

Vertragsnummer/Kennung Auftraggeber 1 _____

Vertragsnummer/Kennung Auftraggeber 2 _____

Vertragsnummer/Kennung Auftragnehmer V21706/1090200/3011110

Seite 1 von 17

Vertrag über IT-Dienstleistungen**Inhaltsangabe**

| | | |
|-------|---|----|
| 1 | Gegenstand und Bestandteile des Vertrages..... | 3 |
| 1.1 | Vertragsgegenstand | 3 |
| 1.2 | Vertragsbestandteile..... | 3 |
| 1.2.1 | dieser Vertragstext | 3 |
| 1.2.2 | Allgemeine Vertragsbedingungen von Dataport (Dataport AVB) in der jeweils geltenden Fassung..... | 3 |
| 1.2.3 | folgende Anlagen: | 4 |
| 1.2.4 | die Ergänzenden Vertragsbedingungen für IT-Dienstleistungen (EVB-IT Dienstleistungs-AGB) in der bei Vertragsschluss geltenden Fassung | 4 |
| 1.2.5 | sowie die Allgemeinen Vertragsbedingungen für die Ausführung von Leistungen (VOL/B) in der bei Vertragsschluss geltenden Fassung. | 4 |
| 2 | Überblick über die vereinbarten Leistungen..... | 5 |
| 3 | Beschreibung der Leistungen/Laufzeit und Kündigung..... | 5 |
| 3.1 | Art, Umfang und Termine | 5 |
| 3.2 | Einmalig zu erbringende Leistungen..... | 5 |
| 3.3 | Regelmäßig zu erbringende Leistungen | 6 |
| 3.4 | Leistungen, die nur auf Abruf erbracht werden sollen..... | 6 |
| 3.5 | Abweichende Kündigungsregelung und abzulösende Verträge | 6 |
| 4 | Vergütung | 7 |
| 4.1 | Vergütung nach Aufwand erfolgt gem. Preisblatt 2a und Muster Leistungsnachweis Dienstleistung | 7 |
| 4.1.1 | Kategorien..... | 7 |
| 4.1.2 | Abweichende Regelungen für die Bestimmung und Vergütung von Personentagessätzen | 8 |
| 4.1.3 | Reisekosten/Nebenkosten*/Materialkosten/Reisezeiten | 8 |
| 4.1.4 | Preisanpassung..... | 8 |
| 4.1.5 | Fälligkeit und Zahlung | 8 |
| 4.1.6 | Besondere Bestimmungen zur Vergütung nach Aufwand | 8 |
| 4.2 | Vergütung zum Pauschalfestpreis gem. Anlage 2b | 9 |
| 4.3 | Rechnungsadresse gem. Anlage 1a-1b..... | 9 |
| 5 | Service- und Reaktionszeiten* | 9 |
| 5.1 | Servicezeiten* | 9 |
| 5.2 | Reaktionszeiten* | 9 |
| 6 | Ansprechpartner gem. Anlage 1a-1b | 10 |
| 7 | Besondere Anforderungen an Mitarbeiter des Auftragnehmers | 10 |
| 8 | Mitwirkungs- und Beistelleistungen des Auftraggebers | 10 |
| 8.1 | Anlage 1a-1b Ansprechpartner | 10 |
| 8.2 | Folgende weitere Beistelleistungen werden vereinbart:..... | 11 |
| 9 | Abweichende Nutzungsrechte an den Leistungsergebnissen, Erfindungen..... | 11 |
| 10 | Quellcode* | 11 |
| 11 | Abweichende Haftungsregelungen..... | 12 |
| 12 | Vertragsstrafen | 12 |
| 13 | Weitere Regelungen | 13 |
| 13.1 | Datenschutz, Geheimhaltung und Sicherheit..... | 13 |

Vertragsnummer/Kennung Auftraggeber 1 _____

Vertragsnummer/Kennung Auftraggeber 2 _____

Vertragsnummer/Kennung Auftragnehmer V21706/1090200/3011110

Seite 2 von 17

| | | |
|--------|--|----|
| 13.2 | Haftpflichtversicherung | 13 |
| 13.3 | Teleservice* | 13 |
| 13.4 | Dokumentations- und Berichtspflichten | 13 |
| 13.5 | Interessenkonflikt..... | 13 |
| 14 | Pflichten nach Vertragsende | 13 |
| 15 | Sonstige Vereinbarungen | 13 |
| 15.1 | Allgemeines | 13 |
| 15.2 | Umsatzsteuer..... | 14 |
| 15.2.1 | Umsatzsteuer für Leistungen, die bis zum 31.12.2024 erbracht werden..... | 14 |
| 15.2.2 | Umsatzsteuer für Leistungen, die ab dem 01.01.2025 erbracht werden (gilt für AG1)..... | 14 |
| 15.2.3 | Umsatzsteuer für Leistungen, die ab dem 01.01.2025 erbracht werden (gilt für AG2)..... | 14 |
| 15.3 | Verschwiegenheitspflicht | 14 |
| 15.4 | Bremer Informationsfreiheitsgesetz (gilt für AG2)..... | 14 |
| 15.5 | Ablösungen von Vereinbarungen/ Vorvereinbarungen | 14 |
| 15.6 | Weisungen..... | 15 |
| 15.7 | Verwendung der vertraglichen Leistungen | 15 |
| 15.8 | Auftragsverarbeitung | 15 |
| 15.9 | ITJG (gilt für AG1)..... | 15 |
| 15.10 | Beauftragung, Service und Support..... | 15 |
| 15.11 | Festlegung von Auftragsberechtigten | 15 |
| 15.12 | Vertragsunterzeichnung..... | 15 |

Vertragsnummer/Kennung Auftraggeber 1 _____

Vertragsnummer/Kennung Auftraggeber 2 _____

Vertragsnummer/Kennung Auftragnehmer V21706/1090200/3011110

Vertrag über IT-Dienstleistungen

Zwischen

Land Schleswig-Holstein vertreten durch
Ministerium für Justiz und Gesundheit des Landes Schleswig-Holstein
Referat II 35
Lorentzendamm 35
24106 Kiel
— im Folgenden „Auftraggeber 1“ (AG1) genannt —

Die Senatorin für Justiz und Verfassung
Richtweg 16 - 22
28195 Bremen
— im Folgenden „Auftraggeber 2“ (AG2) genannt —

Wenn alle Auftraggeber als Gesamtheit gemeint sind, werden diese folgend „Auftraggeber“ genannt.

und

Dataport
Anstalt öffentlichen Rechts
Altenholzer Straße 10-14
24161 Altenholz
— im Folgenden „Auftragnehmer“ (AN) genannt —

wird folgender Vertrag geschlossen:

1 Gegenstand und Bestandteile des Vertrages

1.1 Vertragsgegenstand

Gegenstand des Vertrages sind Dienstleistungen des Auftragnehmers:

PDF Compressor: Verfahrensinfrastruktur für das Verfahren im Rechenzentrum

1.2 Vertragsbestandteile

Es gelten als Vertragsbestandteile in folgender Rangfolge:

1.2.1 dieser Vertragstext

1.2.2 Allgemeine Vertragsbedingungen von Dataport (Dataport AVB) in der jeweils geltenden Fassung

EVB-IT Dienstvertrag



Vertragsnummer/Kennung Auftraggeber 1 _____

Vertragsnummer/Kennung Auftraggeber 2 _____

Vertragsnummer/Kennung Auftragnehmer V21706/1090200/3011110

Seite 4 von 17

1.2.3 folgende Anlagen:

| Anlagen zum EVB-IT Dienstvertrag | | | |
|----------------------------------|--|--|---------------|
| Anlage Nr. | Bezeichnung | Datum/ Version | Anzahl Seiten |
| 1 | 2 | 3 | 4 |
| 1a | Ansprechpartner AG1 | - | 1 |
| 1b | Ansprechpartner AG2 | - | 1 |
| 2a | Preisblatt Aufwände alle AG | 19.04.2024/ Version 6.0 | 2 |
| 2b | Preisblatt Jährlicher Festpreis alle AG | 19.04.2024/ Version 6.0 | 1 |
| 3 | Datenschutzrechtliche Festlegung des Auftraggebers | Vorlagenver- sion 2.1 | 2 |
| 4 | Anlage ITJG AG1 | 28.04.2020/ Version 1.2 | 11 |
| 5a | Service Level Agreement Verfahrensinfrastruktur im Dataport Rechenzentrum Teil A – Allgemeiner Teil – (SLA VI A) | 01.11.2022/ Vorlagenver- sion 2.04 | 18 |
| 5b | Service Level Agreement Verfahrensinfrastruktur im Dataport Rechenzentrum Teil B (spezifischer Teil für Verfahren PDF Compressor (PDFCOMP_ML001)) (SLA VI B) | 01.11.2022/ Version 2.06 | 13 |
| 6a | Security Service Level Agreement Grundschutzkonformer Verfahrensbetrieb PDF Compressor ML Allgemeiner Teil (Teil A) (SSLA A) | 08.11.2021/ Version 2.0.15 | 14 |
| 6b | Security Service Level Agreement Grundschutzkonformer Verfahrensbetrieb PDF Compressor ML Verfahrensspezifischer Teil (Teil B) (SSLA B) | 22.03.2011 | 4 |
| 7 | Muster Leistungsnachweis Dienstleistung | 15.08.2016 | 2 |

Es gelten die Anlagen in folgender Rangfolge 1a, 1b, 4, 2a, 2b, 3, 5a, 6b, 6a, 7.

1.2.4 die Ergänzenden Vertragsbedingungen für IT-Dienstleistungen (EVB-IT Dienstleistungs-AGB) in der bei Vertragsschluss geltenden Fassung

1.2.5 sowie die Allgemeinen Vertragsbedingungen für die Ausführung von Leistungen (VOL/B) in der bei Vertragsschluss geltenden Fassung.

EVB-IT Dienstvertrag



Vertragsnummer/Kennung Auftraggeber 1 _____

Vertragsnummer/Kennung Auftraggeber 2 _____

Vertragsnummer/Kennung Auftragnehmer V21706/1090200/3011110

Seite 5 von 17

Die EVB-IT Dienstleistungs-AGB stehen unter www.cio.bund.de und die VOL/B unter www.bmwk.de zur Einsichtnahme bereit.

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

Für alle in diesem Vertrag genannten Beträge gilt einheitlich der Euro als Währung. Die vereinbarten Vergütungen verstehen sich zuzüglich der gesetzlichen Umsatzsteuer, soweit Umsatzsteuerpflicht besteht.

2 Überblick über die vereinbarten Leistungen

Der Auftragnehmer erbringt für den Auftraggeber folgende Dienstleistungen:

- Beratung
- Projektleitungsunterstützung
- Schulung
- Einführungsunterstützung
- Betreiberleistungen
- Benutzerunterstützungsleistungen
- Providerleistungen ohne Inhaltsverantwortlichkeit
- Unterstützung bei Planungsleistungen
- Unterstützung bei Softwareentwicklung
- Hotline
- sonstige Dienstleistungen: gem. SLA VI A, SLA VI B, SSLA A und SSLA B

3 Beschreibung der Leistungen/Laufzeit und Kündigung

3.1 Art, Umfang und Termine

Dieser Vertrag beginnt am 01.04.2024 und gilt für unbestimmte Zeit.

Art, Umfang und Termine der zu erbringenden Leistungen ergeben sich aus der folgenden Tabelle (Termin- und Leistungsplan):

| Lfd. Nr. | Leistung (ggf. Verweis auf Anlage) | Ort der Leistung | Beginn ¹ | Ende/Termin ² |
|----------|---------------------------------------|------------------|---------------------|--------------------------|
| 1 | 2 | 3 | 4 | 5 |
| 1. | Hosting | beim AN | 01.04.2024 | |
| 2. | IT-Sicherheitskoordination | beim AN | 01.05.2024 | |
| 3. | Hosting optional | beim AN | 01.04.2024 | |

- Feiertage im Sinne dieses Vertrages sind die Feiertage in Schleswig-Holstein, sowie der 24.12. und 31.12. abweichend von Ziffer 5.1 EVB-IT Dienstleistungs-AGB).

3.2 Einmalig zu erbringende Leistungen

- Die Leistungen gemäß Nummer 3.1 lfd. Nr. _____ werden einmalig erbracht.

¹ wenn keine Vorgabe für Beginn, dann Feld leer lassen

² z.B. festes Datum ggf. mit Uhrzeit oder „nach 48 Monaten“ (wenn Vertrag unbefristet, dann Feld leer lassen)

Vertragsnummer/Kennung Auftraggeber 1 _____

Vertragsnummer/Kennung Auftraggeber 2 _____

Vertragsnummer/Kennung Auftragnehmer V21706/1090200/3011110

Seite 6 von 17

3.3 Regelmäßig zu erbringende Leistungen

- Die Leistungen gemäß Nummer 3.1 lfd. Nr. 1-2 werden
- in folgendem Zyklus erbracht:
- wöchentlich
 monatlich
- jeweils
- an folgenden Tagen: _____ (Wochentag(e) bzw. bei monatlichen Zyklen auch „1. Montag im Monat“)
- in der Zeit von _____ bis _____ (Uhrzeit)
nicht jedoch an Feiertagen.
- in folgenden Zyklen zu folgenden Zeiten erbracht: gemäß SLA VI Pkt. 2.2.2.

3.4 Leistungen, die nur auf Abruf erbracht werden sollen

- Die Leistungen gemäß Nummer 3.1 lfd. Nr. 3 werden nur auf Abruf erbracht.
- Der Mindestvorlauf für den Abruf beträgt _____ (Stunden/Tage).
- Die geschätzte Abnahme beträgt _____ (Stunden/Tage) pro _____ (z.B. Vertragsmonat/Vertragsquartal/Vertragsjahr/Vertragslaufzeit).
- Die vereinbarte Mindestabnahme beträgt _____ (Stunden/Tage) pro _____ (z.B. Vertragsmonat, Vertragsquartal, Vertragsjahr, Vertragslaufzeit).
- Die Mindestabnahme für Leistungen, die Reisen erforderlich machen, beträgt pro Abruf _____ (Stunden/Tage).

Soweit Leistungen nur auf Abruf zu erbringen sind, hält sich der Auftragnehmer in dem vorgenannten Zeitraum zur Leistungserbringung bereit.

3.5 Abweichende Kündigungsregelung und abzulösende Verträge

- Abweichend von Ziffer 15.1 EVB-IT Dienstleistungs-AGB beträgt die Kündigungsfrist _____ Monat(e) zum Ablauf eines _____ (z.B. Kalendermonats/Kalendervierteljahres/Kalenderjahres).
- Abweichend von Ziffer 15.1 EVB-IT Dienstleistungs-AGB wird bei vereinbarter fester Laufzeit ein Sonderkündigungsrecht gem. Anlage Nr. _____ vereinbart.
- Abweichend von Ziffer 15.1 EVB-IT Dienstleistungs-AGB:

Dieser Vertrag kann von jedem Auftraggeber erstmals unter Wahrung einer Frist von 6 Monat(en) zum 31.03.2025 gekündigt werden. Danach kann er zum Ende eines Kalenderjahres unter Wahrung einer Frist von 6 Monat(en) gekündigt werden. Die Kündigung eines Auftraggebers wirkt sich für und gegen alle Auftraggeber aus mit der Folge, dass die Kündigung für alle Auftraggeber Wirkung entfaltet. Die Kündigung bedarf der Textform.

Im Falle einer Kündigung durch einen Auftraggeber, wird der Auftragnehmer den verbleibenden Auftraggebern über die Leistungen dieses Vertrages vor Vertragsbeendigung ein neues Vertragsangebot unterbreiten

Der kündigende Auftraggeber trägt eventuelle Kosten für den Rückbau. Neben den Kosten für infrastrukturelle Ressourcen, kann es zu zuzüglichem Personalaufwand kommen. Die Kosten hierfür trägt der kündigende Auftraggeber.

Haushaltsvorbehalt (gilt nur für AG1)

Der Auftraggeber kann diesen Vertrag außerordentlich unter Wahrung einer Frist von 30 Tagen zum Monatsende kündigen, wenn die erforderlichen Haushaltsmittel nicht zur Verfügung stehen. Der Auftraggeber hat diese Haushaltmittel beantragt und wird sich für ihre Bewilligung einsetzen. Macht der Auftraggeber von diesem Kündigungsrecht Gebrauch, so hat der Auftragnehmer Anspruch auf Ersatz der aus der vorzeitigen Vertragsbeendigung resultierenden Kosten bzw. Schäden.

EVB-IT Dienstvertrag



Vertragsnummer/Kennung Auftraggeber 1 _____

Vertragsnummer/Kennung Auftraggeber 2 _____

Vertragsnummer/Kennung Auftragnehmer V21706/1090200/3011110

Seite 7 von 17

| Abzulösende Verträge/ Verfahren | Beginn | Ende |
|---------------------------------|--------|------|
| | | |
| | | |

4 Vergütung

4.1 Vergütung nach Aufwand erfolgt gem. Preisblatt 2a und Muster Leistungsnachweis Dienstleistung

- Die Leistungen werden gemäß Anlage 2a-2e mit einer Obergrenzenregelung vergütet

- Nummer 3.1 lfd. Nr. _____ werden nach Aufwand gemäß Kategorie(n) _____ aus Nummer 4.1.1
 mit einer Obergrenze in Höhe von _____ Euro
 Nummer 3.1 lfd. Nr. _____ werden nach Aufwand gemäß Kategorie(n) _____ aus Nummer 4.1.1
 mit einer Obergrenze in Höhe von _____ Euro
 Nummer 3.1 lfd. Nr. _____ werden nach Aufwand gemäß Kategorie(n) _____ aus Nummer 4.1.1
 mit einer Obergrenze in Höhe von _____ Euro

Leistungsnachweise und Rechnungen inkl. der Aufteilung des zu zahlenden Betrages pro Auftraggeber werden allen Auftraggebern zur Verfügung gestellt. Jeder prüft die Unterlagen sachlich und rechnerisch richtig und bezahlt seinen Anteil.

4.1.1 Kategorien

| Lfd. Nr. | Bezeichnung der Kategorie | Vergütung für Tätigkeiten innerhalb der zuschlagsfreien Zeiten | | Zuschläge in Prozent auf die Vergütungssätze aus Spalten 3 und 4 für Tätigkeiten innerhalb nachfolgender Zeiten | | | | | |
|-------------|---------------------------|--|------------|---|---------|---|---------------------|---|---|
| | | Stundensatz | Tages-satz | Montag bis Freitag (Arbeitstage) außerhalb der zuschlagsfreien Zeiten | Samstag | | Sonn- und Feiertage | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | |
| Kategorie 1 | | | | % | % | % | % | % | % |
| Kategorie 2 | | | | % | % | % | % | % | % |
| Kategorie 3 | | | | % | % | % | % | % | % |

EVB-IT Dienstvertrag



Vertragsnummer/Kennung Auftraggeber 1 _____

Vertragsnummer/Kennung Auftraggeber 2 _____

Vertragsnummer/Kennung Auftragnehmer V21706/1090200/3011110

Seite 8 von 17

Festlegung der zuschlagsfreien Zeiten:

| Arbeitstag | zuschlagsfreie Zeiten | | | |
|-----------------------|-----------------------|-----|-----|-----|
| | von | Uhr | bis | Uhr |
| Montag bis Donnerstag | | | | |
| Freitag | | | | |

Weitere Vereinbarungen gemäß Anlage Nr. _____.

4.1.2 Abweichende Regelungen für die Bestimmung und Vergütung von Personentagessätzen

Abweichend von Ziffer 9.2.4 Satz 2 EVB-IT Dienstleistungs-AGB können bei entsprechendem Nachweis pro Kalendertag bis zu 10 Stunden abgerechnet werden.

