Vertrag über die Beschaffung von IT-Dienstleistungen

Zwischen

Finanzbehörde
Große Bleichen 27
20354 Hamburg

– im Folgenden „Auftraggeber" genannt –

und

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

– im Folgenden „Auftragnehmer" genannt –

wird folgender Vertrag geschlossen:

1 Vertragsgegenstand und Vergütung

1.1 Projekt-/Vertragsbezeichnung

Hamburger Transparenzgesetz - Entwicklung und Betrieb Such- und Suchvorbereitungssystem

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

1.3 Die Leistungen des Auftragnehmers werden

☒ nach Aufwand gemäß Nummer 5.1

☒ zum jährlichen Festpreis gemäß Nummer 5.2 in Höhe von
316.906,02 € (bei gewählter Variante 1) oder
338.377,28 € (bei gewählter Variante 2)

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

2 Vertragsbestandteile

2.1 Es gelten nacheinander als Vertragsbestandteile:

- dieser Vertrag (Seiten 1 bis 8) mit Anlagen Nr. 1, 2, 3, 4A, 4B, 5A und 5B
- Allgemeine Vertragsbedingungen von Dataport in der bei Vertragsschluss geltenden Fassung (s. 11.1)
- Dataport Datenschutz-Leitlinie über technische und organisatorische Maßnahmen bei der Datenverarbeitung im Auftrag (s. 11.1)
- Ergänzende Vertragsbedingungen für die Erbringung von IT-Dienstleistungen (EVB-IT Dienstleistung) in der bei Vertragsschluss geltenden Fassung
- Vergabe- und Vertragsordnung für Leistungen – ausgenommen Bauleistungen – Teil B (VOL/B) in der bei Vertragsschluss geltenden Fassung

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

3 Art und Umfang der Dienstleistungen

3.1 Art der Dienstleistungen

Der Auftragnehmer erbringt für den Auftraggeber folgende Dienstleistungen:

3.1.1 ☐ Beratung
3.1.2 ☐ Projektleitungsunterstützung
3.1.3 ☐ Schulung
3.1.4 ☐ Einführungsunterstützung
3.1.5 ☐ Betreiberleistungen
3.1.6 ☐ Benutzerunterstützungsleistungen
3.1.7 ☐ Providerleistungen ohne Inhaltsverantwortlichkeit
3.1.8 ☒ sonstige Dienstleistungen: gemäß Anlagen **1, 2, 3, 4A, 4B, 5A, und 5B**

3.2 Umfang der Dienstleistungen des Auftragnehmers

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

☒ folgenden den Vertragsparteien vorliegenden Dokumenten

	Version	vom
HmbTG-IT-System Beschreibung der Anforderungen	1.0	21.08.2013
HmbTG-IT-System Lösungsarchitektur	1.0	26.09.2013

Diese Dokumente befinden sich in der stetigen Fortschreibung.

☒ der Leistungsbeschreibung des Auftragnehmers

Hamburger Transparenzgesetz - Entwicklung und Betrieb Such- und Suchvorbereitungssystem - Testleistungen	Anlage(n) Nr.	2
Hamburger Transparenzgesetz - Entwicklung und Betrieb Such- und Suchvorbereitungssystem - Entwicklung/Betrieb des CKAN		3
RZ-SLA Allgemeiner Teil (Teil A)		4A
RZ-SLA Verfahrensspezifischer Teil (Teil B) für Variante 1		4B Variante 1
RZ-SLA Verfahrensspezifischer Teil (Teil B) für Variante 2		4B Variante 2
TVM SLA Allgemeiner Teil (Teil A)		5A
TVM SLA Verfahrensspezifischer Teil (Teil B)		5B

☒ folgenden weiteren Dokumenten:

	Anlage(n) Nr.
Entgeltübersicht	1
Übersicht Arbeitspakete	Anhang A zur Anlage 2

Es gelten die Dokumente in

☐ obiger Reihenfolge

☒ folgender Reihenfolge: 1, 2, Anhang A zur Anlage 2, 3, 4B, 4A, 5B und 5A

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

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

3.3 Vergütungsbestimmende Faktoren aus dem Bereich des Auftraggebers

Vergütungsbestimmende Faktoren aus dem Bereich des Auftraggebers sind

a) die Mitwirkungsleistungen des Auftraggebers gemäß Nummer 8

b) folgende weitere Faktoren:

4 Ort der Dienstleistungen / Leistungszeitraum

4.1 Ort der Dienstleistungen in den Räumlichkeiten des Auftragnehmers

4.2 Zeiträume der Dienstleistungen

Leistungen (gemäß Nummer 3.1)	**Geplanter Leistungszeitraum**		**Verbindlicher Leistungszeitraum**	
	Beginn	**Ende**	**Beginn**	**Ende**
gem. Anlage 2, gem. Anlage 3, 4A, 4B, 5A, 5B			01.10.2013, im Übrigen nach Projektfortschritt	31.12.2014 bezogen auf Anlage 2, im Übrigen nach Projektfortschritt

