## Vertrag über IT-Dienstleistungen

## dWebTor Betrieb vom Mitarbeiterportal Bremen (MiP) Betriebsvertrag für die dWebTor Anbindung des Verfahrens Mitarbeiterportal 1. Änderung: Geändertes Preisblatt

| | | |
|---|---|---|
| zwischen | Der Senator für Finanzen Abteilung 4 - Zentrales IT-Management Digitalisierung öffentlicher Dienste, Rudolf-Hilferding-Platz 1, 28195 Bremen | „Auftraggeber" (AG) |
| und | Dataport, Anstalt öffentlichen Rechts, Altenholzer Straße 10-14, 24161 Altenholz | „Auftragnehmer" (AN) |

### 1. Leistungsumfang

Der Leistungsumfang ergibt sich aus dem Preisblatt Anlage(n) 2a, 2b

| Lfd. Nr. | Leistung (ggf. auch Kategorie, Berater) | Ort der Leistung | Leistungszeitraum | | Vergütung pro Einheit (Personentag, Stunden, Stück etc.) | Vergütungsart: Aufwand ggf. inkl. Obergrenze (OG) bzw. Pauschalfestpreis |
|---|---|---|---|---|---|---|
| | | | Beginn | Ende/Termin | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1 | V18780-1/3011005 Gem. Anlage 4 | Beim Auftragnehmer | 01.07.2025 | | gemäß Preisblatt Anlage(n) 2a, 2b | gemäß Preisblatt Anlage(n) 2a, 2b |
| 2 | V18780/3011005 | Beim Auftragnehmer | 01.07.2022 | 30.06.2025 | gemäß Preisblatt Anlage(n) 2a, 2b | gemäß Preisblatt Anlage(n) 2a, 2b |

☒ Reisekosten werden nicht gesondert vergütet.

☐ Reisekosten werden wie folgt vergütet

☒ Reisezeiten werden nicht gesondert vergütet.

☐ Reisezeiten werden wie folgt vergütet

### 2. Vertragsbestandteile

Es gelten nacheinander als Vertragsbestandteile:

- dieses Vertragsformular (Seiten 1 bis 3)
- Allgemeine Vertragsbedingungen von Dataport (Dataport AVB) in der jeweils geltenden Fassung (s. Nr. 3.1)
- Vertragsanlage(n) in folgender hierarchischer Reihenfolge: Nr. 1, 2a, 2b, 3, 4, 5, 6, 7, 8
- Ergänzende Vertragsbedingungen für die Erbringung von IT-Dienstleistungen (EVB-IT Dienstleistungs-AGB) in der bei Vertragsschluss geltenden Fassung
- Vergabe- und Vertragsordnung für Leistungen – ausgenommen Bauleistungen – Teil B (VOL/B) in der bei Vertragsschluss geltenden Fassung

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

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.

### 3. Sonstige Vereinbarungen

3.1 Allgemeines

Die Dataport AVB sind im Internet unter www.dataport.de veröffentlicht.

3.2 Umsatzsteuer

3.2.1 Verwendung der vertraglichen Leistungen

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

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

3.2.2 Umsatzsteuer bei anteiliger nicht-hoheitlicher Verwendung

☐ Der Auftraggeber bestätigt, dass die in diesem Vertrag bezogenen Leistungen durch den Auftraggeber anteilig im Rahmen seiner hoheitlichen Aufgabenwahrnehmung genutzt werden.

Es erfolgt eine Aufteilung der Rechnung in nichtsteuerbare Beistandsleistung und steuerbare Leistung zuzüglich gesetzlicher Umsatzsteuer. Die in diesem Vertrag bezogenen Leistungen werden vom Auftraggeber zu __ % hoheitlich verwendet. Die zu 100% fehlenden __ % der Leistungen unterliegen somit der Umsatzsteuer. Der nicht-hoheitliche Teil der Leistungsverwendung unterliegt der Umsatzsteuer und wird gesondert mit Umsatzsteuer in Rechnung gestellt.

3.2.3 Umsatzsteuer für im Hoheitsbereich verwendete Leistungen, die bis zur erstmaligen Anwendung des § 2b UStG 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.

3.2.4 Umsatzsteuer für im Hoheitsbereich verwendete Leistungen, die ab der erstmaligen Anwendung des § 2b UStG erbracht werden

Die aus diesem Vertrag seitens des Auftragnehmers zu erbringenden Leistungen unterliegen nicht der Umsatzsteuer, da diese aufgrund des Gesetzes zur Gewährleistung der digitalen Souveränität der Freien Hansestadt Bremen nur von juristischen Personen des öffentlichen Rechts erbracht werden dürfen (§ 2b Abs. 3 Nr. 1 UStG). Ausgenommen sind Leistungen auf dem Gebiet des Telekommunikationswesen (§ 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 Steuer-behörde in Anspruch genommen werden, hat der Auftraggeber dem Auftragnehmer die gezahlte Umsatzsteuer in voller Höhe zu erstatten, ggf. auch rückwirkend.

3.3 Verschwiegenheitspflicht

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

3.4 Bremer Informationsfreiheitsgesetz

3.4.1 Dieser Vertrag unterliegt dem Bremischen Informationsfreiheitsgesetz (BremIFG).

Er wird gemäß § 11 im zentralen elektronischen Informationsregister der Freien Hansestadt Bremen veröffentlicht. Unabhängig von einer Veröffentlichung kann er Gegenstand von Auskunftsanträgen nach dem BremIFG sein.

3.4.2 ☐ Optionale Erklärung der Nichtveröffentlichung

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

3.5 Mitwirkungs- und Beistellleistungen des Auftraggebers

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

3.5.1 Anlage 1 Ansprechpartner

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

Änderungen der Anlage 1 Ansprechpartner sind unverzüglich schriftlich mitzuteilen. Hierfür wird eine neue Anlage 1 vom Auftraggeber ausgefüllt. Die Anlage wird auf Anforderung durch den/ die Key Account Manager/ Key Account Managerin zur Verfügung gestellt. Die neue Anlage ist an [redacted] zu senden.

3.5.2 Gem. Anlage 4 Pkt. 2.3 und Anlage 5 Pkt. 5.2

3.5.3 Folgende weitere Beistellleistungen werden vereinbart

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

3.6 Ablösungen von Vereinbarungen/ Vorvereinbarungen

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

3.7 Weisungen

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

3.8 Laufzeit und Kündigung

Dieser Vertrag beginnt am 01.07.2025 und gilt für unbestimmte Zeit. Er ersetzt den Vertrag/die Änderungsverfahren gemäß Nummer 1 und führt dessen/deren Leistungen fort, soweit diese nicht durch Erfüllung oder auf sonstige Weise erledigt sind. Er kann erstmals unter Wahrung einer Frist von 6 Monaten zum 30.06.2026 gekündigt werden. Danach kann er zum Ende eines Kalenderjahres unter Wahrung einer Frist von 6 Monaten gekündigt werden. Die Kündigung bedarf der Textform.

3.9 Datenschutzrechtliche Auftragsverarbeitung

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

| **Auftragnehmer** | **Auftraggeber** |
|---|---|
| Ort, Datum: Bremen | Ort, Datum: |

[redacted]

# Ansprechpartner

zum Vertrag über die Beschaffung von IT-Dienstleistungen

| | |
|---|---|
| **Vertragsnummer/Kennung Auftraggeber:** | Ref. 32 |
| **Auftraggeber:** | **Der Senator für Finanzen**<br>**Abteilung 4 - Zentrales IT-Management**<br>**Digitalisierung öffentlicher Dienste**<br>**Rudolf-Hilferding-Platz 1**<br>**28195 Bremen** |
| **Rechnungsempfänger:** | **Freie Hansestadt Bremen**<br>**- Rechnungseingang FHB -**<br>**Senator für Finanzen**<br><br>**28026 Bremen** |
| **Leitweg-ID** | [redacted] |

Der Rechnungsempfänger ist immer auch der Mahnungsempfänger.

| | |
|---|---|
| **Zentrale Ansprechpartner des Auftragnehmers:** | [redacted] |
| **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.

Das Dokument ist gültig: bei Vertragsschluss

# Preisblatt Aufwände

## Gültig ab dem 01.07.2025

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

Mit einer jährlichen Obergrenze von 20.000,00 €.

Die Abrechnung erfolgt nach Aufwand.