Abweichend von Ziffer 9.2.4 Sätze 2 und 3 Dienstleistungs-AGB kann ein voller Tagessatz nur in Rechnung gestellt werden, wenn mindestens 10 Stunden geleistet wurden. Werden weniger als 10 Zeitstunden pro Tag geleistet, sind diese anteilig in Rechnung zu stellen.

abweichend von Ziffer 9.2.4 gelten folgende Vereinbarungen gemäß Anlage Nr. _____.

4.1.3 Reisekosten/Nebenkosten*/Materialkosten/Reisezeiten

Reisekosten werden nicht gesondert vergütet

Reisekosten werden vergütet gemäß Anlage Nr. 2a

Nebenkosten werden nicht gesondert vergütet

Nebenkosten werden vergütet gemäß Anlage Nr.

Materialkosten werden nicht gesondert vergütet

Materialkosten werden vergütet gemäß Anlage Nr. _____.

Reisezeiten werden nicht gesondert vergütet.

Reisezeiten werden zu 50 % als Arbeitszeiten vergütet.

Reisezeiten werden vergütet gemäß Anlage Nr. 2a.

4.1.4 Preisanpassung

Es wird eine Preisanpassung

gemäß Ziffer 9.5 EVB-IT Dienstleistungs-AGB

gemäß Anlage Nr.

gemäß Ziffer 3.1 Dataport AVB

vereinbart.

4.1.5 Fälligkeit und Zahlung

Die Vergütung ist abweichend von Ziffer 9.3 EVB-IT Dienstleistungs-AGB nicht monatlich nachträglich fällig, sondern

zum 15. des auf die Leistungserbringung folgenden Monats.

wie folgt _____.

gemäß § 7 Abs. 4 Dataport Benutzungsordnung.

4.1.6 Besondere Bestimmungen zur Vergütung nach Aufwand

Besondere Bestimmungen zur Vergütung nach Aufwand sind in Anlage Nr. _____ vereinbart.

EVB-IT Dienstvertrag



Vertragsnummer/Kennung Auftraggeber 1 _____

Vertragsnummer/Kennung Auftraggeber 2 _____

Vertragsnummer/Kennung Auftragnehmer V21706/1090200/3011110

Seite 9 von 17

4.2 Vergütung zum Pauschalfestpreis gem. Anlage 2b

- Die Leistungen gemäß Nummer 3.1 lfd. Nr. _____ werden zum Pauschalfestpreis in Höhe von insgesamt _____ Euro vergütet.
- Es werden folgende Abschlagszahlungen vereinbart:
Betrag: _____ Anlass: _____.
Betrag: _____ Anlass: _____.
Betrag: _____ Anlass: _____.
 Oracle Leistungen:

4.3 Rechnungsadresse gem. Anlage 1a-1b

Rechnungen sind an folgende Anschrift zu richten:

5 Service- und Reaktionszeiten*

- Für die Leistungen gemäß Nummer 3.1 lfd. Nr. 1-3 werden folgende Service- und Reaktionszeiten* vereinbart:

5.1 Servicezeiten*

| Tag | | Uhrzeit | | | |
|---------------|-----|---------|-----|--|-----|
| | bis | | von | | bis |
| | bis | | von | | bis |
| | bis | | von | | bis |
| An Sonntagen | | | von | | bis |
| An Feiertagen | | | von | | bis |

- Vereinbarungen zu Servicezeiten* gemäß SLA VI Pkt. 2.2.2

5.2 Reaktionszeiten*

| Leistung gemäß Nummer 3.1 | Anlass/Problemkategorie | Reaktionszeit* in Stunden |
|---------------------------|-------------------------|---------------------------|
| | | |
| | | |
| | | |

- Die Reaktionszeiten* werden in Anlage Nr. SLA VI A Pkt. 2.3.1 festgelegt.

Reaktionszeiten* beginnen ausschließlich mit Zugang der entsprechenden Meldung oder dem Eintritt des vereinbarten Ereignisses während der vereinbarten Servicezeiten* und laufen ausschließlich während der vereinbarten Servicezeiten*. Ergänzend können in Nummer 12 für die Nichteinhaltung der o.g. Zeiten Vertragsstrafen vereinbart werden.

EVB-IT Dienstvertrag



Vertragsnummer/Kennung Auftraggeber 1 _____

Vertragsnummer/Kennung Auftraggeber 2 _____

Vertragsnummer/Kennung Auftragnehmer V21706/1090200/3011110

Seite 10 von 17

6 Ansprechpartner gem. Anlage 1a-1b

Ansprechpartner des Auftraggebers (Name, Adresse, Abteilung, Telefon, Fax, E-Mail):

Ansprechpartner des Auftragnehmers (Name, Adresse, Abteilung, Telefon, Fax, E-Mail):

7 Besondere Anforderungen an Mitarbeiter des Auftragnehmers

- Mindestanforderungen an das einzusetzende Personal des Auftragnehmers:

| Lfd. Nr. | Position | Schlüsselposition ge- mäß Ziffer 8.3 EVB- IT Dienstleistungs- AGB (ja/nein) | Fachliche Qualifika- tion | Sicherheits- überprüfung Ü 1, 2 oder 3 ³ | Sonstige Anforde- rungen, z.B. weitere Sicherheitsanforde- rungen |
|-------------|----------|---|------------------------------|--|---|
| 1 | 2 | 3 | 4 | 5 | 6 |
| | | | | | |
| | | | | | |
| | | | | | |

- Abweichend von Ziffer 8.1 EVB-IT Dienstleistungs-AGB ist der Auftragnehmer verpflichtet, für die Leistungen gemäß Nummer 3.1 lfd. Nr. _____ nur Personal einzusetzen, welches bereit ist, sich aufgrund des Verpflichtungsgesetzes verpflichten zu lassen.
- Abweichend von Ziffer 8.1 EVB-IT Dienstleistungs-AGB ist der Auftragnehmer berechtigt, für die Leistungen gemäß Nummer 3.1 lfd. Nr. _____ auch Personal einzusetzen, welches lediglich in folgender Sprache zu kommunizieren in der Lage ist: _____.
- Mindestanforderungen an das einzusetzende Personal des Auftragnehmers ergeben sich aus Anlage Nr. _____.

8 Mitwirkungs- und Beistelleistungen des Auftraggebers

- Folgende Mitwirkungsleistungen des Auftraggebers werden abweichend und zusätzlich zu Ziffer 14 EVB-IT Dienstleistungs-AGB vereinbart:

8.1 Anlage 1a-1b Ansprechpartner

Der Auftraggeber benennt gemäß Anlage 1a-1b mindestens zwei Mitarbeiterinnen/Mitarbeiter, die dem Auftragnehmer als Ansprechpartnerinnen/Ansprechpartner zur Verfügung stehen.

Änderungen der Anlage 1a-1b Ansprechpartner sind unverzüglich in Textform mitzuteilen. Hierfür wird eine neue Anlage 1a-1d vom Auftraggeber ausgefüllt. Die Anlage wird auf Anforderung durch den Kundenbetreuer zur Verfügung gestellt. Die neue Anlage ist an _____ zu senden.

- Die Mitwirkungsleistungen des Auftraggebers ergeben sich abweichend und zusätzlich zu Ziffer 14 EVB-IT Dienstleistungs-AGB SLA VI A Pkt. 1.2, SLA VI B Pkt. 1.4, und SSLA A Pkt. 5.2

³ Stufen der Sicherheitsüberprüfung gemäß Sicherheitsüberprüfungsgesetz

Vertragsnummer/Kennung Auftraggeber 1 _____

Vertragsnummer/Kennung Auftraggeber 2 _____

Vertragsnummer/Kennung Auftragnehmer V21706/1090200/3011110

Seite 11 von 17

8.2 Folgende weitere Beistelleistungen werden vereinbart:

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

9 Abweichende Nutzungsrechte an den Leistungsergebnissen, Erfindungen

Für folgende Leistungsergebnisse werden von Ziffer 3 EVB-IT Dienstleistungs-AGB abweichende Nutzungsrechte vereinbart:

- Abweichend von Ziffer 3 EVB-IT Dienstleistungs-AGB gelten folgende abweichende Nutzungsrechte:

Der Auftragnehmer räumt dem Auftraggeber das nicht ausschließliche, dauerhafte, unwiderrufliche und nicht übertragbare Recht ein, die im Rahmen des Vertrages gelieferte Software und sonstige verkörperten Dienstleistungsergebnisse für eigene Zwecke zu nutzen, sofern es sich nicht um Standardsoftware anderer Hersteller handelt.

Bei Standardsoftware anderer Hersteller gelten die jeweils zum Zeitpunkt der Bestellung gültigen Lizenzbedingungen und Produktbenutzungsrechte des Softwareherstellers oder Zulieferers des Auftragnehmers.

- Für alle Ergebnisse der Leistungen gemäß Nummer 3.1 gilt Ziffer 3.1 EVB-IT Dienstleistungs-AGB mit der Maßgabe, dass statt des dort aufgeführten nicht ausschließlichen Nutzungsrechts ein ausschließliches Nutzungsrecht gewährt wird, vorbestehende Werke jedoch ausgenommen.
- Für folgende Ergebnisse der Leistungen gemäß Nummer 3.1 gilt Ziffer 3.1 EVB-IT Dienstleistungs-AGB mit der Maßgabe, dass statt des dort aufgeführten nicht ausschließlichen Nutzungsrechts ein ausschließliches Nutzungsrecht gewährt wird, vorbestehende Werke jedoch ausgenommen: _____.
- Für alle Ergebnisse der Leistungen gemäß Nummer 3.1 gilt Ziffer 3.1 EVB-IT Dienstleistungs-AGB mit der Maßgabe, dass eine gewerbliche Verbreitung uneingeschränkt möglich ist.
- Für folgende Ergebnisse der Leistungen gemäß Nummer 3.1 gilt Ziffer 3.1 EVB-IT Dienstleistungs-AGB mit der Maßgabe, dass eine gewerbliche Verbreitung uneingeschränkt möglich ist, _____.
- Für alle Ergebnisse der Leistungen gemäß Nummer 3.1 gilt Ziffer 3.1 EVB-IT Dienstleistungs-AGB mit der Maßgabe, dass jegliche gewerbliche Verbreitung ausgeschlossen ist.
- Für folgende Ergebnisse der Leistungen gemäß Nummer 3.1 gilt Ziffer 3.1 EVB-IT Dienstleistungs-AGB mit der Maßgabe, dass jegliche gewerbliche Verbreitung ausgeschlossen ist: _____.
- Für Erfindungen, die anlässlich der Vertragserfüllung gemacht werden, gelten abweichend von Ziffer 4 EVB-IT Dienstleistungs-AGB die Regelungen in Anlage Nr. _____.

10 Quellcode*

Im Falle der Erstellung oder Bearbeitung von Software:

- ist gemäß Ziffer 3.6 EVB-IT Dienstleistungs-AGB der jeweils aktuelle Stand der Software, einschließlich der Quellcodes* auf folgendem vom Auftraggeber zur Verfügung gestellten Quellcoderepository zu speichern:
_____.
- wird abweichend von Ziffer 3.6 EVB-IT Dienstleistungs-AGB der jeweils aktuelle Stand der Software, einschließlich der Quellcodes* wie folgt gespeichert und dem Auftraggeber zur Verfügung gestellt: _____.
- wird abweichend von Ziffer 3.6 EVB-IT Dienstleistungs-AGB der jeweils aktuelle Stand der Software, einschließlich der Quellcodes* nicht täglich sondern _____ (z.B. am Ende jeder Arbeitswoche) abgespeichert.
- erfolgt die Übergabe des Quellcodes* auch am Ende jedes Leistungsmonats in elektronischer Form auf einem Datenträger.

Vertragsnummer/Kennung Auftraggeber 1 _____

Vertragsnummer/Kennung Auftraggeber 2 _____

Vertragsnummer/Kennung Auftragnehmer V21706/1090200/3011110

Seite 12 von 17

11 Abweichende Haftungsregelungen

- Abweichend von Ziffer 13.1 EVB-IT Dienstleistungs-AGB beträgt die Haftungsobergrenze bei leicht fahrlässigen Pflichtverletzungen
 - pro Schadensfall _____ Euro.
 - insgesamt für diesen Vertrag _____ Euro.
- Abweichend von Ziffer 13.1 EVB-IT Dienstleistungs-AGB gelten für die Haftung bei leicht fahrlässigen Pflichtverletzungen die Regelungen gemäß Anlage Nr. _____.
- Abweichend von Ziffer 13.3 EVB-IT Dienstleistungs-AGB haftet der Auftragnehmer auch für entgangenen Gewinn.
- Abweichend von Ziffer 13 EVB-IT Dienstleistungs-AGB gelten folgende Haftungsregelungen:

Die Haftung der Vertragsparteien ist, gleich aus welchem Rechtsgrunde, auf insgesamt 10% des Leistungsentgelts beschränkt. Bei Verträgen über wiederkehrende und dauernde Leistungen wird das jährliche Leistungsentgelt zu Grunde gelegt; ist die Laufzeit oder Mindestlaufzeit kürzer, so ist das auf diesen Zeitraum entfallende Leistungsentgelt maßgeblich. Die vorstehenden Beschränkungen gelten nicht bei Vorsatz, grober Fahrlässigkeit, bei der Verletzung des Lebens, des Körpers, der Gesundheit oder soweit das Produkthaftungsgesetz zur Anwendung kommt.

12 Vertragsstrafen

- Als vertragsstrafenrelevant im Sinne von Ziffer 10.3 EVB-IT Dienstleistungs-AGB gelten die in Nummer 3.1 lfd. Nr. _____ vereinbarten Leistungstermine.
- Abweichend von Ziffer 10.3 EVB-IT Dienstleistungs-AGB wird für Leistungen gemäß Nummer 3.1 lfd. Nr. _____ die Vertragsstrafenregelung gemäß Anlage Nr. _____ vereinbart.
- Für die Nichteinhaltung von Reaktionszeiten* gilt die Vertragsstrafenregelung aus Ziffer 10.4 EVB-IT Dienstleistungs-AGB.
- Für die Nichteinhaltung von Reaktionszeiten* gelten die Regelungen in Anlage Nr. _____.
- Für jeden Verstoß gegen Ziffer 1.5 oder Ziffer 1.6 der EVB-IT Dienstleistungs-AGB wird eine Vertragsstrafe in Höhe von _____ Euro vereinbart. Dies gilt nicht, wenn der Auftragnehmer den Verstoß nicht zu vertreten hat.
- Für jeden Verstoß des Auftragnehmers gegen die Regelung im ersten Aufzählungspunkt der Ziffer 8.3 EVB-IT Dienstleistungs-AGB wird eine Vertragsstrafe in Höhe von _____ Euro vereinbart. Dies gilt nicht, wenn der Auftragnehmer den Verstoß nicht zu vertreten hat.
- Vertragsstrafen werden ausgeschlossen.

Vertragsnummer/Kennung Auftraggeber 1 _____

Vertragsnummer/Kennung Auftraggeber 2 _____

Vertragsnummer/Kennung Auftragnehmer V21706/1090200/3011110

Seite 13 von 17

13 Weitere Regelungen

13.1 Datenschutz, Geheimhaltung und Sicherheit

Der Auftragnehmer verpflichtet sich für die Laufzeit des Vertrages

- bei der Erbringung der vertraglichen Leistungen die Regelungen zur IT-Sicherheit gemäß Anlage Nr. _____ zu beachten.
- der Geheimschutzbetreuung gemäß Anlage Nr. _____ zu unterstellen.
- die Regelungen des Auftraggebers zur Sicherheit am Einsatzort gemäß Anlage Nr. _____ zu beachten.
- folgende weitere Regelungen einzuhalten: _____.
- Ergänzend zu bzw. abweichend von Ziffer 19 EVB-IT Dienstleistungs-AGB ergeben sich Regelungen zur Geheimhaltung bzw. zur Sicherheit aus Anlage Nr. _____.
- Da durch den Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers verarbeitet werden sollen (Auftragsverarbeitung), treffen die Parteien in Anlage Nr. _____ eine schriftliche Vereinbarung, die zumindest die gesetzlichen Mindestanforderungen beinhaltet.
- Die Parteien treffen sonstige Vereinbarungen zum Datenschutz gemäß Anlage Nr. _____.

13.2 Haftpflichtversicherung

- Der Nachweis einer Haftpflichtversicherung gemäß Ziffer 18 EVB-IT Dienstleistungs-AGB wird vereinbart.

13.3 Teleservice*

- Soweit der Auftragnehmer zur Leistung durch Teleservice* berechtigt ist, wird er diesen ausschließlich aufgrund der Teleservicevereinbarung gemäß Anlage Nr. _____ erbringen und darf dabei ausschließlich folgendes automatisiertes Verfahren einsetzen: _____ (Produktbezeichnung). Dieses Verfahren muss neben den Anforderungen aus Ziffer 1.5 EVB-IT Dienstleistungs-AGB auch den Anforderungen aus der Anlage Nr. _____ genügen.

13.4 Dokumentations- und Berichtspflichten

- Abweichend von Ziffer 6 EVB-IT Dienstleistungs-AGB dokumentiert der Auftragnehmer die Leistungen gemäß Nummer 3.1 lfd. Nr. _____ nicht in deutscher, sondern in _____ Sprache.
- Weitere Dokumentations- und Berichtspflichten des Auftragnehmers ergeben sich aus Anlage Nr. _____.

13.5 Interessenkonflikt

- Regelungen zur Vermeidung eines Interessenskonfliktes ergeben sich aus Anlage Nr. _____.

14 Pflichten nach Vertragsende

- Ergänzend zu Ziffer 16 EVB-IT Dienstleistungs-AGB ergeben sich weitere Vereinbarungen zu den Pflichten des Auftragnehmers nach Vertragsende aus Anlage Nr. _____.

15 Sonstige Vereinbarungen

15.1 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.bmwk.de zur Einsichtnahme bereit.

Vertragsnummer/Kennung Auftraggeber 1 _____

Vertragsnummer/Kennung Auftraggeber 2 _____

Vertragsnummer/Kennung Auftragnehmer V21706/1090200/3011110

Seite 14 von 17

15.2 Umsatzsteuer

15.2.1 Umsatzsteuer für Leistungen, die bis zum 31.12.2024 erbracht werden

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

15.2.2 Umsatzsteuer für Leistungen, die ab dem 01.01.2025 erbracht werden (gilt für AG1)

Die aus diesem Vertrag seitens des Auftragnehmers zu erbringenden Leistungen unterliegen nicht der Umsatzsteuer, da diese aufgrund des Gesetzes zur Gewährleistung der digitalen Souveränität der Freien Hansestadt Bremen nur von juristischen Personen des öffentlichen Rechts erbracht werden dürfen (§ 2b Abs. 3 Nr. 1 UStG). Ausgenommen sind Leistungen auf dem Gebiet des Telekommunikationswesens (§ 2b Abs. 4 Nr. 5 UStG in Verbindung mit Anhang 1 Nr. 1 der RL 2006/112 EG vom 28.11.2006) sowie die Lieferung von neuen Gegenständen, insbesondere Hardware (§ 2b Abs. 4 Nr. 5 UStG in Verbindung mit Anhang 1 Nr. 6 der RL 2006/112 EG vom 28.11.2006), die stets steuerbar und –pflichtig sind. Bundesrechtliche Regelungen, wonach einzelne Leistungen juristischen Personen des öffentlichen Rechts vorbehalten sind (wie § 20 Abs. 3 FVG oder § 126 GBO) bleiben unberührt. Diese Leistungen sind weiterhin nicht steuerbar. Sollte sich durch Änderungen tatsächlicher oder rechtlicher Art oder durch Festsetzung durch eine Steuerbehörde dennoch eine Umsatzsteuerpflicht ergeben und der Auftragnehmer insoweit durch eine Steuerbehörde in Anspruch genommen werden, hat der Auftraggeber dem Auftragnehmer die gezahlte Umsatzsteuer in voller Höhe zu erstatten, ggf. auch rückwirkend.

