq/price-lists/index.html abgerufen werden kann, das Recht, das/die Lizenzprogramm(e) insgesamt bis zu zehn einzelne Tage eines jeden Kalenderjahres auf einem nicht lizenzierten Ersatzrechner in einer Failover-Umgebung ablaufen zu lassen. (Fällt ein Failover-Knoten beispielsweise zwei Stunden am Dienstag und drei Stunden am Freitag aus, zählt dies als zwei Tage.) Das vorstehend ausgeführte Recht gilt nur für Rechner-Cluster mit gemeinsamem Platten-Array. Fällt der Produktionsknoten aus, übernimmt der Failover-Knoten die Funktion als Hauptknoten. Sobald der ursprüngliche . Produktionsknoten repariert wurde, müssen Sie wieder zurückwechseln. Wird der zulässige Failover-Zeitraum von zehn Tagen in einem Kalenderjahr überschritten, muss der Failover-Knoten lizenziert werden. Darüber hinaus ist pro Cluster-Umgebung nur ein Failover-Knoten bis zu zehn einzelne Tage pro Jahr kostenlos. Dies gilt auch dann, wenn mehrere Knoten als Failover-Knoten konfiguriert sind. Betriebsausfallzeiten für Wartungszwecke werden ebenfalls auf die maximal zehn Nutzungstage angerechnet. Bei der Lizenzierung von Optionen für eine Fail6ver-Umgebung muss die Anzahl der Optionslizenzen den Lizenzen der zugehörigen Datenbank entsprechen. Bei der Lizenzierung nach Named User Plus wird zudem nur für einen Failover-Knoten auf die Mindestbenutzervorgaben verzichtet. Jegliche Nutzung außerhalb des im vorangegangen Abschnitt beschriebenen Nutzungsumfangs muss gesondert lizenziert werden. In einer FailoverUmgebung muss zur Lizenzierung einer gegebenen Cluster-Konfiguration für den Produktions- und den Failover-Knoten dieselbe Lizenzmetrik verwendet werden.

Testing: Zwecks Prüfung einzelner physischer Sicherungskopien (Backups) beinhaltet Ihre Lizenz für die Oracle Datenbank (Enterprise Edition, Standard Edition oder Standard Edition One) das Recht, in einem Kalenderjahr die Datenbank bis zu viermal, höchstens aber zwei Tage pro Testlauf, auf einem unlizenzierten Rechner laufen zu lassen. Das vorstehend genannte Recht schließt keine weitere Methode zur Datenwiederherstellung (z. B. Remote-Spiegelung) ein, bei der die Binärdateien der Oracle Programme kopiert oder synchronisiert werden.