Pos. 10-60: Die Rechnungsstellung erfolgt kalendermonatlich nachträglich gem. Leistungsnachweis.
Pos. 70-100: Die Rechnungsstellung erfolgt nach Bereitstellung.
Pos. 110-140: Erfolgt jeweils rückwirkend für ein Quartal auf Basis von Reports

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

Preisblatt erstellt am 30.07.2025
Gemäß Dataport-Servicekatalog - Artikelliste Version 7.2

# Preisblatt Jährlicher Festpreis

## Gültig ab dem 01.07.2025

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

**Gesamtpreis: 16.800,00 €**

[redacted]

Die Rechnungsstellung des Festpreises erfolgt zum 15.06. eines Kalenderjahres.

IAP-Nummer:
(wird von Dataport ausgefüllt) 40841

## Anlage Datenschutzrechtliche Festlegung des Auftraggebers

## Angaben des Verantwortlichen zur Auftragsverarbeitung[1]

| | |
|---|---|
| **Es findet keine Verarbeitung personenbezogener Daten statt.**<br>(Nachfolgende Felder brauchen nicht ausgefüllt werden.) | ☐ |
| **Vertragspartner/in ist Verantwortliche/r**<br>(Verantwortliche können ggf. abweichend zum Vertragspartner sein.) | ☑ |

**Name und Kontaktdaten der oder des Verantwortlichen**
(zu befüllen, wenn Vertragspartner/in nicht Verantwortliche/r ist)

**Name und Kontaktdaten der Vertragspartnerin / des Vertragspartners**
(zu befüllen, wenn Vertragspartner/in nicht Verantwortliche/r ist)

| | |
|---|---|
| **Für die Verarbeitung der personenbezogenen Daten gelten folgende Datenschutzregelungen:** | |
| Verordnung (EU) 2016/679 (DSGVO) | ☑ |
| Zusätzlich folgende bundes- bzw. landesrechtliche Regelungen (bitte Gesetz bzw. VO benennen) | ☑ |

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)

| | |
|---|---|
| Folgende bundes- bzw. landesrechtliche Regelungen zur Umsetzung der RiLi (EU) 2016/680[2] (bitte Gesetz bzw. VO benennen) | ☐ |

| 1. | **Art der Verarbeitung** („Was“)<br>(siehe z. B. Art. 28 Abs. 3 S. 1 DSGVO) |
|---|---|
| | dWebTor ist eine Infrastrukturlösung, die Zugriff von externe auf interne Web-Applikationen ermöglicht. Nutzer:innen erhalten somit Zugriff auf angebundene Verfahren. Der Zugriff ist mit einem dienstlichen oder auch privaten Gerät über das Internet möglich, jedoch ausschließlich auf jeweils freigegebene Inhalte und Anwendungen. |
| | **Zweck der Verarbeitung** („Wofür“)<br>(siehe z. B. Art. 28 Abs. 3 S. 1 DSGVO) |
| | Authentifizierung eines dWebTor-Nutzers aus dem Internet über die Sicherheitsinfrastruktur dWebTor an einer zentralen Zugangsinfrastruktur der FHB für Webdienstleistungen.<br>Für die Absicherung der Authentifizierung wird optional der Multiverfahrensdienst Multifaktorauthentifizierung verwendet. |

| 2. | **Beschreibung der Kategorien von personenbezogenen Daten**<br>(siehe z. B. Art. 28 Abs. 3 S. 1 DSGVO bzw. Art. 30 Abs. 1 S. 2 lit. c) | |
|---|---|---|
| | **Stammdaten** (z.B. Name, Geburtsdatum, Geburtsort, Wohnort) | ☑ |
| | **Kontaktdaten** (z.B. Mailadresse, Telefonnummer, Mobilnummer) | ☑ |
| | **Kennummer** (z.B. Personalnummer, Sozialversicherungsnummer, Steuer-ID) | ☐ |
| | **Identitätsdaten** (z.B. Username, User-ID, Organisationseinheit) | ☑ |
| | **Zahlungsdaten** (z.B. Kontonummer / IBAN, Geldinstitut, Abrechnungsdaten) | ☐ |
| | **Metadaten** (z.B. Protokolldaten, IP-Adresse, Standortdaten, Cookies) | ☑ |
| | **Bilddaten, Videodaten, Audio- und Sprachdaten** | ☐ |
| | **Besondere Kategorien personenbezogener Daten (Art. 9 Abs. 1 DSGVO)**<br>(z.B. rassische und ethnische Herkunft, Gewerkschaftszugehörigkeit, Gesundheit, genetische und biometrische Daten, religiöse oder weltanschauliche Überzeugungen) | ☐ |
| | **Weitere**<br>**(bitte nachfolgend benennen):** | ☐ |
| | | |

IAP-Nummer:
(wird von Dataport ausgefüllt) 40841

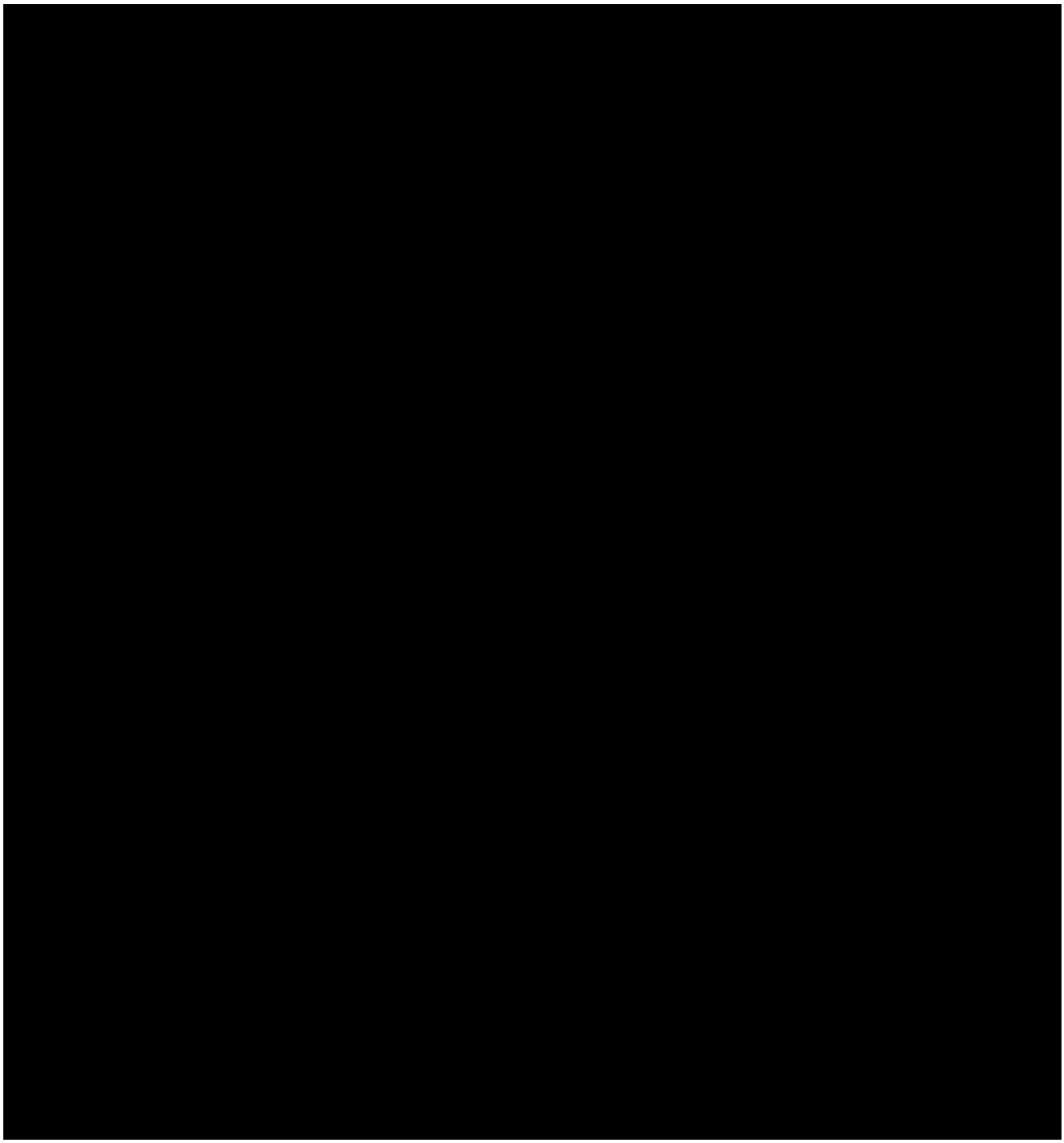
| 3. | **Beschreibung der Kategorien betroffener Personen**<br>(siehe z. B. Art. 28 Abs. 3 S. 1 DSGVO) | |
|---|---|---|
| | Bürger / Einwohner | ☐ |
| | Dienstleister | ☑ |
| | Kunden | ☐ |
| | Interne Beschäftigte (Arbeitnehmer und Beamte) | ☑ |
| | Externe Beschäftigte | ☑ |
| | Bewerber | ☐ |
| | Kinder | ☐ |
| | (Sozial-) Leistungsempfänger | ☐ |
| | Schuldner | ☐ |
| | Patienten | ☐ |
| | Straftäter | ☐ |
| | **Weitere**<br>**(bitte nachfolgend benennen):** | ☐ |
| | | |