15.2.3 Umsatzsteuer für Leistungen, die ab dem 01.01.2025 erbracht werden (gilt für AG2)

Die aus diesem Vertrag seitens des Auftragnehmers zu erbringenden Leistungen unterliegen nicht der Umsatzsteuer, da diese aufgrund des Gesetzes zur Gewährleistung der digitalen Souveränität der Freien Hansestadt Bremen nur von juristischen Personen des öffentlichen Rechts erbracht werden dürfen (§ 2b Abs. 3 Nr. 1 UStG). Ausgenommen sind Leistungen auf dem Gebiet des Telekommunikationswesens (§ 2b Abs. 4 Nr. 5 UStG in Verbindung mit Anhang 1 Nr. 1 der RL 2006/112 EG vom 28.11.2006) sowie die Lieferung von neuen Gegenständen, insbesondere Hardware (§ 2b Abs. 4 Nr. 5 UStG in Verbindung mit Anhang 1 Nr. 6 der RL 2006/112 EG vom 28.11.2006), die stets steuerbar und –pflichtig sind. Bundesrechtliche Regelungen, wonach einzelne Leistungen juristischen Personen des öffentlichen Rechts vorbehalten sind (wie § 20 Abs. 3 FVG oder § 126 GBO) bleiben unberührt. Diese Leistungen sind weiterhin nicht steuerbar. Sollte sich durch Änderungen tatsächlicher oder rechtlicher Art oder durch Festsetzung durch eine Steuerbehörde dennoch eine Umsatzsteuerpflicht ergeben und der Auftragnehmer insoweit durch eine Steuerbehörde in Anspruch genommen werden, hat der Auftraggeber dem Auftragnehmer die gezahlte Umsatzsteuer in voller Höhe zu erstatten, ggf. auch rückwirkend.

15.3 Verschwiegenheitspflicht

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

15.4 Bremer Informationsfreiheitsgesetz (gilt für AG2)

Dieser Vertrag unterliegt dem Bremer 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.

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.

15.5 Ablösungen von Vereinbarungen/ Vorvereinbarungen

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

Vertragsnummer/Kennung Auftraggeber 1 _____

Vertragsnummer/Kennung Auftraggeber 2 _____

Vertragsnummer/Kennung Auftragnehmer V21706/1090200/3011110

Seite 15 von 17

15.6 Weisungen

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

15.7 Verwendung der vertraglichen Leistungen

Der Auftraggeber bestätigt, dass die in diesem Vertrag bezogenen Leistungen durch den Auftraggeber

- ausschließlich im Rahmen seiner Geschäftstätigkeit/ seiner öffentlich-rechtlichen Aufgabenwahrnehmung,
- nicht in einem Betrieb gewerblicher Art und
- nicht im Rahmen von Vermögensverwaltung (z.B. Vermietung) genutzt werden.

15.8 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.

15.9 ITJG (gilt für AG1)

Der Auftragnehmer unterliegt als Auftragsdatenverarbeiter den Regelungen des §17 LDS SH. Gesonderte Aufwände, die im Rahmen der in der Anlage 4 beschriebenen Leistungen erbracht werden, sind nicht in der Kalkulation dieses Vertrages enthalten und werden anlassbezogen gesondert vergütet und separat vereinbart. Die Vertragsparteien sind sich einig, dass eine Anpassung des Vertrages erfolgt, sofern dies notwendig wird, um Anregungen der IT-Kontrollkommission aufzugreifen, die diese im Rahmen von Anhörungen nach §7 Abs. 1 ITJG äußert. Die Vertragsparteien sind sich außerdem einig, dass zukünftige Anpassungen der Anlage ITJG auch auf diesen Vertrag anzuwenden sind.

15.10 Beauftragung, Service und Support

Zukünftige Ausgestaltungsbedarfe werden nach Vertragsschluss zwischen Auftraggeber und Auftragnehmer regelmäßig abgestimmt und ggf. über Änderungsvertragsvorgehen aufgenommen.

Vor Beauftragung bei Dataport haben alle betroffenen Auftraggeber der gewünschten Anpassung zuzustimmen, sodass der benannte Auftraggeber (gem. Anlage 1a-1b), einen vorabgestimmten Auftrag an Dataport gibt. Der Auftraggeber der gewünschten Anpassung ist für die Herstellung eines auftraggeberseitigen Konsenses verantwortlich.

15.11 Festlegung von Auftragsberechtigten

Die Benennung von Auftragsberechtigten zur Erteilung von Aufträgen bzw. ergänzenden Weisungen zu technischen und organisatorischen Maßnahmen im Rahmen der Auftragsverarbeitung, sind je Auftraggeber notwendig. Eine Abstimmung erfolgt unter den Auftraggebern ohne Beteiligung des Auftragnehmers. Die Benennung der Auftragsberechtigten erfolgt formlos durch die vertraglichen oder fachlichen Ansprechpartner per E-Mail. Bei einer gemeinsamen Beauftragung aller Auftraggeber ist ein zentraler Ansprechpartner zur Beauftragung seitens der Auftraggeber zu benennen.

15.12 Vertragsunterzeichnung

Die Vertragsparteien stimmen unter sich das folgende Vorgehen zur Vertragsunterzeichnung ab. Jeder Auftraggeber erhält eine gleichlautende Abschrift der Vertragsurkunde, die nach Zeichnung an den Auftragnehmer zurückgesendet wird. Der Auftragnehmer sammelt die Urkunden und fügt die gezeichneten Unterschriftenseiten zu einem Gesamtdokument zusammen, das wiederum an die Vertragsparteien verteilt wird. Die Vertragsparteien sind sich einig, dass dieses Vorgehen sich dazu eignet, die Annahme des Vertragsangebotes den anderen Parteien effektiv zu übermitteln.

EVB-IT Dienstvertrag



Vertragsnummer/Kennung Auftraggeber 1 _____

Vertragsnummer/Kennung Auftraggeber 2 _____

Vertragsnummer/Kennung Auftragnehmer V21706/1090200/3011110

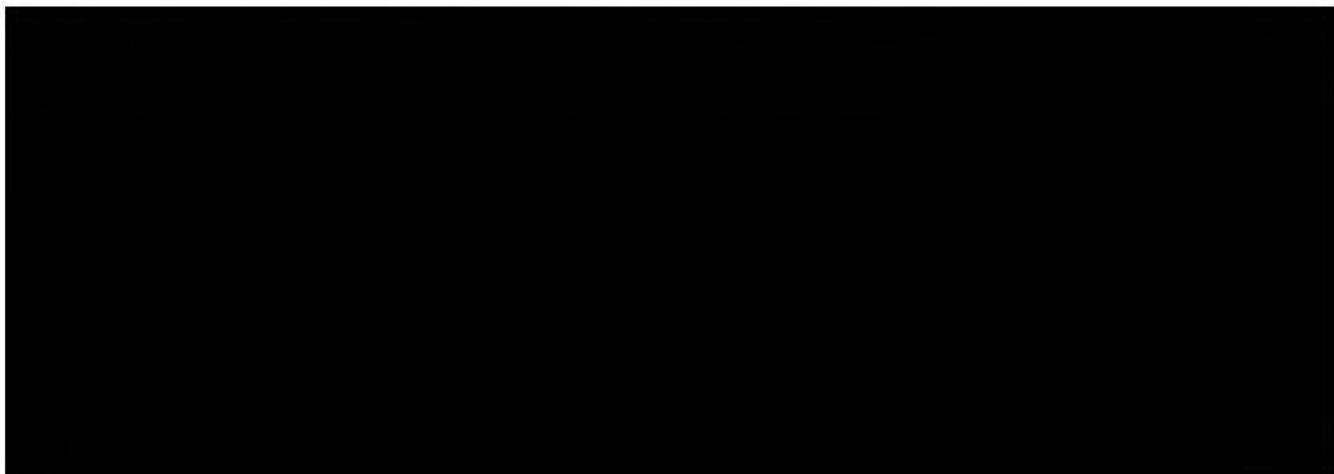
Seite 16 von 17

Auftragnehmer

Auftraggeber 1

Ort, Datum: Altenholz, 13.05.2024 _____

Ort, Datum: _____ , _____



EVB-IT Dienstvertrag



Vertragsnummer/Kennung Auftraggeber 1 _____

Vertragsnummer/Kennung Auftraggeber 2 _____

Vertragsnummer/Kennung Auftragnehmer V21706/1090200/3011110

Seite 17 von 17

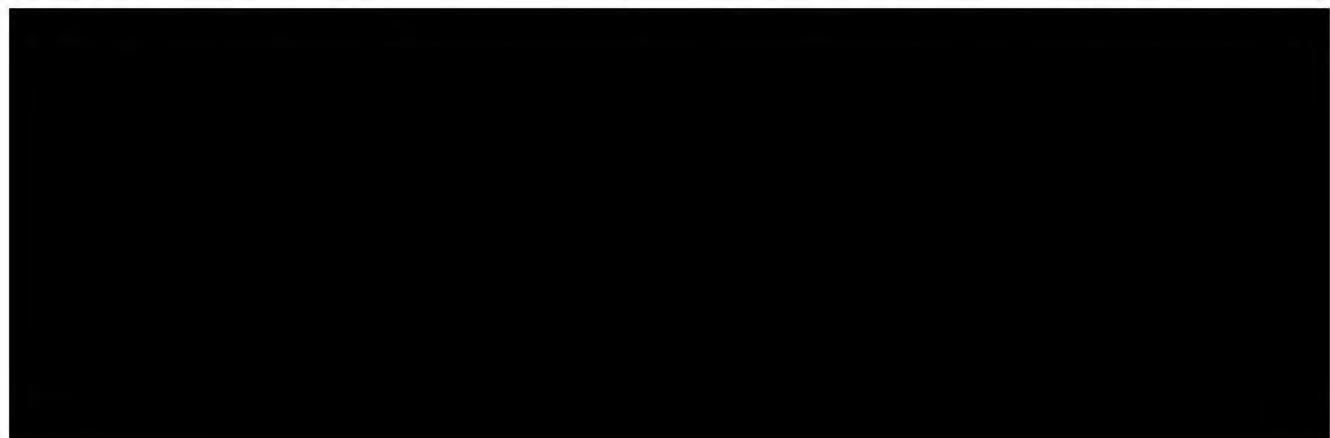
Auftragnehmer

Auftraggeber 2

Ort, Datum: Altenholz, 13.05.2024

Ort, Datum: Bremen,

24.05.2024



Ansprechpartner
zum Vertrag über die Beschaffung von IT-Dienstleistungen

Vertragsnummer/Kennung Auftraggeber: ITWeb113664V

Auftraggeber:
**Ministerium für Justiz und Gesundheit
des Landes Schleswig Holstein
Referat II 35
Lorentzendamm 35
24103 Kiel**

Rechnungsempfänger:
**Ministerium für Justiz und Gesundheit
des Landes Schleswig Holstein
Referat II 35
Lorentzendamm 35
24103 Kiel**

Leitweg-ID

[REDACTED]

Der Rechnungsempfänger ist immer auch der Mahnungsempfänger.

**Zentrale Ansprechpartner des
Auftragnehmers:**

**Vertragliche Ansprechpartner
des Auftraggebers:**

**Fachliche Ansprechpartner des
Auftraggebers:**

1.

2.

**Technische Ansprechpartner
des Auftraggebers:**

1.

2.

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

Ort

, Datum

Ansprechpartner
zum Vertrag über die Beschaffung von IT-Dienstleistungen

Vertragsnummer/Kennung Auftraggeber:

Auftraggeber:

**Die Senatorin für Justiz und Verfassung
Richtweg 16 - 22
28195 Bremen**

Rechnungsempfänger:

**Freie Hansestadt Bremen
- Rechnungseingang FHB -
Senatorin für Justiz und Verfassung
28026 Bremen**

Leitweg-ID

[REDACTED]

Der Rechnungsempfänger ist immer auch der Mahnungsempfänger.

**Zentrale Ansprechpartner des
Auftragnehmers:**

**Vertragliche Ansprechpartner
des Auftraggebers:**

**Fachliche Ansprechpartner des
Auftraggebers:**

1.

[REDACTED]

2.

**Technische Ansprechpartner
des Auftraggebers:**

1.

2.

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

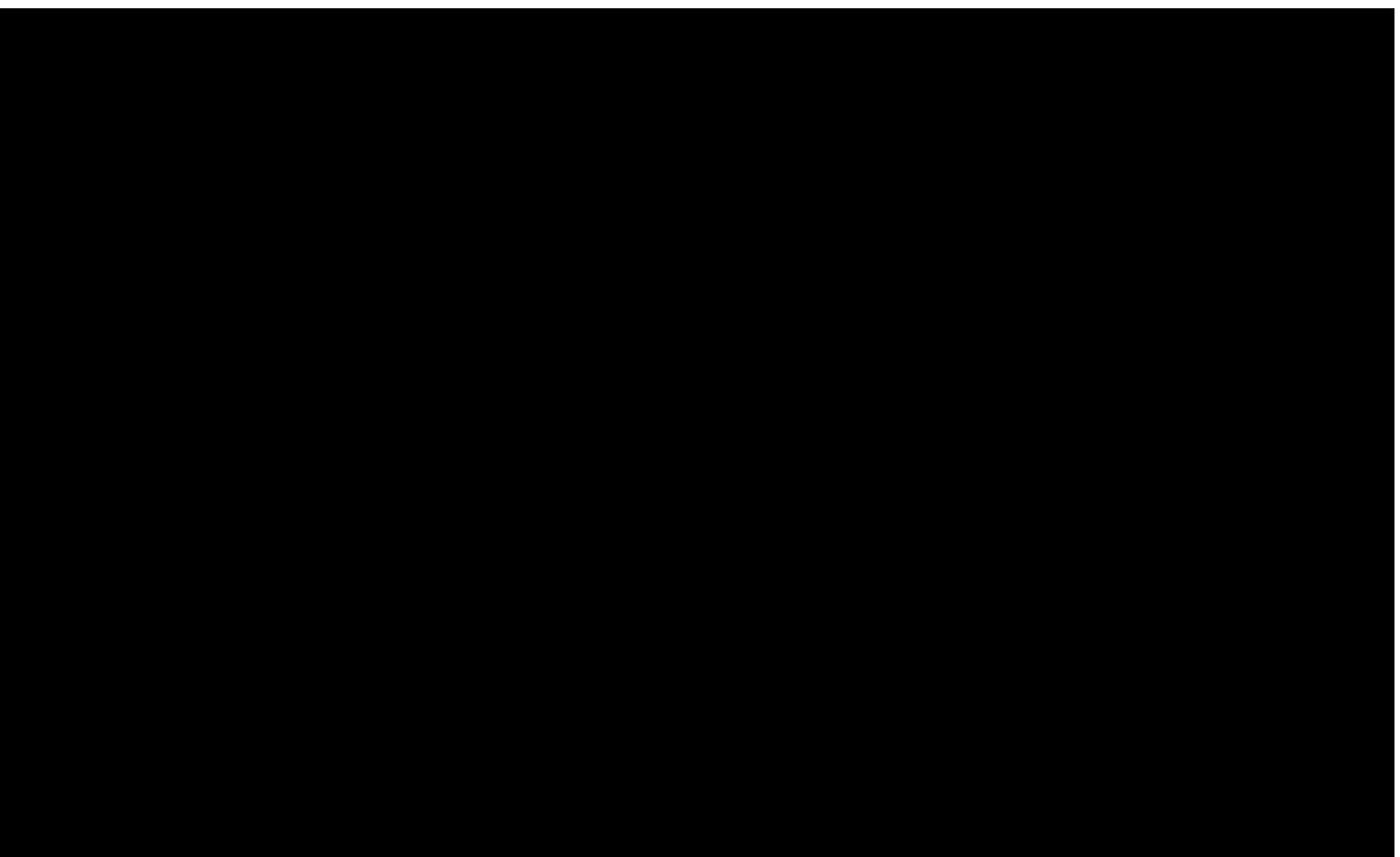
Preisblatt Aufwände

Gültig ab dem 01.04.2024

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

Pos. 10-90: Mit einer jährlichen Obergrenze von 5.000,00 €.

Pos. 100-110: Mit einer jährlichen Obergrenze von 5.000,00 €.



Die Abrechnung erfolgt nach Aufwand.

Pos. 10-20: Die Rechnungsstellung erfolgt pauschal kalendermonatlich nachträglich gem. Kundenauftrag.

Pos. 30-80: Die Rechnungsstellung erfolgt kalendermonatlich nachträglich gem. Leistungsnachweis.

Pos. 90: Die Rechnungsstellung erfolgt kalendermonatlich nachträglich gem. Kostennachweis.

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.

Aufwandsleistungen, die über den in Anlage 2b gem. Pos. 150-160 vereinbarten Umfang hinausgehen

Pos. 100-110: Die Abrechnung erfolgt gem. Anlage 2b.

Anmerkungen zu den Positionen

Ergänzende Ausführung für Positionen 10 bis 70:

Die zuvor genannten Artikel dienen der Abbildung von Aufträgen zur Umsetzung außerhalb der in den SLA vereinbarten Supportzeit und umfassen die Tätigkeiten des TVM und ggf. FVM (Positionen 30-70) sowie ggf. relevanter Unterstützungsleistungen der Systemtechnik und/oder des Datenbankbetriebs im Störungsfall (Positionen 10-20).

[REDACTED] umfasst die ergänzenden Zeiten Mo-Fr.

[REDACTED] umfasst die ergänzenden Zeiten feiertags und am Wochenende.

Die Beauftragung an Dataport muss mit einem Vorlauf von mindestens 12 Wochen erfolgen.

Ergänzende Ausführung für Positionen 80 und 90:

Für die Abrechnung von Reiseaktivitäten im Kundenauftrag für Reisen außerhalb des Trägerlandes. Es gelten die Regelungen des BRKG.

Die Kosten werden zwischen Schleswig-Holstein und Bremen nach dem relativierten jeweils gültigen Königsteiner Schlüssel aufgeteilt.