4.3 Zeiten der Dienstleistungen

Die Leistungen des Auftragnehmers werden erbracht gemäß Anlage SLA RZ Teil A Pkt.4.3, SLA RZ Teil B Pkt.4.1 sowie

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

Montag bis Donnerstag von 08:00 bis 17:00 Uhr

Freitag bis _____ von 08:00 bis 15:00 Uhr

4.3.2 während sonstiger Zeiten

_____ bis _____ von _____ bis _____ Uhr

_____ bis _____ von _____ bis _____ Uhr

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

5 **Vergütung** gem. Leistungsnachweis Dienstleistung

5.1 ☒ **Vergütung nach Aufwand gem. Anlage 1, Anlage 2 und Anhang A zur Anlage 2**

☐ ohne Obergrenze

☒ mit Obergrenze in Höhe von 272.504,00 € für die Pos. 01 bis 07,
- gem. Anlage 1 Entgeltübersicht
- gem. Anlage 2 (Leistungsbeschreibung Testleistungen) Pkt. 3 und Anhang

Bezeichnung des Personals/der Leistung (Leistungskategorie)					Preis innerhalb der Zeiten gemäß 4.3.	
Pos. Nr.	**SAP-Artikel-Nr.**	**Artikelbezeichnung/-code**	**Menge**	**Mengeneinheit**	**Einzelpreis**	**geschätzter Gesamtpreis**
01	21010345	Entwicklungsunterstützung [redacted] Personenmonate geschätzt); jede weitere Std.	[redacted]	Std.	[redacted] €	**91.200,00 €**
02	21010345	Test Online-Portal (geschätzt [redacted] Std.), Testdurchführung, jede weitere Std.	[redacted]	Std.	[redacted] €	**6.992,00 €**
03	21010347	Test Online-Portal (geschätzt [redacted] Std.), Testkonzept, jede weitere Std.	[redacted]	Std.	[redacted] €	**11.592,00 €**
04	21010345	Test [redacted] Harvester (geschätzt [redacted] Std.), Testdurchführung, jede weitere Std.	[redacted]	Std.	[redacted] €	**27.360,00 €**
05	21010347	Test [redacted] Harvester (geschätzt [redacted] Std.), Testkonzept, jede weitere Std.	[redacted]	Std.	[redacted] €	**45.360,00 €**
06	21010345	Technisches Sollkonzept (geschätzt [redacted] Std.), jede weitere Std.	[redacted]	Std.	[redacted] €	**19.000,00 €**
07	21000139	TVM-Konzepte und Erstimplementationen	[redacted]	Stück	71[redacted] €	**71.000,00 €**
		Bei Überschreitung von [redacted] Harvester-Tests gilt für jeden weiteren Test (inkl. automatischer Zulieferung):	[redacted]		[redacted]	
08	21010345	Test je Liefersystem; Testdurchführung (geschätzt: [redacted] Std.)	[redacted]	Std.	[redacted] €	**1.368,00 €**
09	21010347	Test je Liefersystem; Testkonzept (geschätzt: [redacted] Std.)	[redacted]	Std.	[redacted] €	**2.268,00 €**
10	20001061	DP-MSS-STO/SANH, in den Leistungen unter 5.2 sind in Summe [redacted] GB enthalten, jedes weitere kostet:	[redacted]	GB/jährl.	[redacted] €	
11	20001062	DP-MSS-STO/SANM, in den Leistungen unter 5.2 sind in Summe [redacted] GB enthalten, jedes weitere kostet:	[redacted]	GB/jährl.	[redacted] €	

12	20001064	DP-MSS-BACK/30, in den Leistungen unter 5.2 sind in Summe [redacted] GB enthalten, jedes weitere kostet:	1	GB/jährl.	[redacted] €	

Die Abrechnung erfolgt nach Aufwand.

Reisezeiten

☒ Reisezeiten werden nicht gesondert vergütet

☐ Reisezeiten werden vergütet gemäß **Anfahrtspauschale SAP-Nr. 21010791. Die Anfahrtspauschale beträgt derzeit [redacted] pro Person/Kundenbesuch.**

Rechnungsstellung

Die Rechnungsstellung erfolgt ☒ kalendermonatlich nachträglich gem. Leistungsnachweis

Vergütungsvorbehalt

Es wird ein Vergütungsvorbehalt vereinbart

☐ gemäß Ziffer 6.4 EVB-IT Dienstleistung

☐ anderweitige Regelung gemäß Anlage Nr. _____ .