| 4. | **Es findet keine Übermittlung personenbezogener Daten an ein Drittland oder an eine internationale Organisation statt.** (Nachfolgende Felder brauchen nicht ausgefüllt werden.) | ☑ |
|---|---|---|
| | **Übermittlung von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation**<br>(siehe z. B. Art. 30 Abs. 1 S. 2 lit. e DSGVO)<br>(Werden Kundenlösungen genutzt, die nicht im Dataport-Standard betrieben werden, muss dies zuvor von Dataport erarbeitet werden.) | |
| | | |

[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.

## Liste der weiteren Auftragsverarbeiter



# Leistungsbeschreibung

# dWebTor für das Mitarbeiterportal Bremen (MiP)

Version: 1.0
Stand: 04.07.2025

## Inhaltsverzeichnis

# 1 Einleitung

## 1.1 Allgemeines

Mit dWebTor können interne Web-Verfahren aus dem Dataport Rechenzentrum über das Internet mit ungemanagten Clients aufgerufen und bedient werden. Zur Absicherung dieser Zugriffe von extern dienen sowohl technische als auch organisatorische Maßnahmen. Ein externer Zugriff auf einzelne Verfahren ist für Mitarbeiter interessant, die viel mobil unterwegs sind. Aber auch Dienstleister, Ehrenamtliche oder Mitarbeiter, die nicht am Behördennetz angeschlossen sind, können dWebTor für den Zugriff auf interne Verfahren nutzen. dWebtor kann grundsätzlich von allen Trägerländern Dataports eingesetzt werden, die webbasierte Verfahren im Twin Data Center betreiben. Für die Authentifizierung wird ein Benutzerkonto in einem von Dataport gemanagten AD benötigt, sowie weitere Berechtigungs-Strukturen im Hintergrund.

## 1.2 Leistungsgegenstand

Der dWebTor Service setzt sich aus Infrastrukturkosten, Betriebsleistungen sowie fachlichem Verfahrensmanagement und Beratungsleistungen zusammen. Eine genauere Beschreibung der Leistungen und eingesetzten Technik finden sich in Kapitel 3.

# 2 Rahmenbedingungen

Der Auftragnehmer betreibt die Produkt-Infrastruktur (Schutzbedarf Hoch) nach BSI-IT-Grundschutz im Dataport Twin Data Center. Zusätzlich berät, organisiert und koordiniert das Fachliche Verfahrensmanagement Standardaufträge, Neuanfragen und betriebliche Themen auf Seiten des Auftragnehmers.

Der Auftraggeber ist verpflichtet, bestimmte Mitwirkungspflichten zu erbringen, die in Kapitel 2.3. näher erläutert werden. Mitwirkungspflichten ergeben sich insbesondere im Bereich der AD-Berechtigungsstrukturen, der Information und Abstimmungen mit den Endanwendern, sowie Test- und ggf. technische Anpassungspflichten auf Seiten der angebundenen Fachverfahren.

Sollten sich aus betrieblichen oder wirtschaftlichen Gründen erhebliche Änderungen an dem vereinbarten Leistungsumfang oder den Kosten ergeben, wird der Auftraggeber rechtzeitig informiert. Sollte eine Partei den Vertrag kündigen, greifen die Regelungen, die in Kapitel 2.4 erläutert werden.

## 2.1 Changemanagement

Das Changemanagement erfolgt gemäß ITIL. Eine Übersicht über zustimmungspflichtige Changes und Changes ohne Kundenzustimmung gibt die folgende Tabelle:

| Changes | Beschreibung | Tests | Freigaben |
|---|---|---|---|
| Changes mit Kundenzustimmung | Änderungen an der Konfiguration des Zugangs zum Verfahren sowie Neuanbindungen erfordern einen schriftlichen Kundenauftrag | Fachliche Tests nach Konfigurationsänderungen obliegen dem jeweiligen Verantwortlichen des Verfahrens. | Kundenfreigaben sind schriftlich zu erteilen. |
| Changes ohne Kundenzustimmung und Testpflicht | Änderungen an der Basisinfrastruktur, insbesondere Sicherheitsupdates | Fachliche Tests sind nur nach vorheriger Information durch Dataport erforderlich | Es ist keine Kundenfreigabe erforderlich. |

Änderungen an der Infrastruktur werden immer nur auf Basis vom ITIL-Changemanagement durchgeführt. Die Leistung des Auftragnehmers erfolgt ausschließlich auf unterstützten Plattformen, die durch Hersteller freigegeben sind. Daraus ergibt sich regelmäßig eine Veränderung der Infrastruktur. Um den laufenden Betrieb zu sichern, werden diese Veränderungen für den zentralen Teil nach Maßgabe des Auftragnehmers realisiert. Dies wird im Voraus angekündigt. Davon ausgenommen sind kurzfristig durchzuführende, sicherheitsrelevante Änderungen.

## 2.2 Incident Management

Das Incident Management reagiert auf Störungen und sorgt für die schnellstmögliche Wiederherstellung der vereinbaren Services. Störungen werden im Rahmen des bei Dataport standardisierten Incident Managements bearbeitet. Zur Bearbeitung gehören folgende Aufgaben und Zuständigkeiten:

| Aufgaben und Zuständigkeiten | Auftrag-nehmer | Auftrag-geber |
|---|---|---|
| Störungsannahme interne Nutzer (1st Level) | **V, D** | |
| Störungsannahme externe Nutzer Nutzer (1st Level) | | **V, D** |
| 2nd und 3rd Level Incident Steuerung | **V, D** | |
| Eröffnung eines 3rd Level Ticket beim Hersteller und Tracking des Herstellers der IT-Infrastrukturkomponenten | **V, D** | **I** |

Der Auftraggeber ist grundsätzlich verpflichtet, die Anwender in die Bedienung von dWebTor einweisen zu lassen. Interne Anwender können sich bei Problemen mit Ihrem dWebTor Zugang an den Dataport UHD wenden. Externe Anwender sind für den Dataport UHD nicht auftragsberechtigt. Diese Anwendergruppe muss sich bei Problemen an die jeweils behördliche IT wenden, die Ihren Zugang eingerichtet hat. Sollte die IT-Stelle der zugehörigen Behörde das Problem nicht lösen können, ist sie ticketberechtigt und kann sich an den Dataport UHD wenden.

Der Auftragnehmer übernimmt keine Gewähr, dass der dWebTor Zugang unter jedwedem Betriebssystem und jedwedem Browser funktioniert. Grundsätzlich gilt der Browser als Standard für die dWebTor Nutzung für den das angebundene Verfahren empfohlen ist. Im Rahmen vertretbaren Aufwands wird nach Lösungen für Incidents gesucht, die mit einzelnen Browsern oder Betriebssystemen zusammenhängen. Incidents, die aufgrund eines abweichenden Betriebssystems und/oder Browsers nicht gelöst werden können, werden als Known Problem behandelt und nicht weiterverfolgt.

## 2.3 Mitwirkungsrechte und -pflichten

Die vom Auftragnehmer zugesagten Leistungen erfolgen auf Anforderung des Auftraggebers. Für die Bereitstellung des dWebTor Services gibt es sowohl allgemeine als auch verfahrensbezogene Mitwirkungspflichten.