Somit ergibt sich in 2024 nach dem aktuellen Königsteiner Schlüssel von 2019 folgende Aufteilung:

AG1 SH: 78,122 %

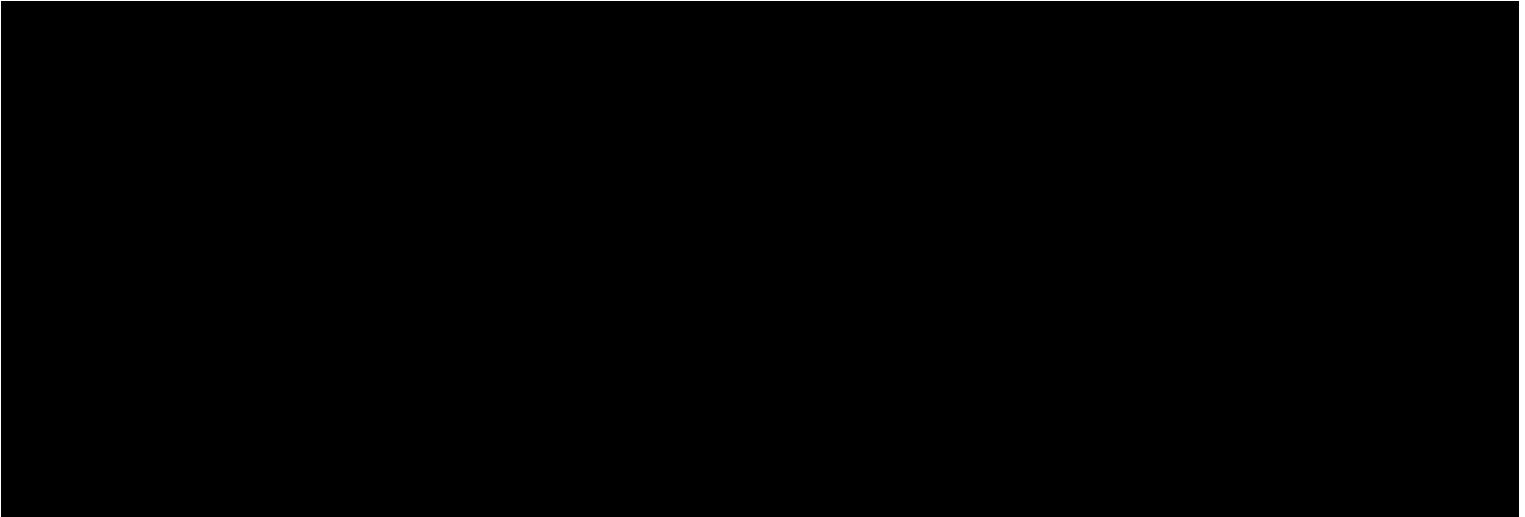
AG2 HB: 21,878 %

Preisblatt Jährlicher Festpreis

Gültig ab dem 01.04.2024

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

Gesamtpreis: 43.912,12 €



Die Rechnungsstellung des Festpreises erfolgt zum 15.06. eines Kalenderjahres.

Anmerkungen zu den Positionen

Die Kosten werden zwischen Schleswig-Holstein und Bremen nach dem relativierten jeweils gültigen Königsteiner Schlüssel aufgeteilt.

Somit ergibt sich in 2024 nach dem aktuellen Königsteiner Schlüssel von 2019 folgende Aufteilung:

AG1 SH: 78,122 %

AG2 HB: 21,878 %

IAP-Nummer: 35601
(wird von Dataport ausgefüllt)

Anlage Datenschutzrechtliche Festlegung des Auftraggebers

Angaben des Verantwortlichen gem. Art. 28 DSGVO zur Auftragsverarbeitung¹

| | |
|---|-------------------------------------|
| Für die Verarbeitung der in Rede stehenden personenbezogenen Daten gelten folgende Datenschutzregelungen: | |
| Verordnung (EU) 2016/679 (DSGVO) | <input checked="" type="checkbox"/> |
| Zusätzlich folgende bundes- bzw. landesrechtliche Regelungen (bitte Gesetz bzw. VO benennen) | <input checked="" type="checkbox"/> |
| BremDSGVOAG sowie Schleswig-Holsteinisches Gesetz zum Schutz personenbezogener Daten - Abschnitte 1 und 2 | |
| Folgende bundes- bzw. landesrechtliche Regelungen zur Umsetzung der RiLi (EU) 2016/680 ² (bitte Gesetz bzw. VO benennen) | <input checked="" type="checkbox"/> |
| 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): BDSG, StPO, OWiG und EGGVG | |
| Es findet keine Verarbeitung personenbezogener Daten statt | <input type="checkbox"/> |

| | |
|-----------|---|
| 1. | Art und Zweck der Verarbeitung (siehe z. B. Art. 28 Abs. 3 S. 1 DSGVO) |
| | Formatwandlung und OCR-Hinterlegung von Dateien unterschiedlicher Ausgangsformate in ein archivfähiges und für die Anzeige durch E-Akten-Programme geeignetes Ziel-PDF-Format. Im Verfahren selbst erfolgt keine weitergehende Speicherung der Daten als für den tatsächlichen Konvertierungsvorgang bis zum Abschluss nötig. |

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

Als Hilfestellung zum Ausfüllen siehe daher:

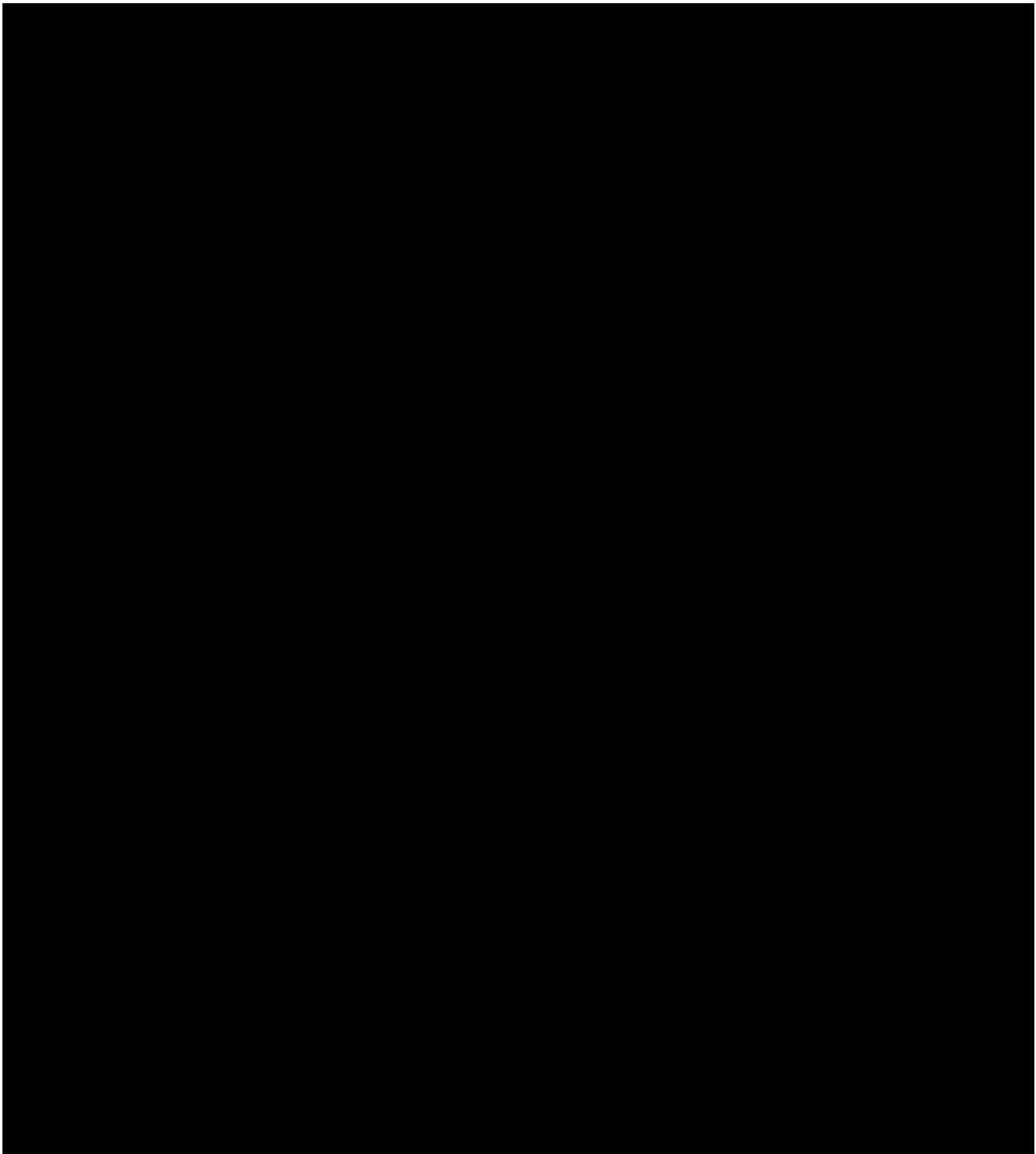
https://www.datenschutzkonferenz-online.de/media/ah/201802_ah_verzeichnis_verarbeitungstaetigkeiten.pdf

² Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.

IAP-Nummer: 35601
(wird von Dataport ausgefüllt)

| | |
|----|---|
| 2. | <p>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)</p> <p>Alle Kategorien von personenbezogenen Daten, die Akteninhalt von gerichtlichen und staatsanwaltschaftlichen Verfahren sein können.</p> <p>darunter folgende Kategorien besonderer personenbezogener Daten (siehe z. B. Art. 9 Abs.1 DSGVO)</p> <p>Im Rahmen der Nachrichtenverarbeitung können im Einzelfall die in Art 9 Abs. 1 DSGVO genannten Kategorien besonderer personenbezogener Daten verarbeitet werden. Für diese gilt die Ausnahmeerlaubnis des Art. 9 Abs. 2 Buchstabe f) DSGVO.</p> |
| 3. | <p>Beschreibung der Kategorien betroffener Personen (siehe z. B. Art. 28 Abs. 3 S. 1 DSGVO)</p> <p>Alle an einem Verfahren aktiv oder passiv beteiligte Personen sowie deren Vertreter. Daneben personenbezogene Daten von Mitarbeiterinnen und Mitarbeiter der Justiz, die das Verfahren nutzen.</p> |
| 4. | <p>Übermittlung von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation (siehe z. B. Art. 30 Abs. 1 S. 2 lit. e DSGVO)</p> <p>./.</p> |

Liste der weiteren Auftragsverarbeiter



Anlage ITJG

**Vereinbarung für den Betrieb von Fachverfahren und
für sonstige IT-Dienstleistungen zur Einhaltung des IT-
Gesetzes für die Justiz des Landes Schleswig-Holstein
(ITJG) nach § 2 Abs. 1 S. 2 i. V. m. § 7 Abs. 1 ITJG**

**Produkt / IT-Dienstleistung: PDF Compressor
(PDFCOMP ML)**

Version: 1.2
Stand: 28.04.2020

Inhaltsverzeichnis

| | | |
|----------|--|----------|
| 1 | Einleitung | 3 |
| 2 | Verpflichtungen zur Umsetzung einzelner Vorgaben im Rahmen des Verfahrensbetriebs und betriebsnaher Unterstützungsleistungen..... | 3 |
| 3 | Verpflichtungen zur Umsetzung einzelner Vorgaben bei sonstigen IT-Dienstleistungen | 7 |

1 Einleitung

Zur Umsetzung der aus dem ITJG resultierenden Anforderungen und Vorgaben verpflichtet sich Dataport als Auftragnehmer (AN) gegenüber dem für Justiz zuständigen Ministerium als Auftraggeber (AG) hiermit auch vertraglich, die Funktionsfähigkeit und die sonstigen besonderen Belange der Justiz sicherzustellen (§ 7 Abs. 1 S. 2 ITJG).

Hierzu verpflichtet sich der AN zur Einhaltung der aus dem ITJG in seiner jeweils geltenden Fassung resultierenden Anforderungen/Vorgaben, insbesondere zur Berücksichtigung und zum Schutz der Funktionsfähigkeit der Justiz und der besonderen Belange der Justiz (vgl. § 2 ITJG) und zur Vornahme aller hierzu erforderlichen Handlungen, Unterlassungen und Duldungen.

Weitergehende Verpflichtungen aus anderen Quellen (insbesondere aus begründeten Benutzungsverhältnissen mit Dataport, Gesetzen, Verordnungen etc.) bleiben unberührt.

Die Umsetzung der einzelnen Vorgaben des ITJG ergeben sich aus:

- Verpflichtungen zur Umsetzung einzelner Vorgaben im Rahmen des Verfahrensbetriebs und betriebsnaher Unterstützungsleistungen (siehe unter 2)
- Verpflichtungen zur Umsetzung einzelner Vorgaben bei sonstigen IT-Dienstleistungen (siehe unter 3)

2 Verpflichtungen zur Umsetzung einzelner Vorgaben im Rahmen des Verfahrensbetriebs und betriebsnaher Unterstützungsleistungen

Der Verfahrensbetrieb und betriebsnahe Unterstützungsleistungen werden in der Rechenzentrumsinfrastruktur des AN durchgeführt. Die im Rahmen des Verfahrensbetriebs erbrachten Leistungen sind in den Service Level Agreements des Betriebsvertrags beschrieben. Zu den betriebsnahen Unterstützungsleistungen zählen u. a. Unterstützungsleistungen unter Verarbeitung von Daten der Justiz wie z. B. Verfahrensmigration oder Datenbankumsetzung.

a) § 2 Abs. 1 S. 2 ITJG i.V.m. § 7 Abs. 1 S. 1 ITJG

Für die in den Gerichten und Staatsanwaltschaften erforderlichen Fachverfahren begründet das für Justiz zuständige Ministerium jeweils eigene Benutzungsverhältnisse gegenüber dem AN. Aufgrund des Charakters des Dienstleistungsverhältnisses überträgt der AN die Ausführung nicht an andere Dienstleister. Eine Berechtigung zur Begründung von Unterauftragsverhältnissen ist ausgeschlossen.

Der AN ist jedoch berechtigt, andere Dienstleister mit Wartungsarbeiten an der Hard- und Software (z.B. Bearbeitung von Tickets im third level Support) zu beauftragen, wenn er die vertraglich geschuldeten Leistungen anderenfalls nicht bzw. nicht in der erforderlichen Qualität (z.B. Performance, Datensicherheit und -schutz) erbringen oder wenn die Einhaltung der jeweiligen Service-Level-Agreements ausnahmsweise nicht mit eigenem Personal erfolgen kann.

Bei Wartungsarbeiten anderer Dienstleister verbleiben die Daten aus den jeweils betroffenen Systemen (Hard- und Software) in jedem Fall beim AN und sind nicht an andere Dienstleister zu übermitteln, von diesen zu speichern, zu verarbeiten oder zu löschen.

Bei der Einschaltung Dritter im Rahmen von Wartungsarbeiten ist die Einhaltung des ITJG durch den AN vertraglich sicherzustellen (§ 2 Abs. 1 S. 2 ITJG).

Der AN teilt dem AG bei Abschluss dieses Vertrages mit, welche IT-Dienstleister eingesetzt werden können. Einen Austausch oder eine Ergänzung innerhalb der Vertragslaufzeit, u.a. bedingt durch die Erforderlichkeit von Neuaußschreibungen aufgrund vergaberechtlicher Vorschriften, teilt der AN dem AG 1 Monat vor Eintritt

der Veränderung mit. Ist der AG mit der Veränderung einverstanden, teilt der AG dies dem AN mit. Sollte der AG nicht innerhalb dieser Frist der Änderung widersprechen, gilt die Änderung als genehmigt. Widerspricht der AG einem neuen IT-Dienstleister, ist der AG berechtigt den Vertrag innerhalb eines Monats ab Zugang der Benachrichtigung ohne Sanktion durch schriftliche Erklärung zum Ende des darauffolgenden Monats zu kündigen. Unterbleibt die Kündigung, gilt die Zustimmung als erteilt.

Der AN sorgt dafür, dass sich alle Personen, die von ihm mit der Bearbeitung oder Erfüllung des Vertrages betraut sind, auf die Einhaltung des ITJG und der daraus resultierenden Maßnahmen und Vorkehrungen verpflichten. Auf Verlangen weist der AN diese Verpflichtungen durch Vorlage geeigneter Unterlagen nach. Der AN stellt außerdem sicher, dass bei den mit Wartungsarbeiten befassten Personen und insbesondere den von ihm zu bestimmenden zugangsberechtigten Administratorinnen und Administratoren „eine obligatorische Sicherheitsüberprüfung“ nach § 15 Abs. 4 Dataport-Staatsvertrag i.V.m. § 34 Hamburgisches Sicherheitsüberprüfungsgesetzes vorausgeht „und dass diese administrativen Tätigkeiten sowie eine Veränderung von Berechtigungen vollumfänglich und revisionssicher protokolliert und die Protokolle der Justizverwaltung als Report zur Verfügung gestellt werden, um etwaige Verstöße gegen das Gesetz umgehend registrieren zu können“ (vgl. Schleswig-Holsteinischer Landtag, Drucksache 18/3224, S. 23). Hierzu werden die Protokolle durch den AN kontrolliert und die Ergebnisse nach Maßgabe des ITJG und der hier geregelten Bestimmungen mitgeteilt. Die regelmäßige Bearbeitungszeit der Sicherheitsüberprüfung liegt bei ca. 8-10 Wochen.

Weitergehende Regelungen (z.B. betreffend Verschlussachen etc.) bleiben unberührt. Bei kurzfristigen Beauftragungen Dritter zur Beseitigung von Betriebsstörungen durch den AN kann eine Sicherheitsüberprüfung nach § 15 Abs. 4 Dataport-Staatsvertrag entfallen, wenn das Fremdpersonal durch sicherheitsüberprüftes Personal des AN begleitet wird. Für die Beseitigung der Betriebsstörung erforderliche Fernzugriffe werden im Wege eines 4-Augen-Prinzips vom AN begleitet und überwacht. Zur Vermeidung von Rechtsverstößen liegt die Kontrolle über die Fernwartungssitzung dabei stets bei einer Administratorin oder einem Administrator des AN, der die Sitzung jederzeit unterbrechen kann. Die Einhaltung weitergehender Verpflichtungen aus anderen Quellen, insbesondere Geheimhaltungsverpflichtungen (z.B. Steuer-, Sozial-, Fernmeldegeheimnis etc.) einschließlich des Datengeheimnisses nach dem ITJG bleiben hiervon unberührt.

Erforderliche Testungen sind vom Auftragnehmer und mit fiktiven Testdaten durchzuführen. Sollte eine Testung mit anderen Daten, u.a. Echtdaten notwendig sein, werden die Testdaten vom AG geliefert und die Verwendung dieser Daten hierdurch genehmigt.

b) § 2 Abs. 2 ITJG

Die IT-Strukturen der Gerichte und Staatsanwaltschaften sind von denen der Landesverwaltung technisch zu trennen. Hierzu werden dedizierte Systeme und Datenbankinstanzen eingesetzt, die eine physische oder logische Trennung von anderen IT-Verfahren gewährleisten.

Bei Bereitstellung und Betreuung der in den Gerichten und Staatsanwaltschaften zum Einsatz kommenden IT ist unter Beachtung des Stands der Technik, insbesondere der in § 2 Abs. 2 ITJG geregelten Maßgaben, sicherzustellen, dass jeglicher Einblick in die richterliche, rechtspflegerische oder staatsanwaltschaftliche Tätigkeit unterbleibt.

c) § 2 Abs. 2 S. 2 Nr. 1 ITJG

Es sind berechtigte Inhaberinnen und Inhaber administrativer Zugänge zu bestimmen und die Bedingungen einer darüber hinaus erforderlichen Öffnung für weitere administrativ berechtigte Personen sind festzulegen. Für den Fall einer unbefugten Öffnung ist eine Information der IT-Kontrollkommission (§ 5 ITJG) und der betroffenen Gerichte und Staatsanwaltschaften sowie ein Verfahren zur Änderung der Zugangsgewährung vorzusehen.

Hierzu werden vom AN administrative Rollen mit minimalen Datenzugriffsberechtigungen versehen und in einem geordneten Prozess zentral vergeben (Rollen-, Rechte- und Berechtigungsmanagement). Die korrekte Zuweisung administrativer Rollen zu namentlich festgelegten Administratorinnen und

Administratoren wird durch Linienvorgesetzte des AN regelmäßig überprüft (Revision vergebener Berechtigungen). Alle Beschäftigten des AN sowie externes für den AN tätiges Personal werden vor Aufnahme der Tätigkeit neben dem allgemeinen Amtsgeheimnis auch auf das datenschutzrechtliche Datengeheimnis sowie bereichsspezifische Geheimhaltungsverpflichtungen (z.B. Steuer-, Sozial-, Fernmeldegeheimnis etc.) einschließlich der Anforderungen nach dem ITJG verpflichtet. Für den Fall einer unbefugten Öffnung des Kreises der zugangsberechtigten Personen werden der AG und die IT-Kontrollkommission vom AN unterrichtet.

d) § 2 Abs. 2 S. 2 Nr. 2 ITJG

Der AN stellt sicher, dass die im Rahmen richterlicher, rechtspflegerischer oder staatsanwaltlicher Tätigkeit erstellten Dokumente von den Administratorinnen und Administratoren weder eingesehen noch an Dritte weitergegeben werden, insbesondere nicht an die in § 1 Absatz 1 ITJG genannten Stellen oder an die diesen nachgeordneten Stellen der Dienstaufsicht.

Berechtigten Administratorinnen und Administratoren kann aus betrieblichen Gründen je nach Rolle der Zugriff auf die Daten und damit die Möglichkeit der unautorisierten Weitergabe nicht entzogen werden. Sie werden per Belehrung und Verpflichtung auf das einschlägige Verbot aus dem ITJG hingewiesen. Im Rahmen des Internen Kontrollsystens des AN werden Protokolldateien stichprobenartig auf unautorisierte Datenabflüsse überprüft. Bei der Protokollauswertung aufgefallene Verstöße werden als Sicherheitsvorfall behandelt und mit der Priorität „kritisch“ versehen. GemIT und die IT-Kontrollkommission werden unverzüglich unterrichtet.

Eine Datenherausgabe und Datenweitergabe seitens Dataport finden ausschließlich auf Grundlage eines Auftrags des AG oder einer richterlichen Anordnung statt. Jede Datenherausgabe wird über das Sicherheitsvorfallmanagement bearbeitet, dokumentiert und an den AG gemeldet. Sofern die Datenherausgabe im Rahmen des Sicherheitsvorfallmanagements als Sicherheitsvorfall identifiziert wird, werden die GemIT und die IT-Kontrollkommission unverzüglich unterrichtet.

e) § 2 Abs. 2 S. 2 Nr. 3 ITJG

Der AN stellt sicher, dass in gleicher Weise eine Weitergabe von Informationen über Merkmale oder Eigenschaften von den in Nummer 2 genannten Dokumenten (Metadaten) und von systemintern automatisch erstellten Protokollen über die Benutzung der zur Verfügung stehenden IT (Logdateien) ausgeschlossen ist.

Dies wird durch die oben nach Ziff. 2 d) dargestellten Maßnahmen sichergestellt.

f) § 2 Abs. 2 S. 2 Nr. 4 ITJG

Der AN stellt sicher, dass Ausnahmen von den Nummern 2 und 3 zugunsten des für Justiz zuständigen Ministeriums oder der ihm nachgeordneten Stellen der Dienstaufsicht nur gemacht werden, soweit sie zu Zwecken oder auf Veranlassung der jeweiligen Dienstaufsicht im Rahmen bestehender Gesetze zulässig sind; soweit Dokumente laufender Verfahren betroffen sind, sind die Ausnahmen nur zulässig, soweit dies zur Ausübung der Dienstaufsicht unerlässlich ist.

Eine Datenherausgabe und Datenweitergabe seitens des AN finden ausschließlich auf Grundlage eines Auftrags des AG oder einer richterlichen Anordnung statt. Jede Datenherausgabe wird über das Sicherheitsvorfallmanagement bearbeitet, dokumentiert und an den AG gemeldet. Sofern die Datenherausgabe im Rahmen des Sicherheitsvorfallmanagements als Sicherheitsvorfall identifiziert wird, werden die GemIT und die IT-Kontrollkommission unverzüglich unterrichtet.

Um der IT-Kontrollkommission gezielte Prüfungen zu ermöglichen, ob die Vorgaben des § 2 Abs. 2 Nr. 4 ITJG beachtet wurden, unterrichtet der AN die IT-Kontrollkommission, wenn ein Auftrag zur Datenherausgabe und Weitergabe nach § 2 Abs. 2 Satz 2 Nr. 4 ITJG durch den AG erteilt wurde. Diese Unterrichtung beschränkt sich – unbeschadet der Überwachungs-, Zutritts und Einsichtsrechte der IT-Kontrollkommission nach § 5 Abs. 5 und 6 ITJG – zunächst auf die Tatsache, dass ein entsprechender Auftrag erteilt wurde. Diese Unterrichtungspflicht des AN entfällt, wenn der AG dem AN schon im Rahmen

der Auftragserteilung erklärt, dass der AG die IT-Kontrollkommission bereits über den Auftrag unterrichtet hat.

g) § 2 Abs. 2 S. 2 Nr. 5 ITJG

Der AN stellt sicher, dass im Übrigen die in Nummer 2 genannten Dokumente sowie die in Nummer 3 aufgeführten Metadaten und Logdateien von den Administratorinnen und Administratoren nur mit Zustimmung der betroffenen Verfasserin oder Nutzerin oder des betroffenen Verfassers oder Nutzers verwendet werden, es sei denn, die Verwendung ist für die Gewährleistung der Ordnungsmäßigkeit eines automatisierten Verfahrens oder sonst für den Betrieb der IT-Infrastruktur unerlässlich.

Hierzu hat der AN ein Rollen-, Rechte- und Berechtigungsmanagement implementiert. Dieses hat zur Folge, dass Administratorinnen und Administratoren nur Zugriff auf Daten erhalten, die sie für die Gewährleistung des ordnungsgemäßen IT-Betriebs benötigen. Dabei werden Rollen so festgelegt, dass Rollenkonflikte ausgeschlossen sind; zur Sicherstellung der Revisionssicherheit der Protokollierung werden Rollen, bei denen ein Konflikt droht, in getrennten Organisationseinheiten angesiedelt.

h) § 2 Abs. 2 S. 2 Nr. 6 ITJG

Der AN stellt sicher, dass jeder Zugriff protokolliert und dem für Justiz zuständigen Ministerium unverzüglich auf direktem Wege mitgeteilt wird; sofern auf individuell zuordnungsfähige Dokumente zugegriffen wurde, benachrichtigt AG die betroffene Verfasserin oder Nutzerin oder den betroffenen Verfasser oder Nutzer unverzüglich auf direktem Wege und auf dem Dienstweg.

Hierzu stellt der AN mittels seiner Administrationsumgebung des Rechenzentrums (derzeit Smart Auditor) eine lückenlose Protokollierung administrativer Tätigkeiten auf Grundlage der Protokollierungsrichtlinie sicher. Die Mitteilung von Datenzugriffen an den AG erfolgt gemäß den Regelungen des „Protokollierungskonzepts für die Justiz SH“.¹

Unbeschadet dessen erfolgt die Auswertung von Protokollen auf Grundlage der Protokollierungsrichtlinie, konkretisiert durch Protokollierungs- und Protokollauswertungskonzepte des AN, siehe SSLA Teil A. Die Durchführung von Protokollauswertungen zum Zwecke der Sicherstellung der Ordnungsmäßigkeit des IT-Betriebes in Kundenverfahren wird durch den AN dokumentiert. Bei der Protokollauswertung aufgefallene Verstöße gegen das ITJG werden vom AN als Sicherheitsvorfall behandelt und mit der Priorität „kritisch“ versehen. Die GemIT und die IT-Kontrollkommission werden unverzüglich unterrichtet.

i) § 4 Abs. 3 ITJG i.V.m. § 5 Abs. 5 und 6 ITJG

Zum Schutz vor unbefugten Zugriffen dürfen u. a. die GemIT und die IT-Kontrollkommission bei externen Dienstleistern Kontrollen durchführen bzw. sich an den Kontrollen anderer Stellen (vgl. § 4 Abs. 4 ITJG) beteiligen.

Gegenstand der Kontrollen ist die Einhaltung dieses Gesetzes, der bestehenden Verträge und aller sonstigen Bestimmungen, die der Bereitstellung von IT-Infrastrukturen, der Betreuung der eingesetzten IT und der Gewährleistung der IT-Sicherheit in den Gerichten und Staatsanwaltschaften dienen.

Soweit zur Aufgabenerfüllung erforderlich, sind der GemIT/IT-Kontrollkommission zu den vorgenannten Zwecken Zutritt zu gewähren und ein uneingeschränktes Auskunfts- und Einsichtsrecht zu gewährleisten.

Nach § 5 Abs. 6 S. 2 ITJG besteht dieses Recht auch bezüglich derjenigen Akten und Dokumente, die sich auf die Rechtsaufsicht über Dataport oder auf die Begründung und Ausgestaltung der Nutzungsverhältnisse zum AN oder auf die Verträge mit anderen externen IT-Dienstleistern beziehen und die einen wesentlichen Bezug zur Organisation und zum Einsatz von IT in den Gerichten und Staatsanwaltschaften haben. Personenbezogene Daten dürfen im Rahmen von Kontrollen auch ohne Kenntnis der Betroffenen erhoben werden. Dokumente, Dateien und Daten im Sinne des § 2 Absatz 2 Satz

¹ Die Lösung der konfigurativen Technik muss noch entwickelt und in einem gesonderten Auftrag durch den AG beim AN beauftragt werden.

2 Nummer 2 und 3 ITJG dürfen im Rahmen von Kontrollen hingegen durch GemIT nur eingesehen oder sonst verwendet werden, soweit dies zur Aufgabenerfüllung unerlässlich ist.

Hierzu verpflichtet sich der AN der GemIT, der IT-Kontrollkommission bzw. den in § 4 Abs. 4 ITJG genannten Stellen in dem nach § 4 Abs. 3, 4 und 5 ITJG bzw. § 5 Abs. 5 und 6 ITJG geregelten Umfang Zutritt und uneingeschränkt Auskunft und Einsicht zu gewähren, soweit dies zur Aufgabenerfüllung erforderlich ist (§§ 4, 5 ITJG). Der Staatsvertrag über die Errichtung von Dataport als rechtsfähige Anstalt des öffentlichen Rechts vom 27. August 2003 (GVOBI. Schl.-H. S. 557), zuletzt geändert durch Staatsvertrag vom 27. September 2013 (GVOBI. Schl.-H. S. 511) bleibt gem. § 1 Abs. 2 ITJG unberührt.

j) § 4 Abs. 5 ITJG i.V.m. § 5 Abs. 5 S. 2 ITJG

Der AN unterrichtet die GemIT unverzüglich über Sicherheitsvorfälle, die auch oder ausschließlich die Justiz betreffen. Die Unterrichtungspflicht gilt gegenüber der IT-Kontrollkommission entsprechend (§ 5 Abs. 5 S. 2 ITJG).

Hierzu werden entsprechende Sicherheitsvorfälle vom Sicherheitsvorfallmanagement des AN unabhängig von ihrer Auswirkung auf den ordnungsgemäßen IT-Betrieb zunächst als „kritisch“ eingestuft.

k) § 5 Abs. 8 ITJG i.V.m. § 5 Abs. 5 ITJG (Auszug § 5 Abs. 8 ITJG)

Stellt die IT-Kontrollkommission Verstöße gegen die in Absatz 5 genannten Bestimmungen bei den in § 1 Abs. 1 ITJG genannten Stellen fest, fordert sie diese unter Setzung einer angemessenen Frist zur Mängelbeseitigung auf. Werden die Verstöße in dieser Frist nicht abgestellt oder handelt es sich um erhebliche Verstöße, spricht die IT-Kontrollkommission eine Beanstandung aus und unterrichtet die zuständige Aufsichtsbehörde und/oder den jeweiligen Vertragspartner der externen IT-Dienstleister.

Hierzu verpflichtet sich der AN von der IT-Kontrollkommission festgestellte Verstöße gegen die in § 5 Abs. 5 ITJG genannten Bestimmungen nach Aufforderung durch die IT-Kontrollkommission binnen der von der IT-Kontrollkommission gesetzten Frist abzustellen (§ 5 Abs. 8 ITJG). Ansprüche des Auftraggebers bleiben davon unberührt.

3 Verpflichtungen zur Umsetzung einzelner Vorgaben bei sonstigen IT-Dienstleistungen

Sonstige IT-Dienstleistungen sind Dienstleistungen in der Infrastruktur des Auftraggebers, bei denen ein Datenzugriff erfolgt oder technisch möglich ist.

a) § 2 Abs. 1 S. 2 ITJG

Für die in den Gerichten und Staatsanwaltschaften erforderliche IT-Unterstützung begründet das für Justiz zuständige Ministerium jeweils eigene Benutzungsverhältnisse gegenüber dem AN. Aufgrund des Charakters des Dienstleistungsverhältnisses überträgt der AN die Ausführung nicht an andere Dienstleister. Eine Berechtigung zur Begründung von Unterauftragsverhältnissen ist ausgeschlossen.

Der AN ist jedoch berechtigt, andere Dienstleister mit Wartungsarbeiten an der Hard- und Software (z.B. Bearbeitung von Tickets im third level Support) zu beauftragen, wenn er die vertraglich geschuldeten Leistungen anderenfalls nicht bzw. nicht in der erforderlichen Qualität (z.B. Performance, Datensicherheit und -schutz) erbringen oder wenn die Einhaltung der jeweiligen Service-Level-Agreements ausnahmsweise nicht mit eigenem Personal erfolgen kann.

Bei Wartungsarbeiten anderer Dienstleister verbleiben die Daten aus den jeweils betroffenen Systemen (Hard- und Software) in jedem Fall beim AN und sind nicht an andere Dienstleister zu übermitteln, von diesen zu speichern, zu verarbeiten oder zu löschen.

Bei der Einschaltung Dritter im Rahmen von IT-Dienstleistungen ist die Einhaltung des ITJG durch den AN vertraglich sicherzustellen (§ 2 Abs. 1 S. 2 ITJG).

Der AN teilt dem AG bei Vertragsabschluss mit, welche IT-Dienstleister eingesetzt werden können. Einen Austausch oder eine Ergänzung innerhalb der Vertragslaufzeit, u.a. bedingt durch die Erforderlichkeit von Neuaußschreibungen aufgrund vergaberechtlicher Vorschriften, teilt der AN dem AG 1 Monat vor Eintritt der Veränderung mit. Ist der AG mit der Veränderung einverstanden, teilt der AG dies dem AN mit. Sollte der AG nicht innerhalb dieser Frist der Änderung widersprechen, gilt die Änderung als genehmigt. Widerspricht der AG einem neuen IT-Dienstleister, ist der AG berechtigt den Vertrag innerhalb eines Monats ab Zugang der Benachrichtigung ohne Sanktion durch schriftliche Erklärung zum Ende des darauffolgenden Monats zu kündigen. Unterbleibt die Kündigung, gilt die Zustimmung als erteilt.

Der AN sorgt dafür, dass sich alle Personen, die von ihm mit der Bearbeitung oder Erfüllung des Vertrages betraut sind, auf die Einhaltung des ITJG und der daraus resultierenden Maßnahmen und Vorkehrungen verpflichten. Auf Verlangen weist der AN diese Verpflichtungen durch Vorlage geeigneter Unterlagen nach. Der AN stellt außerdem sicher, dass bei den mit IT-Dienstleistungen befassten Personen und insbesondere den von ihm zu bestimmenden zugangsberechtigten Administratorinnen und Administratoren „eine obligatorische Sicherheitsüberprüfung“ nach § 15 Abs. 4 Dataport-Staatsvertrag i.V.m. § 34 Hamburgisches Sicherheitsüberprüfungsgesetzes vorausgeht „und dass diese administrativen Tätigkeiten sowie eine Veränderung von Berechtigungen vollumfänglich und revisionssicher protokolliert und die Protokolle der Justizverwaltung als Report zur Verfügung gestellt werden, um etwaige Verstöße gegen das Gesetz umgehend registrieren zu können“ (vgl. Schleswig-Holsteinischer Landtag, Drucksache 18/3224, S. 23). Hierzu werden die Protokolle durch den AN kontrolliert und die Ergebnisse nach Maßgabe des ITJG und der hier geregelten Bestimmungen mitgeteilt. Die regelmäßige Bearbeitungszeit der Sicherheitsüberprüfung liegt bei ca. 8-10 Wochen.

Weitergehende Regelungen (z.B. betreffend Verschlusssachen etc.) bleiben unberührt.

Wenn zur Erbringung einer Dienstleistung durch den AN Informationsverarbeitungstechnik eingesetzt wird, so stellt der AN sicher, dass diese Technik grundsatzkonform betrieben wird.

b) § 2 Abs. 2 ITJG

Die IT-Strukturen der Gerichte und Staatsanwaltschaften sind von denen der Landesverwaltung technisch zu trennen. Hierzu werden dedizierte Systeme und Datenbankinstanzen eingesetzt, die eine physische oder logische Trennung von anderen IT-Verfahren gewährleisten.

Bei Bereitstellung und Betreuung der in den Gerichten und Staatsanwaltschaften zum Einsatz kommenden IT ist unter Beachtung des Stands der Technik, insbesondere der in § 2 Abs. 2 ITJG geregelten Maßgaben, sicherzustellen, dass jeglicher Einblick in die richterliche, rechtspflegerische oder staatsanwaltschaftliche Tätigkeit unterbleibt.

c) § 2 Abs. 2 S. 2 Nr. 1 ITJG

Es sind berechtigte Inhaberinnen und Inhaber administrativer Zugänge zu bestimmen und die Bedingungen einer darüber hinaus erforderlichen Öffnung für weitere administrativ berechtigte Personen sind festzulegen. Für den Fall einer unbefugten Öffnung ist eine Information der IT-Kontrollkommission (§ 5 ITJG) und der betroffenen Gerichte und Staatsanwaltschaften sowie ein Verfahren zur Änderung der Zugangsgewährung vorzusehen.

Hierzu werden vom AN die mit der Umsetzung der IT-Dienstleistung beauftragten Administratorinnen und Administratoren namentlich benannt. Die für die Durchführung der IT-Dienstleistung vergebenen administrativen Berechtigungen folgen dem Minimalprinzip. Die Berechtigungen werden nach Abschluss der Arbeiten unverzüglich entzogen. Alle Beschäftigten des AN sowie externes für den AN tätiges Personal werden vor Aufnahme der Tätigkeit neben dem allgemeinen Amtsgeheimnis auch auf das datenschutzrechtliche Datengeheimnis sowie bereichsspezifische Geheimhaltungsverpflichtungen (z.B. Steuer-, Sozial-, Fernmeldegeheimnis etc.) einschließlich der Anforderungen nach dem ITJG verpflichtet.

d) § 2 Abs. 2 S. 2 Nr. 2 ITJG

Der AN stellt sicher, dass die im Rahmen richterlicher, rechtspflegerischer oder staatsanwaltlicher Tätigkeit erstellten Dokumente von den Administratorinnen und Administratoren weder eingesehen noch an Dritte weitergegeben werden, insbesondere nicht an die in § 1 Absatz 1 ITJG genannten Stellen oder an die diesen nachgeordneten Stellen der Dienstaufsicht.

Berechtigten Administratorinnen und Administratoren kann aus betrieblichen Gründen je nach Rolle der Zugriff auf die Daten und damit die Möglichkeit der unautorisierten Weitergabe nicht entzogen werden. Sie werden per Belehrung und Verpflichtung auf das einschlägige Verbot aus dem ITJG hingewiesen.

Im Sinne des Vier-Augen-Prinzips ist der AG jederzeit berechtigt, die Datenverarbeitung mit eigenem Personal zu begleiten. Die hierfür maßgeblichen Sicherheitsbestimmungen bleiben unberührt.