**Übersicht allgemeiner Mitwirkungspflichten:**

| Aufgaben und Zuständigkeiten | Auftrag-nehmer | Auftrag-geber |
|---|---|---|
| Unterrichtung der Anwender darüber, wie dWebTor funktioniert sowie Verpflichtung der Nutzer zur Einhaltung mitgeltender Sicherheitsregelungen für die Nutzung privater Endgeräte (siehe Anlage 4. | | **V, D** |
| Erstellung und die Pflege von AD-Strukturen, die für das Berechtigungsmanagement von internen und externen Nutzern benötigt werden. | **I, D** | **V** |
| Sicherstellung, dass Externe nur ein Konto in einem internen AD bekommen, wenn sie ein berechtigtes dienstliches Interesse des Trägerlandes über einen gewissen Zeitraum erfüllen. | | **V, D** |
| Sicherstellung, dass Externe nur ein Konto in einem internen AD bekommen, wenn sie mit Namen und Kontaktdaten dem Auftraggeber bekannt sind und einen Ansprechpartner beim Auftraggeber haben. Die Kontaktdaten des Externen sind zu dokumentieren und regelmäßig zu aktualisieren | | **V, D** |
| Sicherstellung, dass ausschließlich Mitarbeiter und Externe dWebTor nutzen, die entweder durch Unterschrift, Dienstvereinbarung/-vorschrift oder eine andere geeignete Möglichkeit die Nutzungsbedingungen bestätigt haben | | **V, D** |
| Zeitnahe Löschung von internen Konten für Externe, wenn diese nicht mehr benötigt werden. | | **V, D** |

**Übersicht verfahrensbezogener Mitwirkungspflichten:**

| Aufgaben und Zuständigkeiten | Auftrag-nehmer | Auftrag-geber |
|---|---|---|
| Betrieb der angebundenen Verfahren und Gewährleistung der Erreichbarkeit. | **I** | **V, D** |
| Anwenderbetreuung bei der Nutzung des Verfahrens über dWebTor. | **I, B** | **V, D** |
| Verfahrensänderungen am angebundenen Verfahren und die Abstimmung dieser mit dem dWebTor-Produktverantwortlichen. | **I, B** | **V, D** |
| Durchführung fachlicher Tests bei Neuanbindung, Veränderungen am Backend oder nach Aufforderung (2.1.) | **I, B** | **V, D** |
| Bearbeitung von Incidents, die durch das angebundene Verfahren verursacht werden oder nicht klar zuordenbar sind. | **I, B** | **V, D** |
| Sicherheitsbetrachtungen und –bewertungen der angebundenen Verfahren sowie Übernahme der Restrisiken wegen des zusätzlichen externen Zugangs über dWebTor | **I, B** | **V, D** |

| | | |
|---|---|---|
| Klärung von Lizenzfragen und Bereitstellung ggf. benötigter Lizenzen für die Nutzung der angebundenen Verfahren über verschiedene Endgeräte über das Internet. | | **V, D** |
| Ggf. Anpassungen der angebundenen Verfahren, wenn Dataport die zugrundeliegende Infrastruktur aus Betriebsgründen ändern muss. | **I, B** | **V, D** |
| Sicherstellung, dass Admin-Konten nicht für einen Zugriff über dWebTor zugelassen werden. | | **V, D** |

Übersicht der für die Berechtigungsstruktur relevanten Mitwirkungspflichten:

| Aufgaben und Zuständigkeiten | Auftrag-nehmer | Auftrag-geber |
|---|---|---|
| *Zustimmung und Abnahme der AD-Strukturen für dWebTor.* | **I, B** | **V, D** |
| *Erstellung und Aufbau erforderlicher AD-Strukturen für dWebTor.* | **V, D, I** | **I** |
| *Pflege der dWebTor AD-Strukturen.* | **V, D** | **I** |
| *Erstellung erforderlicher AD-Strukturen auf Seite des Auftraggebers. Insbesondere erforderliche Berechtigungsgruppen und Usermanagement.* | **I, B** | **V, D** |
| *Sicherstellung, dass nur mit Kontaktdaten bekannte Externe mit einem berechtigten dienstlichen Interesse ein externes Konto erhalten und zur Einhaltung der dWebtor Nutzungsbedingungen verpflichtet sind.* | **I** | **V, D** |
| *Information der Anwender*innen über Pflicht, bei nicht mehr Nutzung des Zugangs die zuständige IT zu informieren und das Konto aus der Berechtigungsgruppe zu entfernen oder im Fall eines externen Kontos löschen zu lassen.* | **I** | **V, D** |
| *Gegenseitige Information bei Änderung relevanter AD-Strukturen.* | **V, D, B, I** | **V, D, B, I** |

## 2.4 Ergänzende Kündigungsmodalitäten

Im Falle einer Kündigung wird der externe Zugang mit sofortiger Wirkung zum Zeitpunkt des Vertragsendes gesperrt. Ein Abbau der Konfiguration und ggf. der begleitenden Strukturen erfolgt durch den Auftragnehmer nach Vertragsende. Der Auftraggeber ist verpflichtet, seine Mitwirkungspflichten bis zum Vertragsende in dem Umfang zu erbringen, der einen geregelten und sicheren Betrieb gewährleistet. Sollte der Auftraggeber dies nicht erfüllen können, behält sich Dataport eine sofortige Sperrung des externen Zugangs vor.

Die folgende Tabelle gibt eine Übersicht über die Rückgabe- und Abbauregelungen:

| **Komponente** | **Rückgabe** | **Abbau** | **Verantwortlich** |
|---|---|---|---|
| ALG-Konfiguration | nein | Ja, nach Vertragsende | Dataport dWebTor |
| AD-Strukturen (Gruppen, Skripte, Passwort-Richtlinie) | Bei Bedarf können die Skripte und Dokumentationen zu den Strukturen bei Vertragsende bereitgestellt werden | Ein Abbau der Strukturen erfolgt bei keiner weiteren Verwendung über andere Verträge nach Vertragsende | Dataport dWebTor |

| | | | |
|---|---|---|---|
| Password Self Service | Erfolgt gemäß Vertragsbestimmungen von Online Dienste | Ja, nach Vertragsende | Dataport Online Dienste |
| Formalien | | Der Abbau der Anbindung wird schriftlich vom Auftragnehmer bestätigt. | Dataport dWebTor |

# 3 Leistungsbeschreibung

dWebTor steht drei Nutzergruppen zur Verfügung: Mitarbeitern des jeweiligen Landes, die bereits über einen AD-Account verfügen, Mitarbeitern des Landes ohne AD-Account sowie Dritten, die einen Zugriff aus dienstlichem Interesse des Landes oder zur Erfüllung dienstlicher Aufgaben aufgrund von Rechtsvorschriften benötigen und noch kein Zugangskonto besitzen („externe Nutzer“). Der Zugriff von extern erfolgt mittels eines Sicherheitsgateways (ALG).

Das Sicherheitsgateway übernimmt die Authentifizierung der Nutzer und sichert den Aufruf des Verfahrens aus dem Internet.

Authentifizierung der Nutzer

Die Authentifizierung der Nutzer erfolgt gegen das jeweilige Landes AD. Die Authentifizierung erfolgt mindestens mit Benutzernamen und Passwort (Single Faktor). Die AD Konten sind durch das ALG gegen mutwillige Sperrung durch Angriffe geschützt. Die Nutzung einer Multifaktor Authentifizierung (MFA) ist vorgesehen und zum Teil bereits konfiguriert. Bei Aktivierung der MFA verlangt das Sicherheitsgateway einen zusätzlichen Passcode.

Aufruf des Verfahrens aus dem Internet.

Der Datenstrom wird auf dem ALG terminiert. Das ALG entschlüsselt den Datenstrom und prüft den Datenverkehr auf verdächtige Muster (Hackerangriffe wie z.B. SQL Injection), um ihn dann wieder zu verschlüsseln und weiterzuleiten. Es hält grundsätzlich zwei Datenverbindungen offen – eine zum Client und eine zum internen Verfahren. Auf diese Art kommuniziert der Client niemals direkt mit dem Verfahren aus dem Internet heraus. Ein TimeOut verhindert das unbegrenzte Laufen einer Session, sollte ein Anwender sich nicht korrekt abmelden.

Die Pflege der externen Nutzerkonten wird durch Skripte unterstützt.

Das ALG verarbeitet keine personenbezogenen Daten, außer „Benutzername und Passwort“ bei der Authentifizierung an dem jeweils zuständigen AD. Das ALG prüft zusätzlich anhand einer zentralen Berechtigungsgruppe, ob ein Nutzer von extern zugreifen darf. Nach drei Fehlversuchen bei der Passworteingabe wird das Konto eines Anwenders für den externen Zugang 60 Minuten lang gesperrt.

## 3.1 Leistungsumfang

Zur Nutzung von dWebTor können unterschiedliche Servicepakete (XS und S) vereinbart werden, die sowohl Infrastrukturkosten als auch Betriebs- und Fachleistungen umfassen. Der Leistungsumfang ist zum Teil an individuelle Wünsche oder Rahmenbedingungen anpassbar, dazu mehr im Kapitel 3.3. „Optionale Leistungen und Leistungen nach Aufwand“.