Eine Datenherausgabe und Datenweitergabe seitens Dataport finden ausschließlich auf Grundlage eines Auftrags des AG oder einer richterlichen Anordnung statt. Jede Datenherausgabe wird über das Sicherheitsvorfallmanagement bearbeitet, dokumentiert und an den AG gemeldet. Sofern die Datenherausgabe im Rahmen des Sicherheitsvorfallmanagements als Sicherheitsvorfall identifiziert wird, werden die GemIT und die IT-Kontrollkommission unverzüglich unterrichtet.

Der Zugriff auf die Daten wird nur solange wie für die Durchführung der IT-Dienstleistung notwendig eingeräumt. Soweit Daten auf Geräten des AN gespeichert werden, sind sie nach der Verarbeitung zu löschen. Die Löschung ist dem AG zu bestätigen.

e) § 2 Abs. 2 S. 2 Nr. 3 ITJG

Der AN stellt sicher, dass in gleicher Weise eine Weitergabe von Informationen über Merkmale oder Eigenschaften von den in Nummer 2 genannten Dokumenten (Metadaten) und von systemintern automatisch erstellten Protokollen über die Benutzung der zur Verfügung stehenden IT (Logdateien) ausgeschlossen ist.

Dies wird durch die oben nach Ziff. 3 d) dargestellten Maßnahmen sichergestellt.

f) § 2 Abs. 2 S. 2 Nr. 4 ITJG

Der AN stellt sicher, dass Ausnahmen von den Nummern 2 und 3 zugunsten des für Justiz zuständigen Ministeriums oder der ihm nachgeordneten Stellen der Dienstaufsicht nur gemacht werden, soweit sie zu Zwecken oder auf Veranlassung der jeweiligen Dienstaufsicht im Rahmen bestehender Gesetze zulässig sind; soweit Dokumente laufender Verfahren betroffen sind, sind die Ausnahmen nur zulässig, soweit dies zur Ausübung der Dienstaufsicht unerlässlich ist.

Eine Datenherausgabe und Datenweitergabe seitens des AN finden ausschließlich auf Grundlage eines Auftrags des AG oder einer richterlichen Anordnung statt. Jede Datenherausgabe wird über das Sicherheitsvorfallmanagement bearbeitet, dokumentiert und an den AG gemeldet. Sofern die Datenherausgabe im Rahmen des Sicherheitsvorfallmanagements als Sicherheitsvorfall identifiziert wird, werden die GemIT und die IT-Kontrollkommission unverzüglich unterrichtet.

Um der IT-Kontrollkommission gezielte Prüfungen zu ermöglichen, ob die Vorgaben des § 2 Abs. 2 Nr. 4 ITJG beachtet wurden, unterrichtet der AN die IT-Kontrollkommission, wenn ein Auftrag zur Datenherausgabe und Weitergabe nach § 2 Abs. 2 Satz 2 Nr. 4 ITJG durch den AG erteilt wurde. Diese Unterrichtung beschränkt sich – unbeschadet der Überwachungs-, Zutritts und Einsichtsrechte der IT-Kontrollkommission nach § 5 Abs. 5 und 6 ITJG – zunächst auf die Tatsache, dass ein entsprechender Auftrag erteilt wurde. Diese Unterrichtungspflicht des AN entfällt, wenn der AG dem AN schon im Rahmen der Auftragserteilung erklärt, dass der AG die IT-Kontrollkommission bereits über den Auftrag unterrichtet hat.

g) § 2 Abs. 2 S. 2 Nr. 5 ITJG

Der AN stellt sicher, dass im Übrigen die in Nummer 2 genannten Dokumente sowie die in Nummer 3 aufgeführten Metadaten und Logdateien von den Administratorinnen und Administratoren nur mit Zustimmung der betroffenen Verfasserin oder Nutzerin oder des betroffenen Verfassers oder Nutzers

verwendet werden, es sei denn, die Verwendung ist für die Gewährleistung der Ordnungsmäßigkeit eines automatisierten Verfahrens oder sonst für den Betrieb der IT-Infrastruktur unerlässlich.

Administratorinnen und Administratoren erhalten hierzu ausschließlich Zugriff auf Daten, die sie im Auftrag des AG zur Ausführung der für den IT-Betrieb unerlässlichen IT-Dienstleistung benötigen.

h) § 2 Abs. 2 S. 2 Nr. 6 ITJG

Der AN stellt sicher, dass jeder Zugriff protokolliert und dem für Justiz zuständigen Ministerium unverzüglich auf direktem Wege mitgeteilt wird; sofern auf individuell zuordnungsfähige Dokumente zugegriffen wurde, benachrichtigt AG die betroffene Verfasserin oder Nutzerin oder den betroffenen Verfasser oder Nutzer unverzüglich auf direktem Wege und auf dem Dienstweg.

Hierzu protokolliert der AN manuell die Zugriffe auf Datenbestände des AG. Die Protokolle sind dem AG unverzüglich zur Verfügung zu stellen. Die Bereitstellung der Protokolldaten kann auch in Form eines Berichtes erfolgen. Die Mitteilung von beabsichtigten Datenzugriffen an den AG erfolgt vorab im Rahmen der Auftragsklärung sowie ggf. während der Leistungserbringung.

Bei der Protokollauswertung aufgefallene Verstöße gegen das ITJG werden vom AN als Sicherheitsvorfall behandelt und mit der Priorität „kritisch“ versehen. Die GemIT und die IT-Kontrollkommission werden unverzüglich unterrichtet.

i) § 4 Abs. 3 ITJG i.V.m. § 5 Abs. 5 und 6 ITJG

Zum Schutz vor unbefugten Zugriffen dürfen u. a. die GemIT und die IT-Kontrollkommission bei externen Dienstleistern Kontrollen durchführen bzw. sich an den Kontrollen anderer Stellen (vgl. § 4 Abs. 4 ITJG) beteiligen.

Gegenstand der Kontrollen ist die Einhaltung dieses Gesetzes, der bestehenden Verträge und aller sonstigen Bestimmungen, die der Bereitstellung von IT-Infrastrukturen, der Betreuung der eingesetzten IT und der Gewährleistung der IT-Sicherheit in den Gerichten und Staatsanwaltschaften dienen.

Soweit zur Aufgabenerfüllung erforderlich, sind der GemIT/IT-Kontrollkommission zu den vorgenannten Zwecken Zutritt zu gewähren und ein uneingeschränktes Auskunfts- und Einsichtsrecht zu gewährleisten.

Nach § 5 Abs. 6 S. 2 ITJG besteht dieses Recht auch bezüglich derjenigen Akten und Dokumente, die sich auf die Rechtsaufsicht über Dataport oder auf die Begründung und Ausgestaltung der Benutzungsverhältnisse zum AN oder auf die Verträge mit anderen externen IT-Dienstleistern beziehen und die einen wesentlichen Bezug zur Organisation und zum Einsatz von IT in den Gerichten und Staatsanwaltschaften haben. Personenbezogene Daten dürfen im Rahmen von Kontrollen auch ohne Kenntnis der Betroffenen erhoben werden. Dokumente, Dateien und Daten im Sinne des § 2 Absatz 2 Satz 2 Nummer 2 und 3 ITJG dürfen im Rahmen von Kontrollen hingegen durch GemIT nur eingesehen oder sonst verwendet werden, soweit dies zur Aufgabenerfüllung unerlässlich ist.

Hierzu verpflichtet sich der AN der GemIT, der IT-Kontrollkommission bzw. den in § 4 Abs. 4 ITJG genannten Stellen in dem nach § 4 Abs. 3, 4 und 5 ITJG bzw. § 5 Abs. 5 und 6 ITJG geregelten Umfang Zutritt und uneingeschränkt Auskunft und Einsicht zu gewähren, soweit dies zur Aufgabenerfüllung erforderlich ist (§§ 4, 5 ITJG). Der Staatsvertrag über die Errichtung von Dataport als rechtsfähige Anstalt des öffentlichen Rechts vom 27. August 2003 (GVOBl. Schl.-H. S. 557), zuletzt geändert durch Staatsvertrag vom 27. September 2013 (GVOBl. Schl.-H. S. 511) bleibt gem. § 1 Abs. 2 ITJG unberührt.

j) § 4 Abs. 5 ITJG i.V.m. § 5 Abs. 5 S. 2 ITJG

Der AN unterrichtet die GemIT unverzüglich über Sicherheitsvorfälle, die auch oder ausschließlich die Justiz betreffen. Die Unterrichtungspflicht gilt gegenüber der IT-Kontrollkommission entsprechend (§ 5 Abs. 5 S. 2 ITJG).

Hierzu werden entsprechende Sicherheitsvorfälle vom Sicherheitsvorfallmanagement des AN unabhängig von ihrer Auswirkung auf den ordnungsgemäßen IT-Betrieb zunächst als „kritisch“ eingestuft.

k) § 5 Abs. 8 ITJG i.V.m. § 5 Abs. 5 ITJG (Auszug § 5 Abs. 8 ITJG)

Stellt die IT-Kontrollkommission Verstöße gegen die in Absatz 5 genannten Bestimmungen bei den in § 1 Abs. 1 ITJG genannten Stellen fest, fordert sie diese unter Setzung einer angemessenen Frist zur Mängelbeseitigung auf. Werden die Verstöße in dieser Frist nicht abgestellt oder handelt es sich um erhebliche Verstöße, spricht die IT-Kontrollkommission eine Beanstandung aus und unterrichtet die zuständige Aufsichtsbehörde und/oder den jeweiligen Vertragspartner der externen IT-Dienstleister.

Hierzu verpflichtet sich der AN von der IT-Kontrollkommission festgestellte Verstöße gegen die in § 5 Abs. 5 ITJG genannten Bestimmungen nach Aufforderung durch die IT-Kontrollkommission binnen der von der IT-Kontrollkommission gesetzten Frist abzustellen (§ 5 Abs. 8 ITJG). Ansprüche des Auftraggebers bleiben davon unberührt.

Service Level Agreement

Verfahrensinfrastruktur im Dataport Rechenzentrum

Teil A – Allgemeiner Teil -

Inhaltsverzeichnis

| | |
|--|-----------|
| Inhaltsverzeichnis | 2 |
| 1 Einleitung | 3 |
| 1.1 Aufbau des Dokumentes | 3 |
| 1.2 Allgemeine Mitwirkungsrechte und -pflichten | 3 |
| 2 Grundlagen der Leistungserbringung..... | 4 |
| 2.1 Betrachtung der Servicekette | 4 |
| 2.1.1 Netzwerk-Anbindung | 4 |
| 2.2 Serviceübergreifende Regelungen..... | 5 |
| 2.2.1 Wartungsfenster | 5 |
| 2.2.2 Supportzeit Standard..... | 5 |
| 2.2.3 Störungsannahme | 6 |
| 2.2.4 Personendaten der Nutzer für die Störungsannahme..... | 6 |
| 2.2.5 Changemanagement und Patchmanagement..... | 6 |
| 2.2.6 Zeitfenster für Sicherheitsupdates..... | 7 |
| 2.2.7 Release Management | 7 |
| 2.3 Serviceübergreifende Leistungskennzahlen (KPIs) | 8 |
| 2.3.1 Reaktionszeit | 8 |
| 2.4 Betriebsverantwortung..... | 8 |
| 3 Rollendefinition..... | 9 |
| 4 Leistungsspezifische KPIs und Reporting | 10 |
| 4.1 Verfügbarkeit (Availability)..... | 10 |
| 4.2 Auslastung | 10 |
| 5 Störungsprioritäten | 11 |
| 6 Glossar | 13 |
| 6.1 Definition der Verfügbarkeit | 17 |
| 6.1.1 Messung der Verfügbarkeit | 18 |
| 6.1.2 Ausfallzeiten, die die Verfügbarkeit nicht beeinträchtigen..... | 18 |

1 Einleitung

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

1.1 Aufbau des Dokumentes

Diese Anlage enthält nach der Einleitung die folgenden Kapitel:

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

1.2 Allgemeine Mitwirkungsrechte und -pflichten

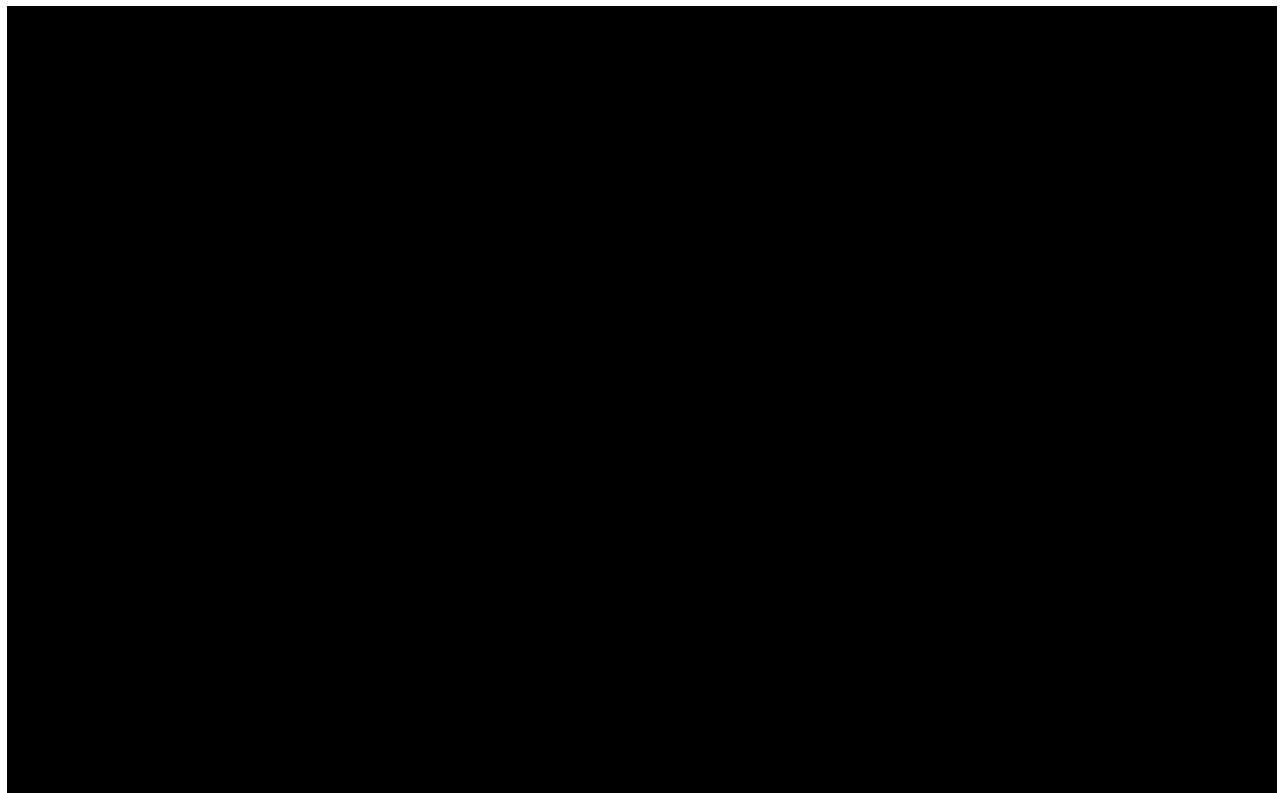
Die von Dataport zugesagten Leistungen erfordern Mitwirkungspflichten und Beistellleistungen des Auftraggebers.

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.

A large rectangular area of the page has been completely blacked out, indicating that the original content has been redacted or removed.

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:

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

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

2.2.2 Supportzeit Standard

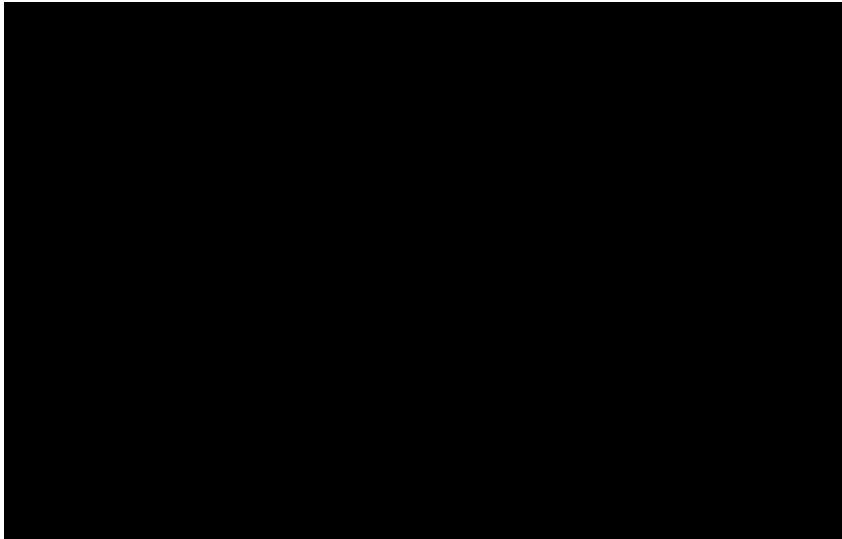
Für alle Services gilt einheitlich die Supportzeit Standard. Während der Supportzeit werden Störungen behoben und Aufträge angenommen.

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

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

2.2.3 Störungsannahme

Das Callcenter ist grundsätzlich Ansprechpartner für Störungen in der Supportzeit Standard.



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

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

2.2.4 Personendaten der Nutzer für die Störungsannahme

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

2.2.5 Changemanagement und Patchmanagement

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

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

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

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

Patchmanagement ist notwendig, damit ein sicherer Betrieb im Sinne des BSI Grundschutzes gewährleistet werden kann. Es ist Aufgabe des Auftraggebers, den Verfahrenshersteller auf die Verwendung von im Support befindlicher Software hinzuweisen und rechtzeitig einen Wechsel einzuplanen, wenn genutzte Anwendungen ihr End of Support (EOS) erreichen, sofern diese Aufgabe durch den Auftragsverarbeiter nicht im Rahmen einer Beauftragung zum fachlichen Verfahrensmanagement erbracht wird.