### 3.1.1 Leistungsumfang der dWebTor Servicepakete

Im Folgenden werden die Leistungen für die Pakete „XS“ und „S“ näher erläutert.

Immer inkludiert im dWebTor-Service sind eine Reihe von Betriebs- und fachlichen Leistungen. Die folgenden VDBI-Tabellen geben dazu eine Übersicht. Für Mitwirkungspflichten des Auftraggebers ist das Kapitel 2.3 maßgeblich.

**Im dWebTor Servicepaket sind folgende Betriebsleistungen vorhanden:**

| Aufgaben und Zuständigkeiten | Auftrag-nehmer | Auftrag-geber |
|---|---|---|
| Betrieb der Infrastruktur und aller zugehörigen Komponenten im TDC gemäß BSI Vorgaben, inkl. Lizenzmanagement. | **V, D** | |
| (Weiter-)Entwicklung der technischen dWebTor Architektur. | **V, D** | **I** |
| Technische Umsetzung von Anbindungen webbasierter Fachverfahren. | **V, D** | **B, I** |
| Technische Umsetzung von Konfigurationsänderungen aufgrund von neuen oder geänderten Sicherheits- sowie sonstiger Anforderungen. | **V, D** | **B, I** |
| Durchführung und Koordination von Konfigurationsmanagement und Change Management für alle betriebsrelevanten Bereiche. | **V, D** | **I** |
| Antwort auf Anfragen zu Störungen und Problemen beim Auftraggeber. | **V, D** | **I** |
| Beseitigung von Störungen, Restart / Recovery von Systemkomponenten unter Einhaltung der Eskalationsverfahren. | **V, D** | **I** |
| Kapazitätsüberwachung und -auswertung der Hardware und Systemsoftware, ggf. Maßnahmenplanung bei Kapazitätsverletzungen (+/-). | **V, D, B** | |

**Im dWebTor Servicepaket sind folgende fachlichen Leistungen vorhanden:**

| Aufgaben und Zuständigkeiten | Auftrag-nehmer | Auftrag-geber |
|---|---|---|
| Fachliche Organisation und Begleitung des technischen Betriebes. | **V, D** | |
| Fachliche Begleitung und Organisation von Anbindungen webbasierter Fachverfahren. | **V, D** | **B, I** |
| Fachliche Organisation und Begleitung von Konfigurationsänderungen aufgrund von neuen oder geänderten Sicherheits- sowie sonstiger Anforderungen. | **V, D** | **B, I** |
| Regelmäßige Fortführung, Prüfung und ggf. Erweiterung des Sicherheitskonzeptes. | **V, D** | **I** |
| Support von Endanwendern und Ticketbearbeitung gem. 2.2 | **V, D** | **I** |

Für die notwendigen Berechtigungsstrukturen erbringt der Auftragnehmer folgende Leistungen:

- Die Pflege einer zentralen dWebTor Ressourcengruppe, die für dWebTor berechtigt, inkl. Berechtigungskonzept gemäß aktueller AD-Richtlinien Dataports. *
- Bereitstellung des Kontotyps dWebTor-Benutzer im KPT inkl. eigener Passwortrichtlinie
- Statistik über die Anzahl der Nutzer:innen (intern und extern), anonymisierte Reports bei Bedarf an den Auftraggeber. Die Vollständigkeit der Statistik wird durch die Einhaltung des Berechtigungskonzeptes bedingt.
- Bei Abruf: Kosten für externe Konten werden auf Basis der Statistik regelmäßig abgerechnet.

* Hinweis: Die detaillierte Rollen- und Berechtigungsstruktur liegt in der Verantwortung des Auftraggebers. Bei Bedarf können Unterstützungsleistungen nach Aufwand beim Auftragnehmer beauftragt werden.

## 3.2 Leistungsabgrenzung

Im dWebTor Service nicht enthalten sind die folgenden Tätigkeiten:

- Fachliche Konzeption neuer fachlicher Anforderungen: Eine erste Einschätzung zu neuen generellen Anforderungen an den dWebTor-Zugang kann erfolgen, allerdings ist eine fachliche Konzeption, auf deren Basis ein Umsetzungsprojekt starten kann, gesondert als Projekt zu beauftragen. Die Produktverantwortung dWebTor behält sich in jedem Fall vor, Änderungen am Produkt dWebTor begründet abzulehnen, wenn beispielsweise die Natur des Produktes durch eine Änderung zu stark verändert werden würde oder es nicht vertretbare Auswirkungen auf andere Kunden des Produktes gibt.

- Technische Umsetzung neuer fachlicher Anforderungen: Die technische Umsetzung neuer genereller Anforderungen erfolgt grundsätzlich auf Basis eines zuvor zu erstellenden Konzepts und ist Teil eines Änderungs-/ oder Einführungsprojektes, das der Auftraggeber gesondert beauftragen muss. Eine technische Umsetzung neuer fachlicher Anforderungen an dWebTor selbst ist stets und ausschließlich durch die Produktverantwortung von dWebTor zu beauftragen.

- Individualisierung der Log-In Maske: Anforderungen auf eine Individualisierung der Log-In Maske müssen auf technische Umsetzbarkeit geprüft werden. Personalleistungen für die Prüfung und Umsetzung werden nach Aufwand in Rechnung gestellt.

- Planung und Durchführung von Schulungen: Es werden keine Schulungen zur Nutzung von dWebTor geplant oder durchgeführt.

- Projektleistungen zur Einführung neuer technischer Lösungen oder Teillösungen: Projektmanagement-Tätigkeiten oder Beratungsleistungen für die Einführung neuer technischer Lösungen oder Teillösungen sind gesondert zu beauftragen.

- Personalleistungen in Zusammenhang mit einem Passwort Self Service für dWebTor Nutzer, die über den Support der Nutzer hinausgehen.

Auf technischer Seite gelten folgende Beschränkungen:

- Der Zugriff aus dem Internet benötigt auf Anwender Seite ausreichende Bandbreite, um das Verfahren nutzen zu können. dWebTor übernimmt keine Verantwortung für den Internetanschluss des Anwenders.

- Grundsätzlich ist die zugrunde liegende ALG-Technik für Erweiterungen skalierbar. Dennoch sind die Ressourcen der zugrunde liegenden ALG-Technik begrenzt. Je nach Erhöhung der Anwenderzahlen und veröffentlichten Verfahren können technische Erweiterungen notwendig sein, die Aufwand und ggf. weitere Kosten mit sich bringen.

- Die Hauptaufgabe des ALG liegt in der Durchführung der Authentifizierung und der Überwachung des Datenstroms auf Angriffe. Notwendige Anpassungen an den Berechtigungsstrukturen des Verfahrens für Unterscheidungen zwischen internem und externem Zugriff können nicht über das ALG abgebildet werden.

- Die Authentifizierungstechnologie wird gelegentlich an neue Anforderungen und Sicherheitsstandards angepasst. Dadurch können sich Zuarbeiten auf Verfahrensebene ergeben, damit der Zugriff weiterhin funktioniert.

## 3.3 Optionale Leistungen und Leistungen nach Aufwand

Grundsätzlich wird aus den vereinbarten Kontingenten zum Festpreis geleistet. Sind diese Kontingente überschritten oder werden Aufträge platziert, die nicht zum beschriebenen Leistungsumfang gehören, wird die Leistung nach Aufwand in Rechnung gestellt. Sollten Zusatzleistungen benötigt werden, die im Folgenden nicht beschrieben werden, müssen diese geprüft und gesondert beauftragt werden.