2.2.6 Zeitfenster für Sicherheitsupdates

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

2.2.7 Release Management

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

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

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

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

2.3 Serviceübergreifende Leistungskennzahlen (KPIs)

2.3.1 Reaktionszeit

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

| Störungspriorität ¹ | Reaktionszeiten |
|--------------------------------|-----------------|
| Kritisch (1) | |
| Hoch (2) | |
| Mittel (3) | |
| Niedrig (4) | |

Die vereinbarte Zielwahrscheinlichkeit P_{Soll} für die Erreichung der Reaktionszeiten pro Kalendermonat beträgt ■■■■■

Reporting

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

2.4 Betriebsverantwortung

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

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

¹ Für eine detaillierte Definition siehe Abschnitt 4 in diesem Dokument

3 Rollendefinition

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

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

4 Leistungsspezifische KPIs und Reporting

4.1 Verfügbarkeit (Availability)

Definition siehe Teil A; Ziffer 6.1

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

4.2 Auslastung

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

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

5 Störungsprioritäten

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

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

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

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

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

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

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

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

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

6 Glossar

| Begriff | Definition |
|---------------------------------------|--|
| Application Layer Gateway (ALG) | Sicherheitskomponente in einem Computernetzwerk |
| Bearbeitungszeit | Die Bearbeitungszeit ist die Zeitspanne zwischen der Beauftragung eines Services bzw. einer Aktivität durch den Auftraggeber über einen vorgegebenen Weg (z. B. Auftrag zum Einrichten eines Telefonanschlusses) bis zur erfolgreichen Durchführung des beauftragten Services bzw. der Aktivität. |
| Betriebszeit | Die Betriebszeit ist der Zeitraum, in dem die vereinbarten Ressourcen (Services) vom Auftragsverarbeiter (AV) zur Verfügung gestellt werden und grundsätzlich genutzt werden können. Dies ist generell an 365 Tagen pro Jahr, 24 h pro Tag, der Fall. Die Betriebszeit wird eingeschränkt durch Zeiten, zu denen auf Grund von höherer Gewalt keine Dienstleistung möglich ist und durch Wartungsarbeiten. |
| Bezugsgröße | Messgröße, bezogen auf die eine Leistungskennziffer definiert ist. Beispiel: Die Leistungskennziffer „Reaktionszeit“ ist bezogen auf die Bezugsgröße „Supportzeit“ definiert. |
| Bezugszeitraum (Messzeitraum) | Der Zeitraum, auf den sich eine Leistungskennziffer bezieht und in dem die tatsächlich erbrachte Qualität der Leistung gemessen wird. Sofern nicht anders angegeben (z. B. im Fall der Verfügbarkeit) beziehen sich alle angegebenen Metriken jeweils auf einen Messzeitraum von einem Kalendermonat. |
| Business Service (BS) | Bündelung von IT-Services |
| Callcenter | Das Callcenter ist grundsätzlich Ansprechpartner für Störungen. |
| Fachliches Verfahrensmanagement (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 |
| Leistungsübergabepunkt (LÜP) | Bezugspunkt der Definition von Service Leveln. Die Services werden dem Auftraggeber am LÜP zur Verfügung gestellt. Einflüsse auf die Servicequalität ab LÜP sind nicht Bestandteil der vom Auftragsverarbeiter zugesagten Leistungen. Analog sind die Details der Serviceerbringung durch den Auftragsverarbeiter bis zum LÜP alleine unter der Verantwortung des AV. |
| Maintenance Window (MW) | Das Maintenance Window hat den primären Fokus Sicherheitsupdates oder Patches der standardisierten SW-Komponenten (Betriebssystem, Middleware) auf den Servern durchzuführen. |
| Operational Level Agreement (OLA) | Dataport-interne Beschreibung von Leistungen nach ihrer Qualität und Ausprägung. Zweck ist die interne Absicherung der nach außen bzw. gegenüber dem Auftraggeber zugesagten Service Levels. |
| Reaktionszeit | Die Reaktionszeit ist die Zeitspanne zwischen der Meldung einer Störung über den vereinbarten Störmeldeweg und dem Beginn der inhaltlich qualifizierten Bearbeitung durch Dataport. Zur Messung der Reaktionszeit wird der Zeitpunkt der Störungsmeldung und der Status „in Bearbeitung“ in der ITSM Suite bei Dataport verwendet. Die Reaktionszeit ist grundsätzlich abhängig von der Priorität der Störung. Je nach SLA-Klasse im Servicekatalog sind die Prioritäten „kritisch“ oder „hoch“ evtl. nicht verfügbar. |
| Twin Data Center | Dataport Rechenzentren in Alsterdorf und Norderstedt |
| Security Service Level Agreement (SSLA) | Ergänzung eines SLA zur Verfahrensinfrastruktur. Mit dem Security Service Level Agreement wird zwischen den Vertragspartnern vereinbart, wie der Betrieb unter Informationssicherheitsgesichtspunkten auf Basis des IT-Grundschutzes des Bundesamtes für Informationssicherheit (BSI) unter Nutzung des Sicherheitsmanagementsystems des Auftragsverarbeiters erfolgt. |
| Service | Standardisierte Bündelung von Leistungen; aufgeführt im Servicekatalog und relevant für die Preisgestaltung |
| Service Desk | Das Service Desk ist die Anlaufstelle für die Nutzer, d.h. alle Störungen werden hier zunächst angenommen und bearbeitet. Regelfhaft wird diese Aufgabe vom Callcenter übernommen |

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

| Begriff | Definition |
|--|--|
| Supportzeit | <p>Die Supportzeit Standard beschreibt den Zeitraum, in dem Störungen und Anfragen entgegengenommen werden und auf sie reagiert wird.</p> <p>In der erweiterten Supportzeit werden nur Störungen entgegengenommen und bearbeitet.</p> <p>Die Supportzeit liegt innerhalb der Betriebszeit und kann sich auch über das Wartungsfenster erstrecken.</p> |
| Technisches Verfahrensmanagement (TVM) | <p>Das technische Verfahrensmanagement umfasst administrative Tätigkeiten in systemnaher Software (Middleware 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.</p> |
| User Help Desk (UHD) | <p>Der User Help Desk ist eine besondere Ausprägung des Service Desk bei Dataport bei entsprechender gesonderter vertraglicher Grundlage.</p> <p>Der UHD hat die schnellstmögliche Wiederherstellung der Arbeitsfähigkeit der Nutzerin/des Nutzers im Falle von IT-Störungen zum Ziel. Dazu übernimmt der User Help Desk in einem definierten Rahmen für definierte Produkte Handling Hilfe im Rahmen der Erstlösung für die Nutzerin/den Nutzer. Der User Help Desk übernimmt auch die Annahme und die Bearbeitung von Incidents.</p> |
| Verfahren | <p>Die IT-Unterstützung für die Durchführung von Fachaufgaben des Auftraggebers</p> |
| Verfahrensumgebungen | <p>Verfahrensumgebungen können in folgenden Produktionsstufen bereitgestellt werden:</p> <ul style="list-style-type: none"> • 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 Patches der Betriebssysteme oder Middleware 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 |

| Begriff | Definition |
|---------------------------------------|--|
| Verfahrensupdates | Grundsätzlich nicht Gegenstand des Wartungsfensters oder des Maintenance Windows. Sind separat zu vereinbaren. |
| Vertrag | Ein Vertrag kontrahiert eine gegen Entgelt angebotene Bündelung eines oder mehrerer Business Services. |
| Wide Area Network (WAN) | Rechnernetz, welches sich über einen sehr großen geografischen Bereich erstreckt. |
| Wartungsfenster | <p>Zeitfenster für Wartungsarbeiten an den Systemen mit dem primären Fokus: Updates / Erneuerungen / Wartungsarbeiten an den RZ-Diensten und der Netzinfrastruktur durchzuführen. Es wird zwischen dem Standard-Wartungsfenster (regelmäßig pro Woche) und besonderen Wartungsfenstern (auf gesonderte Vereinbarung) unterschieden.</p> <p>Das Wartungsfenster liegt in der Betriebszeit.</p> <p>Während des Wartungsfensters muss nicht generell von einer Nichtverfügbarkeit der Services ausgegangen werden. Jedoch sind im Wartungsfenster Serviceunterbrechungen möglich.</p> <p>Sollte in Sonderfällen ein längeres Wartungsfenster beansprucht werden, so erfolgt dies in direkter Absprache mit dem Auftraggeber. Der Auftraggeber wird nur in begründeten Fällen die Durchführung von Wartungsmaßnahmen einschränken. Der Auftragsverarbeiter wird in diesen Fällen unverzüglich über sich ggf. daraus ergebenden Mehraufwand und Folgen informieren.</p> |
| Zielwahrscheinlichkeit (P_{Soll}) | <p>Zusätzlich zum Sollwert kann eine Wahrscheinlichkeit angegeben werden, mit der der Sollwert während des Bezugszeitraumes (Messzeitraumes) erreicht werden soll. Ist keine Zielwahrscheinlichkeit angegeben, so gilt eine Zielwahrscheinlichkeit von 100%, d.h. alle gemessenen Leistungen müssen gleich oder besser als der Sollwert sein.</p> <p>Eine Zielwahrscheinlichkeit kann nur für Kennziffern angegeben werden, die in vielen Einzelmessungen oder Einzelereignissen bestimmt werden (z. B. Reaktionen auf einzelne Störungen).</p> <p>Beispiel: Leistungskennziffer sei die Reaktionszeit, der Sollwert sei 30 Minuten, die Zielwahrscheinlichkeit sei 90%, der Bezugszeitraum sei ein Kalendermonat. Dies bedeutet, dass in einem Kalendermonat mindestens 90% aller tatsächlichen Reaktionszeiten \leq 30 Minuten betragen müssen.</p> |

6.1 Definition der Verfügbarkeit

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

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

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

Für die Bezugszeit gilt:

Bezogen auf die Betriebszeit werden die Verfahrensinfrastrukturen grundsätzlich mit der Verfügbarkeitsklasse [REDACTED] zur Verfügung gestellt.

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

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

Grundsätzlich stehen folgenden Verfügbarkeitsklassen für Verfahrensinfrastrukturen zur Verfügung:

6.1.1 Messung der Verfügbarkeit

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

6.1.2 Ausfallzeiten, die die Verfügbarkeit nicht beeinträchtigen

Bei der Berechnung der Verfügbarkeit werden nicht berücksichtigt:

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

Service Level Agreement

Verfahrensinfrastruktur im Dataport Rechenzentrum

**Teil B (spezifischer Teil für Verfahren PDF Compressor
(PDFCOMP_ML001))**

Inhaltsverzeichnis

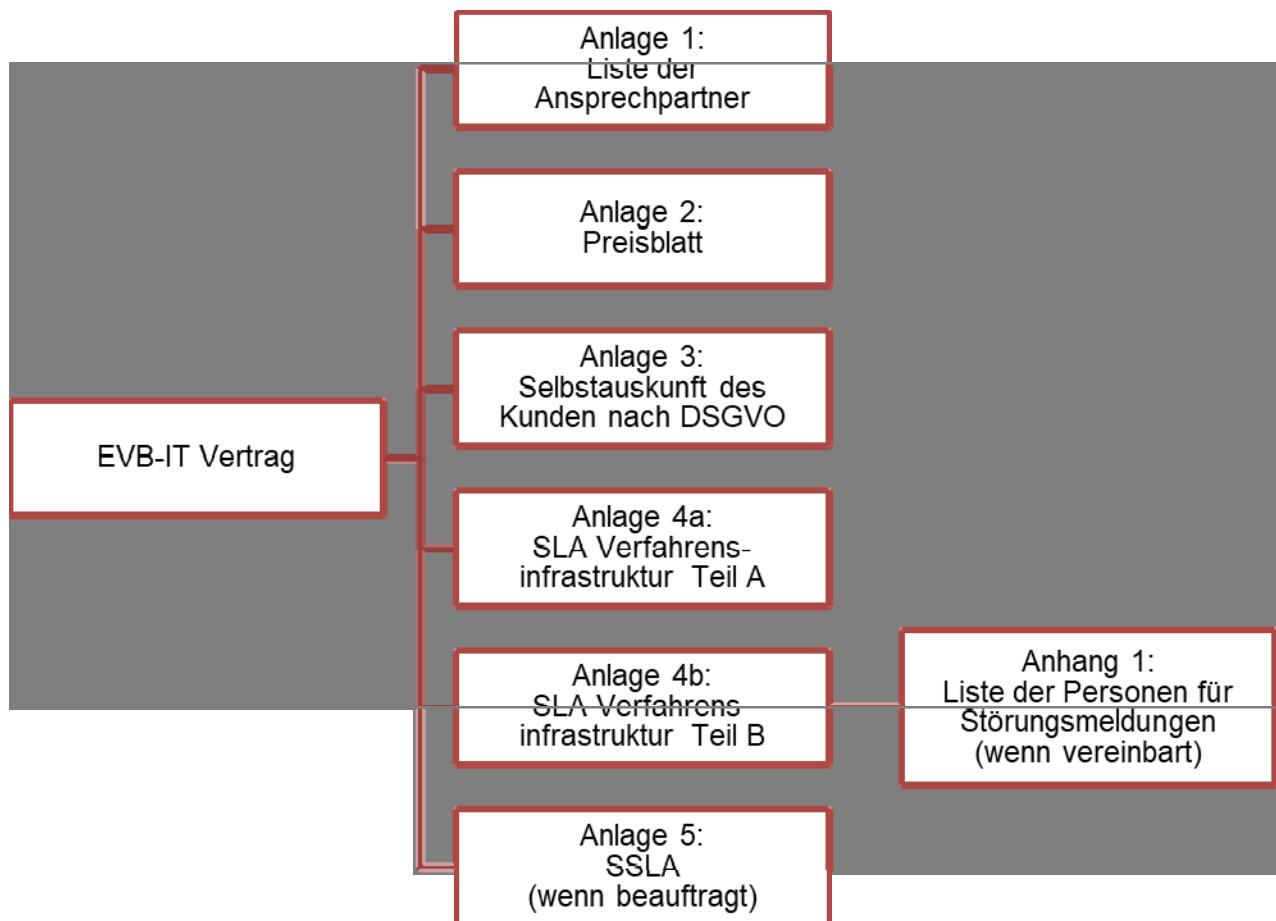
| | |
|---|----------|
| Inhaltsverzeichnis | 2 |
| 1 Einleitung | 4 |
| 1.1 Einbindung des SLAs in die Vertragsstruktur | 4 |
| 1.2 Aufbau des Dokumentes | 4 |
| 1.3 Rollenzuordnung | 5 |
| 1.4 Mitwirkungsrechte und –pflichten | 5 |
| 2 Rahmen der Leistungserbringung | 6 |
| 2.1 Servicerelevante Regelungen | 6 |
| 2.1.1 Supportzeiten | 6 |
| 2.1.2 Service Request Management | 6 |
| 3 Leistungsbeschreibung Verfahrensinfrastruktur | 7 |
| 3.1 Beschreibung des Fachverfahrens | 7 |
| 3.2 Bereitgestellte Umgebungen | 7 |
| 3.2.1 Leistungsbeschränkung bei Verzicht von zusätzlichen Umgebungen | 7 |
| 3.3 Details zu Server-Services | 7 |
| 3.3.1 Bereitgestellte Server-Services | 8 |
| 3.3.2 Zentraler Fileservice | 9 |
| 3.3.3 Fileservice Economy | 9 |
| 3.3.4 Application Level Gateway-Funktionalität (ALG) | 9 |
| 3.3.5 Backup & Recovery | 9 |
| 3.3.6 Container | 10 |
| 3.4 Geteilte Betriebsverantwortung/ Service Fernzugriff Adminplattform (SFA) | 10 |
| 3.5 Details zum Technischen Verfahrensmanagement | 10 |
| 3.5.1 Serviceklassifikation | 10 |
| 3.5.2 Schnittstellen zu anderen Fachverfahren | 10 |
| 3.5.3 Benutzerverwaltung | 11 |
| 3.5.4 Zeitlich befristeter und überwachter Fernzugriff | 11 |
| 3.6 Leistungseinschränkungen | 11 |
| 3.6.1 Leistungsbeschränkung bei geteilter Betriebsverantwortung | 11 |
| 3.6.2 Leistungsbeschränkung bei manuellem, schreibenden Zugriff auf den Fileservice des Backendverfahrens | 11 |

| | | |
|---|--|----|
| 4 | Leistungsspezifische KPIs und Reporting | 12 |
| 5 | Maßnahmen bei Beendigung der Leistung..... | 13 |

1 Einleitung

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

1.1 Einbindung des SLAs in die Vertragsstruktur



1.2 Aufbau des Dokumentes

Diese Anlage enthält nach der Einleitung die folgenden Kapitel:

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

1.3 Rollenzuordnung

Für diesen SLA sind die Rollen wie folgt zugeordnet:

| Rolle | Rolleninhaber |
|---|--|
| Auftraggeber (AG) | Siehe EVB-IT |
| Auftragsverarbeiter (AV) | Siehe EVB-IT |
| Zusätzliche Auftragsberechtigte (AB) zur Anlage 1 EVB-IT: | keine |
| Nutzer | Nutzer der Verfahrensinfrastruktur, müssen nicht dem Auftraggeber zugehörig sein |

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

1.4 Mitwirkungsrechte und –pflichten

Der Auftraggeber stellt gemäß Anlage 1 des EVB-IT eine Liste mit Ansprechpartnern zur Verfügung, welche gleichzeitig Auftragsberechtigte für Serviceabrufe aus dem Vertrag sind und informiert umgehend darüber, wenn sich Änderungen ergeben. Diese Verpflichtung gilt ebenso für den Auftragsverarbeiter.

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

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

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

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

2 Rahmen der Leistungserbringung

2.1 Servicerelevante Regelungen

2.1.1 Supportzeiten

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 4.1 des EVB-IT)

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

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

3 Leistungsbeschreibung Verfahrensinfrastruktur

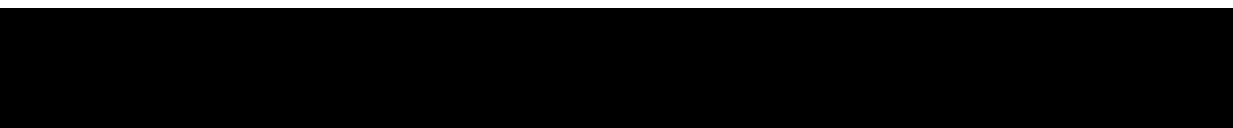
Für das nachfolgend beschriebene Fachverfahren werden eine oder mehrere Verfahrensumgebungen entsprechend den jeweiligen Produktionsstufen im Rechenzentrum von Dataport bereitgestellt. Die jeweilige Verfahrensumgebung nutzt die RZ-Basisdienste entsprechend der ausgewählten SLA-Klasse, dem Sicherheitsbereich, 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 PDF-Compressor Enterprise konvertiert archivierbare Dokumente bzw. Dateien in ein einheitliches PDF/A2 Dateiformat, inklusive effizienter OCR-Verarbeitung von Textebenen.

3.2 Bereitgestellte Umgebungen



3.2.1 Leistungsbeschränkung bei Verzicht von zusätzlichen Umgebungen

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

3.3 Details zu Server-Services

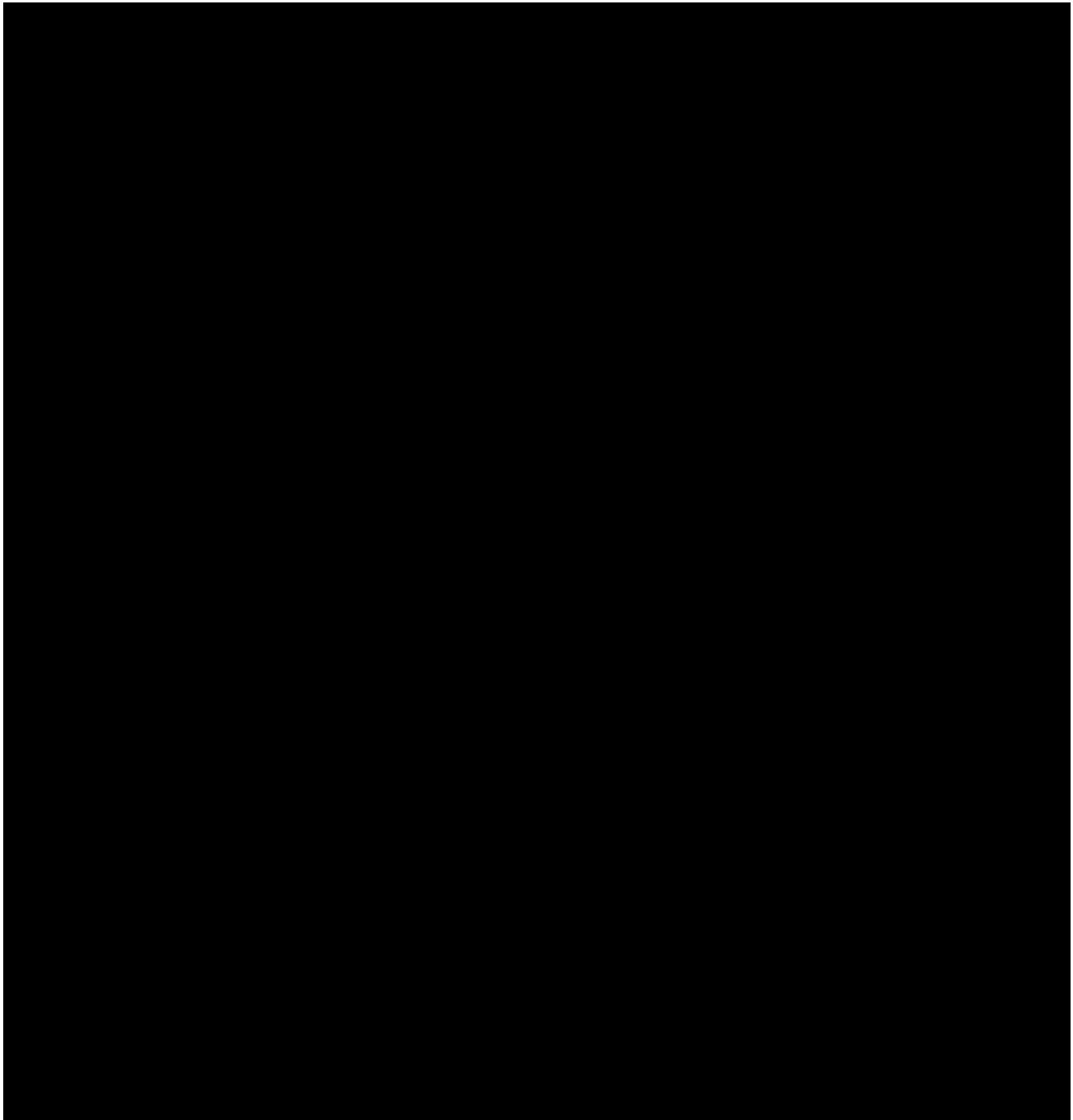
Alle nachfolgenden Server-Services werden nur mit Betriebssystemen und Middleware bereitgestellt, die sich im offiziellen Herstellersupport befindet. Bei absehbarem Auslaufen des Herstellersupports wird der Auftragsverarbeiter rechtzeitig (regelhaft mit mindestens 24 Monaten Vorlaufzeit) auf den Auftraggeber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

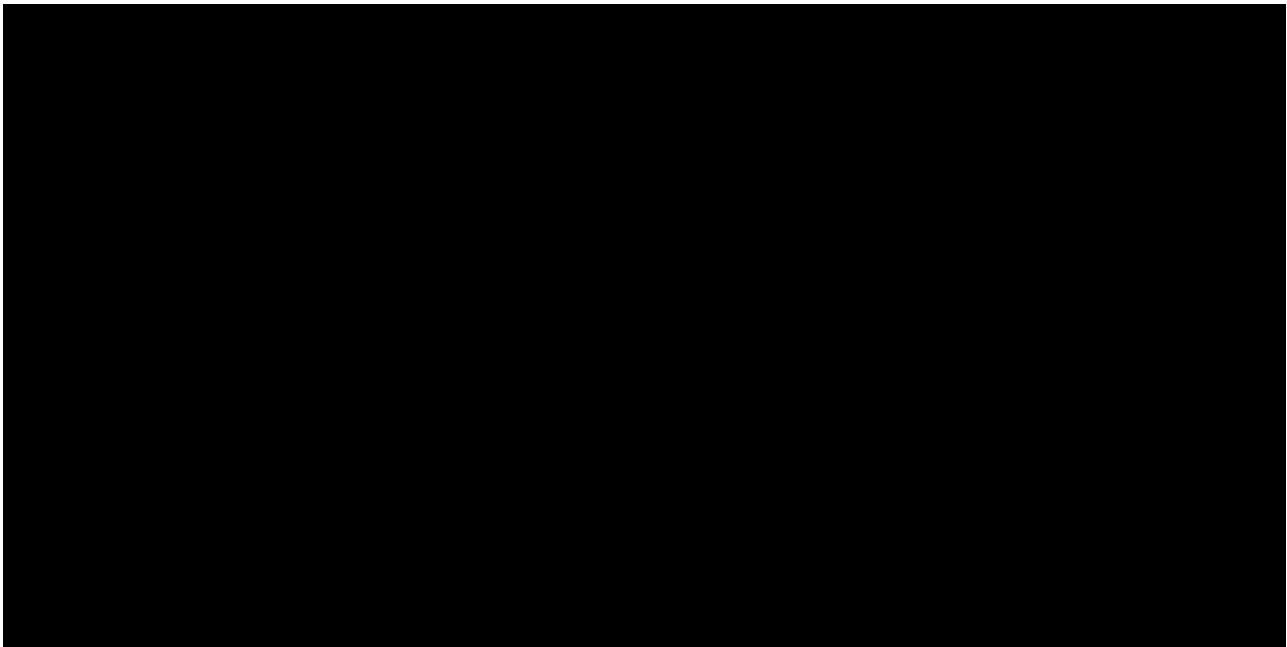
Der Auftraggeber hat keinen Anspruch auf Weiterbetrieb von Verfahrensinfrastrukturen mit Betriebssystemen oder Middleware, für die kein Herstellersupport mehr besteht.

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

3.3.1 **Bereitgestellte Server-Services**

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





Die Lizenzen für das Betriebssystem und den Web-Service sind Bestandteil des Web-Services.

3.3.2 Zentraler Fileservice

Nicht Bestandteil des SLAs.

3.3.3 Fileservice Economy

Nicht Bestandteil des SLAs.

3.3.4 Application Level Gateway-Funktionalität (ALG)

Nicht Bestandteil des SLAs.

3.3.5 Backup & Recovery

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

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

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

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

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

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

3.3.6 Container

Nicht Bestandteil des SLAs.

3.4 Geteilte Betriebsverantwortung/ Service Fernzugriff Adminplattform (SFA)

Nicht Bestandteil des SLAs.

3.5 Details zum Technischen Verfahrensmanagement

3.5.1 Serviceklassifikation

Für das technische Verfahrensmanagement wird folgende Ausprägung vereinbart:

| Spezifikation der Leistungsklasse | |
|-----------------------------------|--|
| Anzahl Benutzer (named) | |
| Anzahl Umgebungen | |
| Anzahl / Art Server | |
| Anzahl Updates | |
| Anzahl Schnittstellen | |

3.5.2 Schnittstellen zu anderen Fachverfahren

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

| Produktionsstufen | Schnittstellen |
|-------------------|----------------|
| Test | |

3.5.3 Benutzerverwaltung

Die Benutzerverwaltung für die Verfahrensinfrastruktur erfolgt:

- über die Benutzerverwaltung der Active Directory der Länder: Schleswig-Holstein: lr.landsh.de, Bremen: land.hb-netz.de

Die Benutzerverwaltung ist nicht Bestandteil dieser Leistungsvereinbarung.

3.5.4 Zeitlich befristeter und überwachter Fernzugriff

Nicht Bestandteil des SLAs.

3.6 Leistungseinschränkungen

3.6.1 Leistungsbeschränkung bei geteilter Betriebsverantwortung

Nicht Bestandteil des SLAs.

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

Nicht Bestandteil des SLAs.

4 Leistungsspezifische KPIs und Reporting

Es wurden keine weiteren leistungsspezifischen KPIs und Reports vereinbart.

5 Maßnahmen bei Beendigung der Leistung

Es wurden keine individuellen Absprachen zu Maßnahmen bei Beendigung der Leistung vereinbart.

Security Service Level Agreement

Grundschutzkonformer Verfahrensbetrieb PDF Compressor ML

Allgemeiner Teil (Teil A)

Inhaltsverzeichnis

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

1. Einleitung

1.1 Leistungsgegenstand

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

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

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

1.2 Aufbau des Dokumentes

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

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

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

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

2. Leistungsumfang und -beschreibung

2.1 Informationssicherheitsmanagementsystem (ISMS)

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

- die im IT-Sicherheits- und Datenschutzmanagementhandbuch des Auftragnehmers festgelegten und mit denen im Geschäftsverteilungsplan (GVP¹) dokumentierten Funktionsträger
- die im IT-Sicherheits- und Datenschutzmanagementhandbuch des Auftragnehmers festgelegten Prozesse des Informationssicherheitsmanagements:
 - der Betrieb des ISMS
 - die Umsetzung der Grundschutz-Vorgehensweise auf Grundlage des BSI-Standards 200-2
 - die Sicherheitskonzepterstellung
 - das Sicherheitsvorfallmanagement
 - das Notfall- und Notfallvorsorgemanagement
- sowie das sicherheitsrelevante Regelwerk des Auftragnehmers zur Informationssicherheit

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

2.2 Verfahrensbezogener IT-Sicherheitskoordinator (ITSK)

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

Der IT SK steht für die Beantwortung verfahrensbezogener Sicherheitsfragen im Verantwortungsbereich des Auftragnehmers zur Verfügung. Er ist für das verfahrens- oder dienstbezogene Sicherheitsvorfallmanagement beim Auftragnehmer verantwortlich und damit die Schnittstelle des Auftraggebers in die Sicherheitsmanagementorganisation und die Sicherheitsmanagementprozesse des Auftragnehmers.

Der IT SK ist verantwortlich für die Erstellung des auftragsbezogenen Sicherheitskonzeptes sowie die jährliche Bereitstellung des Sicherheitsnachweises² (siehe Kapitel 2.4). Er überwacht während der Vertragslaufzeit die Aufrechterhaltung des grundschutzkonformen Betriebes für die vom Auftragnehmer verantwortete, auftragsbezogene Infrastruktur.

¹ Der Geschäftsverteilungsplan als nicht kundenöffentlichtes Dokument kann entsprechend der Regelungen des Kapitels 3.3 (Einsicht in interne Dokumente des Auftragnehmers) eingesehen werden.

² Der Sicherheitsnachweis ist die Dokumentation des Umsetzungsstandes aller relevanten Sicherheitsanforderungen.

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

2.3 Grundschutzkonformer Betrieb

Der Auftragnehmer verpflichtet sich, die vom BSI in den IT-Grundschutzkatalogen³ vorgegebenen BASIS- und STANDARD-Anforderungen, die in den Zuständigkeitsbereich des Auftragnehmers fallen, für den von dieser Vereinbarung betroffenen Informationsverbund umzusetzen.

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

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

2.4 Erstellung und Pflege der Sicherheitsdokumentation

2.4.1 Umfang

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

Das Sicherheitskonzept beschreibt die nach IT-Grundschutz-Methodik zusammengefasste Struktur des betrachteten Informationsverbundes sowie die maßgeblichen⁴ Sicherheitsanforderungen im Zuständigkeitsbereich des Auftragnehmers.

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

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

2.4.2 Struktur und Standardordner

³ Die aktuelle Version der IT-Grundschutz-Kataloge kann beim BSI abgerufen werden (www.bsi.bund.de).

⁴ Die Festlegung der relevanten Sicherheitsanforderungen erfolgt auf Grundlage der Modellierungsvorschriften des BSI-Standards 200-2.

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

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

2.4.2.1 A.0 Richtlinien für Informationssicherheit

Die Rahmenbedingungen zur Umsetzung des grundsatzkonformen 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 betrachter Gefährdungslagen (Risiken) und festgelegter Sicherheitsanforderungen.

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

2.4.2.4 A.4 Grundschutzerhebung (Sicherheitsnachweis)

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

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

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

2.4.2.5 A.D0 Ergänzende Sicherheitskonzepte

Sofern für den unter dieser Vereinbarung betrachteten Informationsverbund weitere Sicherheitskonzepte maßgeblich sind, werden diese in diesem Ordner beigelegt.⁵

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 Umsetzung erforderlich sind, werden diese in die Sicherheitsdokumentation (Ordner A.D1) aufgenommen.

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

⁵ Für Verfahren, die mindestens in Teilen im Twin Data Center (TDC) betrieben werden, ist dies das der BSI-Zertifizierung unterliegende Sicherheitskonzept des Rechenzentrums.

2.4.3 Optionale Ordner und Dokumente

2.4.3.1 A.2 Schutzbedarfsfeststellung

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

2.4.3.2 A.5 Risikoanalyse

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

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

2.4.3.3 A.6 Risikobehandlung

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

2.5 Gemeinsamer Workshop

Der Auftragnehmer führt mit dem Auftraggeber einen gemeinsamen Workshop zur Sicherheitsbetrachtung der für den Informationsverbund maßgeblichen Fachanwendung durch. Gegenstand des Workshops ist die Durchführung von Sicherheitschecks für den oder die maßgeblichen 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 Bausteinenebene). Kommt keine Fachanwendung zum Einsatz (z.B. bei einem reinen Infraukturbetrieb) kann der Workshop entbehrlich sein.

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

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

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

2.6 Bereitstellung

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

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

2.7 Prüfung der Umsetzung

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

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

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

3. Abgrenzung der Leistungen

3.1 Spezifische datenschutzrechtliche Anforderungen

Der mit dem SSLA vereinbarte IT-Grundschutzkonforme Betrieb behandelt die Grundwerte der Informationssicherheit (Vertraulichkeit, Verfügbarkeit, Integrität). Der unter Kapitel 2 aufgeführte Leistungsumfang ist grundsätzlich geeignet, die Sicherheitsanforderungen sowie ihren Umsetzungsstand in geeigneter Form nachzuweisen und damit einen wesentlichen Beitrag zur Erfüllung 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 Umsetzungsverantwortung dafür liegt beim Verantwortlichen und geht im Zuge der Auftragsverarbeitung nicht auf den Auftragsverarbeiter (Auftragnehmer) über. Besondere Sicherheits- oder Dokumentationsanforderungen, die sich aus solchen spezifisch datenschutzrechtlichen Anforderungen ergeben, sind - soweit nicht an anderer Stelle im EVB-IT-Vertrag berücksichtigt - gesondert zu beauftragen.

3.2 Abgrenzung des betrachteten Informationsverbundes

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

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

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

3.3 Einsicht in interne Dokumente des Auftragnehmers

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

3.4 Abweichungen

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

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

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

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

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

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

3.5 Fortschreibung des IT-Grundschutzes

Der IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik unterliegt der ständigen Fortschreibung. Hieraus kann sich z.B. bei wesentlichen Neuerungen oder Änderungen der IT-Grundschutzstandards (z.B. neue oder geänderte Sicherheitsanforderungen) eine Veränderung des 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 200-2 vollständiges Sicherheitskonzept erforderliche Leistungen sind nicht Teil der vorliegenden Vereinbarung:

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

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

4.1 Geteilte Verantwortung auf Bausteinenebene

In den beim Auftragnehmer modellierten IT-Grundschutz-Bausteinen können sich Sicherheitsanforderungen befinden, für die die Umsetzungsverantwortung beim Auftraggeber liegt⁶. Sofern die Umsetzung dieser Anforderungen beim Auftragnehmer nicht beauftragt wurde, werden diese Sicherheitsanforderungen als "entbehrlich" dokumentiert. Erfolgt die Prüfung der Umsetzung in einem gemeinsamen Workshop (vgl. Kapitel 2.4.2), wird der Umsetzungsstand in der Verwaltungssoftware des Auftragnehmers dokumentiert.

4.2 Datenexport

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

⁶ Bausteine die einer "geteilten" Verantwortung unterliegen, finden sich insbesondere auf Schicht der Anwendungen wieder (beispielsweise Anforderungen an Freigabeprozesse für Patches der Fachanwendung, Einrichtung eines Internet-Redaktionsteams, Freigabe von Webseiteninhalten bei Webservern, Anforderungen an die Beschaffung, Anforderungen an den sicherheitsbezogenen Leistungsumfang einer Anwendungssoftware etc.)

5. Leistungsvoraussetzungen

5.1 Schutzbedarf feststellung und Risikoanalyse nach IT-Grundschutz

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

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

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

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

5.2 Mitwirkungspflichten des Auftraggebers

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

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

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

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

- 2) Risikobewertung⁷ bei der Erweiterung des betrachteten IT-Verbundes um fachliche oder technische Komponenten oder der Erweiterung um Kommunikationsschnittstellen, insbesondere zu Verfahren mit niedrigerem Sicherheitsniveau⁸
- 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 Sicherheitsanforderungen ergeben. Der Auftragnehmer teilt diese dem Auftraggeber bei Kenntnisserlangung 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, Softwarematerien 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.

⁷ ggf. schließt das auch die Aktualisierung der Risikoanalyse nach BSI-Standard 200-3 mit ein

⁸ z.B. zu Verfahren, die nicht IT-Grundsatzkonform betrieben werden

Security Service Level Agreement

**Grundschutzkonformer Verfahrensbetrieb
PDF Compressor ML**

Verfahrensspezifischer Teil (Teil B)

Inhaltsverzeichnis

| | | |
|---|---|---|
| 1 | Einleitung | 3 |
| 2 | Ergebnisse der Risikoanalyse..... | 3 |
| 3 | Spezifische Teil-Sicherheitskonzepte | 3 |

1 Einleitung

Der SSLA Teil B beauftragt ergänzende Sicherheitsmaßnahmen, welche über die im SSLA Teil A (Umsetzung von Maßnahmen des Grundschutzkataloges mit dem Schutzbedarf Normal) vereinbarten Leistungen hinausgehen und in Verantwortung von Dataport umgesetzt werden müssen. Dies ist grundsätzlich für Verfahren mit erhöhtem Schutzbedarf erforderlich, sofern risikominimierende Maßnahmen definiert wurden, die im Rahmen des Standardbetriebes nicht umgesetzt werden (können).

Voraussetzung für die Festlegung zusätzlicher Maßnahmen ist eine vom Auftraggeber durchgeführte ergänzende Sicherheits- und Risikoanalyse nach BSI-Standard 200-3, in der ergänzende Sicherheitsmaßnahmen für die Behandlung erhöhter Gefährdungen bei hohem oder sehr hohem Schutzbedarf ermittelt wurden.

Die Auflistung der über das Grundschutzniveau "Normal" hinaus durch den Auftragnehmer umzusetzenden zusätzlichen Maßnahmen finden sich im Kapitel 2 des SSLA Teil B. Im Kapitel 3 werden Leistungen in Rahmen der Erstellung möglicher spezifischer Teil-Sicherheitskonzepte, wie z.B. Datensicherungskonzept oder Notfallvorsorgekonzept festgelegt.

2 Ergebnisse der Risikoanalyse

Der Schutzbedarf des Verfahrens wurde vom Auftraggeber mit „normal“ für die aufzubauende Testumgebung definiert. Der Schutzbedarf des Verfahrens für die Produktion wird perspektivisch mit „hoch“ eingeschätzt, ist jedoch nicht formal erfolgt. Der Auftragnehmer wird mit der Umsetzung folgender Maßnahme beauftragt:

- Verfahrensplatzierung im Datacenter Justiz (DCJ)

3 Spezifische Teil-Sicherheitskonzepte

Es werden keine spezifischen Teil-Sicherheitskonzepte beauftragt.

Erläuterungen und Glossar

| | |
|-----------------------|--|
| BSI | Bundesamt für Sicherheit in der Informationstechnik |
| Sicherheitskonzept | Auch IT-Sicherheitskonzept; das formale Vorgehen nach BSI-Standard 200-2 wird eingehalten |
| Sicherheitskonzeption | Teil-Sicherheitskonzept, dem nach der IT-Grundsatzvorgehensweise im BSI-Standard 200-2 vorgegebene Teile fehlen können. Die Sicherheitskonzeption enthält bei Dataport in jedem Falle Maßnahmen, die nach den Modellierungsregeln des BSI ausgewählt werden. |
| SSLA | Security Service Level Agreements |

EVB-IT Dienstvertrag Vxxxxx/xxxxxxxx



Leistungsnachweis

zum Vertrag über die Beschaffung von Dienstleistungen

Auftraggeber:

Dataport Auftragsnummer:

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.

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



Positionsübersicht

| Position | Positionsbezeichnung | Stunden gesamt |
|----------|----------------------|----------------|
| | | |
| | Gesamt | |

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

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

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