Übersicht Leistungen nach Aufwand und optionale Leistungen:

| Aufgaben und Zuständigkeiten | Auftrag-nehmer | Auftrag-geber |
|---|---|---|
| Leistungen nach Aufwand | | |
| Anschaffen und Einspielen von Zertifikaten für eine gesicherte, verschlüsselte Verbindung. | **V, D** | **B, I** |
| Zusätzliche Verfahrensanbindungen | **V, D** | **B, I** |
| dWebTor Konten, Abrechnung auf Basis monatlicher Reports gemäß Leistungsumfang mit oder ohne MVD MFA | **V, D** | **B, I** |
| Erhöhung der Anzahl der Gesamtnutzer des externen Zugangs über dWebTor | **V, D** | **I** |
| Fachliche Betreuung des Passwort Self Services im Bremen Serviceportal (bei Bedarf) | **V, D** | **I** |
| Skripte für verschiedene Mechanismen und Statistiken (z.B. Skripte zur Deaktivierung und Löschung von ungenutzten externen Konten). | **V, D** | **B, I** |
| Dokumentation der Strukturen | **V, D** | **B, I** |
| Optionale Leistungen | | |
| Fachliche Beratungsleistung hinsichtlich neuer fachlicher Anforderungen an dWebTor. | **V, D** | **B, I** |
| Beauftragung, Begleitung und Nacharbeiten von Penetrationstests | **V, D** | **I** |
| Umfangreichere Sicherheitsberatung zu veränderten Bedingungen, neuen Anforderungen etc. | **V, D** | **B, I** |
| Technische Beratungsleistung hinsichtlich neuer fachlicher Anforderungen an dWebTor. | **V, D** | **B, I** |
| Ausschreibung eines Penetrationstests für den externen Zugang und Auswertung desselbigen für angebundene Verfahren nach Absprache. | **V, D** | **I** |

### 3.3.1 Leistung nach Aufwand – dWebTor Konten

Für die Nutzung von dWebTor erhalten externe Nutzer ein AD-Konto im AD land.hb-netz.de mit dem Kontentyp dWebTor.

[redacted]

[redacted]

Solange die Multifaktorauthentifizierung nicht aktiviert wurde, wird als Abrechnungsgrundlage der Service „Service AD-Konto dWebTor “ herangezogen. Sobald die erste dWebTor Rollengruppe die

Multifaktorauthentifizierung nutzen muss, wird als Abrechnungsgrundlage der Service „Service AD-Konto dWebTor MVD MFA“ verwendet.

### 3.3.2 Erläuterung zum Usermanagement beim Auftraggeber

Die jeweiligen IT-Stellen der teilnehmenden Ressorts sind für die Benutzer- und Gruppenverwaltung selbst zuständig und fungieren als Ansprechpartner für die eigenen externen dWebTor-Benutzer. Auch für interne dWebTor-Nutzer übernehmen die IT-Stellen die Aufgabe, die Gruppenmitgliedschaft für die dWebTor-Berechtigung zu verwalten. Dies gilt sowohl für Basis als auch Non-Basis-Kunden. Non-Basis-Kunden müssen zumindest zwei Arbeitsplätze so vollwertig ausstatten, dass eine Administration der dWebTor-Konten und Berechtigungsstrukturen eigenständig erfolgen kann.

[redacted]

Die IT-Stelle der beitretenden Behörde übernimmt die Gesamtverantwortung für „ihre“ dWebTor-Konten und Sicherheitsgruppen. Die Benutzer- und Gruppenverwaltung erfolgt ausschließlich über das Kontenpflegetool und ist nicht Bestandteil dieser Leistungsbeschreibung.

| Aufgaben und Zuständigkeiten | Auftrag-nehmer | Auftrag-geber |
|---|---|---|
| Verwaltung der Benutzerkonten | | **V, D** |
| Verwaltung der Rollengruppen | **I, B** | **V, D** |
| Verwaltung der Ressourcengruppe | **V, D** | |
| Berechtigung der Rollengruppen | **V, B** | **I** |

### 3.3.3 Erläuterung zu den AD-Leistungen des Auftragnehmers

Der Auftragnehmer stellt sicher, dass das AD und die dazugehörigen Autorisierungs- und Authentifizierungsdienste zu den vereinbarten Zeiten und der vereinbarten Qualität zur Verfügung stehen und uneingeschränkt genutzt werden können. Darüber hinaus ist der Auftragnehmer für die Administration der folgenden zentralen Sicherheitsgruppen zuständig:

[redacted]

Die detaillierte Rollenberechtigungsstruktur obliegt dem Auftraggeber.

### 3.3.4 Erläuterung zum Passwort Self Service

Externen dWebTor-Nutzern steht ein Passwort Self Service im Serviceportal Bremen zur Verfügung. Er dient den externen Nutzern dazu, sich selbst ihr erstes Passwort zu vergeben, oder bei Bedarf auch ein neues Passwort zu vergeben. Die Passwortvergabe erfolgt automatisiert und wird über die im dWebTor-Konto hinterlegte Email bestätigt. Die Webapplikation des Passwort Self Services wird von Dataport Onlinedienste gemäß den fachlichen Vorgaben entwickelt und gepflegt. Die Abrechnung erfolgt nach Aufwand oder auf Basis eines gesonderten Vertrags.

# 4 Leistungskennzahlen

Leistungskennzahlen für Betriebsleistungen.

Die Verfügbarkeit wird für dWebTor bis zur Datenübergabeschnittstelle ans WAN / Internet garantiert.

Ist die Verfügbarkeit durch folgende Gründe gestört, so gilt die Gewährleistung der Verfügbarkeit für diese Zeiten nicht:

- aufgrund von höherer Gewalt und Katastrophen
- Qualität der beigestellten Software
- Unterbrechung aufgrund von Vorgaben des Auftraggebers
- infolge Unterbleibens oder verzögerter Erfüllung von Mitwirkungspflichten durch den Auftraggeber

# 5 Erläuterungen

## 5.1 Glossar

| | |
|---|---|
| AD | Active Directory |
| ALG | Application Layer Gateway |
| KPT | Kontenpflegetool |
| MFA | Multi Faktor Authentifizierung |
| OU | Organizational Unit |
| TDC | Twin Data Center |

## 5.2 Erläuterung VDBI

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

# Security Service Level Agreement

# für dWebTor Betrieb des Mitarbeiterportals Bremen

## Inhaltsverzeichnis

# 1. Einleitung

## 1.1 Leistungsgegenstand

Mit der Anlage **S**ecurity **S**ervice **L**evel **A**greement (SSLA) wird zwischen den Vertragspartnern ergänzend vereinbart, wie die Leistungserbringung des zugrundeliegendem Betriebs- oder Servicevertrages unter Informationssicherheitsgesichtspunkten erfolgt.

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

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

## 1.2 Aufbau des Dokumentes

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

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

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

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

# 2. Leistungsumfang und -beschreibung

## 2.1 Informationssicherheitsmanagementsystem (ISMS)

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

- die im IT-Sicherheits- und Datenschutzmanagementhandbuch des Auftragnehmers festgelegten und mit denen im Geschäftsverteilungsplan (GVP[1]) dokumentierten Funktionsträger
- die im IT-Sicherheits- und Datenschutzmanagementhandbuch des Auftragnehmers festgelegten Prozesse des Informationssicherheitsmanagements:
  - der Betrieb des ISMS
  - die Umsetzung der Grundschutz-Vorgehensweise auf Grundlage des BSI-Standards 200-2
  - die Sicherheitskonzepterstellung
  - das Sicherheitsvorfallmanagement
  - das Notfall- und Notfallvorsorgemanagement
- sowie das sicherheitsrelevante Regelwerk des Auftragnehmers zur Informationssicherheit

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

## 2.2 Verfahrensbezogener IT-Sicherheitskoordinator (ITSK)

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

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

Der ITSK ist verantwortlich für die Erstellung des auftragsbezogenen Sicherheitskonzeptes sowie die jährliche Bereitstellung des Sicherheitsnachweises[2] (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 kundenöffentliches 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-Grundschutzkatalogen[3] vorgegebenen BASIS- und STANDARD-Anforderungen, die in den Zuständigkeitsbereich des Auftragnehmers fallen, für den von dieser Vereinbarung betroffenen Informationsverbund umzusetzen.

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

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

## 2.4 Erstellung und Pflege der Sicherheitsdokumentation

### 2.4.1 Umfang

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

Das Sicherheitskonzept beschreibt die nach IT-Grundschutz-Methodik zusammengefasste Struktur des betrachteten Informationsverbundes sowie die maßgeblichen[4] 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.

---

[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.

### 2.4.2 Struktur und Standardordner

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

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

#### 2.4.2.1 A.0 Richtlinien für Informationssicherheit

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

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

#### 2.4.2.2 A.1 IT-Strukturanalyse

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

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

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

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

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

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

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

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

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

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

#### 2.4.2.5 A.D0 Ergänzende Sicherheitskonzepte

Sofern für den unter dieser Vereinbarung betrachteten Informationsverbund weitere Sicherheitskonzepte maßgeblich sind, werden diese in diesem Ordner beigelegt.[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 Bausteinebene). Kommt keine Fachanwendung zum Einsatz (z.B. bei einem reinen Infrastrukturbetrieb) kann der Workshop entbehrlich sein.

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

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

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

## 2.6 Bereitstellung

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

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

## 2.7 Prüfung der Umsetzung

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

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

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

# 3. Abgrenzung der Leistungen

## 3.1 Spezifische datenschutzrechtliche Anforderungen

Der mit dem SSLA vereinbarte IT-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 Bausteinebene).

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

## 3.3 Einsicht in interne Dokumente des Auftragnehmers

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

## 3.4 Abweichungen

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

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

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

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

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

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

## 3.5 Fortschreibung des IT-Grundschutzes

Der IT-Grundschutz des Bundesamtes für 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 Bausteinebene

In den beim Auftragnehmer modellierten IT-Grundschutz-Bausteinen können sich Sicherheitsanforderungen befinden, für die die Umsetzungsverantwortung beim Auftraggeber liegt[6]. 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 Schutzbedarfsfeststellung und Risikoanalyse nach IT-Grundschutz

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

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

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

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

## 5.2 Mitwirkungspflichten des Auftraggebers

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

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

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

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

2) Risikobewertung[7] bei der Erweiterung des betrachteten IT-Verbundes um fachliche oder technische Komponenten oder der Erweiterung um Kommunikationsschnittstellen, insbesondere zu Verfahren mit niedrigerem Sicherheitsniveau[8]
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 Kenntniserlangung unverzüglich mit.

## 5.3 Vertraulichkeit der Sicherheitsdokumentation, Weitergabe

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

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

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

[7] ggf. schließt das auch die Aktualisierung der Risikoanalyse nach BSI-Standard 200-3 mit ein
[8] z.B. zu Verfahren, die nicht IT-Grundschutzkonform betrieben werden

# dWebTor Regelungen für den Einsatz privater Endgeräte

## Nutzerpflichten und Vereinbarungen

Version: 1.5

Stand: 01.11.2024

Inhaltsverzeichnis

# 1 Einleitung

Die dWebTor Infrastruktur stellt den Zugang via Internet auf interne Verfahren mittels ALG-Technologie her. Die Verfahren können webbasiert sein, oder als APP Anwendung bereitgestellt werden. Der Zugriff mit privaten Endgeräten ist grundsätzlich im Rahmen der ein-Faktor-Authentifizierung gestattet. Dadurch ergibt sich ein erhöhtes Risiko für die angebundenen Verfahren z.B. durch das mögliche Eindringen von Schadsoftware (Viren, Würmer, Trojaner). Im Folgenden werden die Risiken und Gegenmaßnahmen zur Risikominimierung für den Einsatz von privaten Endgeräten dargestellt.

# 2 Risiken durch den Einsatz privater Endgeräte und Gegenmaßnahmen

Die folgende Tabelle nennt die wesentlichen erhöhten Risiken durch den Einsatz von privaten Endgeräten für den Zugriff über dWebTor auf interne Webapplikationen oder APP Anwendungen. Gegenübergestellt sind die Maßnahmen, die der Risikominimierung dienen.

| Risiken | Maßnahmen |
|---|---|
| Verlust der Vertraulichkeit und Integrität von Anwendungsdaten durch fehlende Integrität (Virenverseuchung etc.) auf dem zugreifenden Client | Sicherheitshinweise für Nutzer und vertragliche Regelung: Nutzer bekommen bei Antrag auf Zugang eine Vereinbarung mit Nutzungshinweisen für dWebTor und verpflichten sich zur Einhaltung der Regeln per Unterschrift. |
| Eindringen von Schadsoftware ins Verfahren (Spähprogramme wie Keylogger, Viren, Würmer etc.) über Sicherheitslücken im Betriebssystem des zugreifenden Clients | Sicherheitshinweise für Nutzer und vertragliche Regelung: Nutzer bekommen bei Antrag auf Zugang eine Vereinbarung mit Nutzungshinweisen für dWebTor und verpflichten sich zur Einhaltung der Regeln per Unterschrift.<br><br>Virenschutz auf den Servern des Verfahrens (Standard im TDC) |
| Eindringen von Schadsoftware über Sicherheitslücken in Anwendungen auf dem Client | Sicherheitshinweise für Nutzer und vertragliche Regelung: Nutzer bekommen bei Antrag auf Zugang eine Vereinbarung mit Nutzungshinweisen für dWebTor und verpflichten sich zur Einhaltung der Regeln per Unterschrift.<br><br>Virenschutz auf den Servern des Verfahrens (Standard im TDC) |
| Einspielen von trojanischen Pferden durch den zugreifenden Client ins Verfahren | Sicherheitshinweise für Nutzer und vertragliche Regelung: Nutzer bekommen bei Antrag auf Zugang eine Vereinbarung mit Nutzungshinweisen für dWebTor und verpflichten sich zur Einhaltung der Regeln per Unterschrift.<br><br>Virenschutz auf den Servern des Verfahrens (Standard im TDC) |

## 3 Nutzerpflichten und -regelungen

Dieses Kapitel führt im Einzelnen auf, welche Hinweise und Regelungen zur Risikominimierung mit den Endnutzern für die Nutzung von dWebTor mit privaten Endgeräten vereinbart werden sollten:

- Auf dem eingesetzten Endgerät ist ein Zugriffsschutz (z.B. Kennwortschutz, biometrische Merkmale) erforderlich.
- Auf den eingesetzten Endgeräten ist ein Virenschutzprogramm zu nutzen.
- Es müssen regelmäßig Updates für das Betriebssystem und die Firewall, das Virenschutzprogramm und den Browser durchgeführt werden.
- Bei Nichtbenutzung oder wenn sich das Endgerät außerhalb des Aufmerksamkeitsbereiches des Nutzers befindet, ist der Zugriff über dWebTor zu beenden.
- Windows und weitere Endgeräte: Für die Dauer des Zugriffs muss auf dem genutzten Endgerät eine aktive sowie aktuelle Firewall und Antivirensoftware eingesetzt werden.
  Eine Festplattenverschlüsselung wird empfohlen.
- Apple-Endgeräte: Das Gerät muss eine aktuelle Betriebssystemversion unterstützen und ist regelmäßig zu aktualisieren. Das Gerät darf keinen Jailbreak haben und es dürfen nur Apps verwendet werden, die über den offiziellen Apple Store bezogen werden. Das Gerät sollte verschlüsselt und zugangsgeschützt sein. Die Anwender sollten es bei Verlust fernlöschen.
- Android-Endgeräte: Auf dem Gerät sollen stets aktuelle Sicherheitsupdates installiert werden. Es darf nicht gerootet sein und es muss ein Virenscanner genutzt werden. Apps dürfen nur über den offiziellen Google Play Store bezogen werden. Das Gerät sollte verschlüsselt und zugangsgeschützt sein und die Anwender sollten es bei Verlust fernlöschen.
- Dienstliche Dateien oder Daten dürfen nicht über die Dauer des Zugriffs hinaus außerhalb des Landesnetzes (also z.B. auf dem Endgerät, in Online-Speichern oder einem USB-Stick) gespeichert werden.
- Daten und Informationen sind so zu schützen, dass Dritte (einschließlich Familienangehörige) diese nicht einsehen und nicht auf sie zugreifen können. Stellen Sie sicher, dass alle Daten und Informationen nicht an Dritte weitergegeben oder ihnen zugänglich gemacht werden.
- Der Nutzer ist verantwortlich für die Einhaltung des Datenschutzes. Wenn Anlass besteht anzunehmen, dass aufgrund der konkreten Einsatzbedingungen eine Gefährdung personenbezogener Daten nicht mit hinreichender Sicherheit auszuschließen ist, muss die Nutzung über dWebTor unterbleiben.
- Während der Dauer des Zugriffs ist die Fernverwaltung bzw. der Fernzugriff auf das Endgerät nicht gestattet.
- Mit Ablauf des berechtigten Anlasses wird der Zugang durch die zuständige Behörde geschlossen.
- Nutzeraktivitäten, die darauf gerichtet sind, die Dienste funktionsuntauglich zu machen oder ihre Nutzung zu verhindern, zu erschweren oder zu verzögern, sind nicht gestattet.

- Es ist weiterhin nicht gestattet, Dateien mit ausführbaren Programmen oder Skripten (z.B. cgi-, perl-, php-Formate) zu installieren, sog. Junk- oder Spam-Mails, Viren, Würmer oder Trojanische Pferde etc. zu verbreiten oder zu installieren, E-Mail-Bombing oder Denial-of-Service-Attacken zu betreiben oder urheberrechtlich geschützte Werke (z.B. Software, mp3-Dateien, Audioformate, Bildformate) unbefugt zu verteilen.
- Besteht der Verdacht auf Kompromittierung des eingesetzten Gerätes, so ist dieses unverzüglich auszuschalten und der Zugriff ist zu beenden.

## 4 Vergabe von Zugriffsrechten

Die Zugriffsrechtevergabe für dWebTor läuft über das jeweilige interne AD der Kunden über bestimmte OU-Gruppen, die für Nutzerstatistiken oder spezielle Richtlinien genutzt werden können. Externe dürfen nur für dWebTor berechtigt werden, wenn die Regelungen für Externe eingehalten werden (siehe dWebTor_Regelung_Externe_AD). Die Berechtigungsvergabe für interne Mitarbeiter obliegt den jeweiligen Kunden. Es dürfen allerdings keine Admin-Konten für den externen Zugriff berechtigt werden und auch die internen Mitarbeiter müssen den unter Kapitel 3 genannten Nutzerpflichten – und Regelungen zustimmen.

Da interne AD-Konten genutzt werden, haben Nutzer von dWebTor über den externen Zugang in dem jeweils freigegebenen Verfahren dieselben Rechte wie intern. Sie können aber nur über explizit freigegebene und freigeschaltete Verfahren zugreifen.

## 5 Fazit

Die Risiken werden durch die empfohlenen Maßnahmen auf ein akzeptables Maß für Verfahren mit dem Schutzbedarf [redacted] reduziert. Verfahren mit dem Schutzbedarf Hoch müssen im Einzelfall prüfen, ob die beschriebenen Maßnahmen für ihre Sicherheitsanforderungen ausreichend sind.

# 6 Glossar

## Definitionen gemäß BSI

**Integrität** bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf "Daten" angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind. In der Informationstechnik wird er in der Regel aber weiter gefasst und auf "Informationen" angewendet. […] Der Verlust der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert, Angaben zum Autor verfälscht oder Zeitangaben zur Erstellung manipuliert wurden.

**Keylogger** bezeichnet Hard- oder Software zum Mitschneiden von Tastatureingaben. Sie zeichnen alle Tastatureingaben auf, um sie möglichst unbemerkt an einen Angreifer zu übermitteln. Dieser kann dann aus diesen Informationen für ihn wichtige Daten, wie z. B. Anmeldeinformationen oder Kreditkartennummern filtern.

**Schadsoftware** auch Malware oder Schadprogramm. Malware ist ein Kunstwort, abgeleitet aus "Malicious software" und bezeichnet Software, die mit dem Ziel entwickelt wurde, unerwünschte und meistens schädliche Funktionen auszuführen. Beispiele sind Computer-Viren, Würmer und Trojanische Pferde. Schadsoftware ist üblicherweise für eine bestimmte Betriebssystemvariante konzipiert und wird daher meist für verbreitete Systeme und Anwendungen geschrieben.

**Trojanisches Pferd** wird ein Programm mit einer verdeckten, nicht dokumentierten Funktion oder Wirkung genannt. Ein Trojanisches Pferd verbreitet sich nicht selbst, sondern wirbt mit der Nützlichkeit des Wirtsprogrammes für seine Installation durch den Benutzer.

**Vertraulichkeit** ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.

**Würmer** sind Schadsoftware, ähnlich einem Virus, die sich selbst reproduzieren und sich durch Ausnutzung der Kommunikationsschnittstellen selbstständig verbreiten.

**Virus** nennt man eine nicht selbständige Programmroutine, die sich selbst reproduziert und dadurch vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornimmt. (Zusätzlich können programmierte Schadensfunktionen des Virus vorhanden sein.)

# dWebTor:
# Behandlung von Externen in internen ADs

## Regelungen für die Nutzung von dWebTor

Version: 1.4

Stand: 22.04.2025

Inhaltsverzeichnis

# 1 Einleitung

Im Zuge der dWebTor-Infrastruktur erfolgt die Authentifizierung der Nutzer grundsätzlich an den internen Acitve Directories (AD) der Länder bzw. an einem von Dataport gemanagten AD. Die Zugangsdaten werden nach Eingabe auf Richtigkeit gegen das Benutzerkonto geprüft.

dWebTor ermöglicht als Zugangsinfrastruktur die Zusammenarbeit in einem Fachverfahren mit Dritten, die bisher kein Benutzerkonto im AD hatten, da diese nicht zu den Mitarbeiterinnen und Mitarbeitern des Auftraggebers zählen. Für diese sogenannten Externen werden daher Konten in internen ADs benötigt. Diese Konten werden mit dem Kontentyp dWebTor bzw. Zuvex angelegt.

Für die Anlage von Konten für Externe gelten die im Folgenden beschriebenen Regelungen. Die Regelungen dienen dazu, das Risiko zu reduzieren, Unbefugten Zugriff über das landesinterne AD zu geben, Dopplungen zu vermeiden und nicht mehr notwendige Konten zügig aus dem AD zu löschen.

Sofern ein Verfahren eine andere Benutzerverwaltung nutzt, ist die Einhaltung dieser Vorgaben durch das Verfahren bzw. die Benutzerverwaltung sicherzustellen.

Die im Folgenden beschriebenen Regelungen beziehen sich ausschließlich auf die Voraussetzungen für die Kontenanlage und Kontenpflege.

# 2 Mindestanforderungen für die Einrichtung eines internen Kontos für Externe

Dies sind Mindestanforderungen an Externe, damit sie ein internes Konto für die Nutzung von dWebTor bekommen können.

Externe…

- …dürfen noch kein Konto im jeweiligen Trägerland AD besitzen (sofern die Kontenführung im jeweiligen Trägerland AD erfolgt).
- …müssen ein berechtigtes dienstliches Interesse des jeweiligen Trägerlandes mittels des internen Kontos erfüllen.
- ...müssen über einen gewissen Zeitraum dieses dienstliche Interesse wahrnehmen.
- …müssen im jeweiligen Trägerland mit Name und Kontaktdaten bekannt (und dokumentiert) sein.
- … müssen in geeigneter Form zur Einhaltung der Nutzungsbedingungen verpflichtet sein.
- …müssen einen Ansprechpartner in einer Behörde (o.Ä.) im Trägerland besitzen.

Verschärfte Bedingungen gelten für Externe, die über ihren Zugang administrative Aufgaben erfüllen sollen (derzeit über dWebTor nicht vorgesehen):

- Sie müssen zusätzlich eine Sicherheitsprüfung durchlaufen.
- Sie müssen eine Form der Multifaktor-Authentisierung nutzen.

## 3 Löschung von Konten Externer in internen ADs

Sobald die dargestellten Mindestanforderungen durch den Externen nicht mehr erfüllt werden, z.B. die zu erbringende dienstliche Aufgabe vorbei ist, muss das interne Konto wieder gelöscht werden. Verantwortlich sind dafür die jeweiligen IT-Stellen, die das Konto eingerichtet und betreut haben.

Dataport empfiehlt, dass externe Konten nach Ablauf einer festzulegenden Zeitspanne automatisch gesperrt und nach Ablauf einer weiteren Frist automatisch gelöscht werden.

Dazu kann ein Skript genutzt werden, dass ungenutzte Konten von externen Nutzern nach einer Frist deaktiviert und nach Verstreichen einer weiteren Frist automatisch löscht.

Empfohlen werden maximale Fristen von 6 Monaten für die Deaktivierung und weiteren drei Monate für die Löschung des Kontos.

Die jeweils verantwortliche IT wird über die Deaktivierung und Löschung der Konten via Email informiert und kann ggf. aktiv eingreifen, wenn das jeweilige Konto doch noch benötigt werden sollte. Die Zeit, nachdem ein Konto deaktiviert oder gelöscht wird, kann durch die Kunden bestimmt werden, sollte jedoch der obigen Empfehlung vom Sicherheitsmanagement entsprechen.

## 4 Fazit

Die hier dargestellten Regelungen für die Einrichtung von internen Konten für Externe sind im Rahmen der Nutzung von dWebTor einzuhalten. Für Abweichungen von diesen Empfehlungen und damit verbundene Risiken ist der jeweilige Kunde bzw. das jeweilige Verfahren verantwortlich.

**EVB-IT Dienstvertrag Vxxxxx/xxxxxxx**

**Leistungsnachweis Dienstleistung (Seite 1 von 2)**

dataport

# 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.

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

**EVB-IT Dienstvertrag Vxxxxx/xxxxxxx**

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

dataport

| 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.**