5.2 ☒ **Festpreis**

Für die vom Auftragnehmer zu erbringenden Dienstleistungen gem. Anlagen 4A und 4B zahlt der Auftraggeber bei gewählter (bitte ankreuzen) **Variante 1** einen **jährlichen Festpreis** in Höhe von **insgesamt 316.906,02 €** oder bei gewählter **Variante 2** einen **jährlichen Festpreis** in Höhe von **insgesamt 338.377,28 €.**

☒ **Variante 1: Betrieb CKAN ohne IPS**

Der **jährliche Festpreis** setzt sich wie folgt zusammen:

Rechenzentrumsleistungen gemäß RZ Servicekatalog

Pos.	SAP-Artikel-Nr.	Artikelbezeichnung/-code	Menge	Mengeneinheit	Einzelpreis	Gesamtpreis
01	20000978	DP-MSS-APPS/AM/S/SLES	[redacted]	Service	[redacted] €	11.930,92 €
02	20000979	DP-MSS-APPS/AL/S/SLES		Service	€	7.588,34 €
03	20001008	DP-MSS-WEB/AM/S/Apache		Service	€	5.965,46 €
04	20001009	DP-MSS-WEB/AL/S/Apache		Service	€	7.588,34 €
05	20001039	DP-MSS-DB/AL/S/Oracle		Service	€	17.174,96 €
06	20001042	DP-MSS-DB/DXL/S/Oracle		Service	€	17.708,60 €
07	20001061	DP-MSS-STO/SANH		GB	€	17.362,80 €
08	20001062	DP-MSS-STO/SANM		GB	€	13.826,40 €
09	20001064	DP-MSS-BACK/30		GB	€	14.200,20 €
10	20001071	DP-MSS-TVM/Individuell		Paket	€	115.000,00 €
11	21010346	Upgrade Ubuntu		Stück	€	88.560,00 €

☐ **Variante 2: Betrieb CKAN mit IPS**

Der **jährliche Festpreis** setzt sich wie folgt zusammen:

Rechenzentrumsleistungen gemäß RZ Servicekatalog

Pos.	SAP-Artikel-Nr.	Artikelbezeichnung/-code	Menge	Mengeneinheit	Einzelpreis	Gesamtpreis
01	20000978	DP-MSS-APPS/AM/S/SLES	[redacted]	Service	[redacted] €	23.861,84 €
02	20000979	DP-MSS-APPS/AL/S/SLES		Service	€	15.176,68 €
03	20001008	DP-MSS-WEB/AM/S/Apache		Service	€	5.965,46 €
04	20001009	DP-MSS-WEB/AL/S/Apache		Service	€	7.588,34 €
05	20001039	DP-MSS-DB/AL/S/Oracle		Service	€	17.174,96 €
06	20001042	DP-MSS-DB/DXL/S/Oracle		Service	€	17.708,60 €
07	20001061	DP-MSS-STO/SANH		GB	€	17.362,80 €
08	20001062	DP-MSS-STO/SANM		GB	€	13.826,40 €
09	20001064	DP-MSS-BACK/30		GB	€	14.200,20 €
10	20001071	DP-MSS-TVM/Individuell		Paket	€	115.000,00 €
11	21010346	Upgrade Ubuntu		Stück	€	90.512,00 €

Die unterschiedlichen Werte für die Position 11 in Variante 1 und 2 ergeben sich aus unterschiedlichen Serveranzahlen bei den jeweiligen Positionen 1 und 2.

Die Rechnungsstellung des jährlichen Festpreises erfolgt kalendermonatlich nachträglich und anteilig nach Inbetriebnahme der einzeln benannten Positionen.

5.3 Reisekosten und Nebenkosten

☒ Reisekosten werden nicht gesondert vergütet

☐ Reisekosten werden vergütet gemäß **Anfahrtspauschale SAP-Nr. 21010791.**
Die Anfahrtspauschale beträgt derzeit [redacted] pro Person/Kundenbesuch.

☒ Nebenkosten werden nicht gesondert vergütet

☐ Nebenkosten werden vergütet gemäß **Anfahrtspauschale SAP-Nr. 21010791.**
Die Anfahrtspauschale beträgt derzeit [redacted] pro Person/Kundenbesuch.

6 Rechte an den verkörperten Dienstleistungsergebnissen

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

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

_____

_____

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

_____

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

6.4 ☐ Sonstige Nutzungsrechtsvereinbarungen

_____

7 Verantwortlicher Ansprechpartner

des Auftraggebers: [redacted]

des Auftragnehmers: [redacted]

8 Mitwirkungsleistungen des Auftraggebers

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

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

8.2. gem. Anlage SLA RZ Teil A Pkt. 2.3, SLA RZ Teil B Pkt. 2.1 und Anlage 2 Pkt. 3

9 Schlichtungsverfahren

☐ Die Anrufung folgender Schlichtungsstelle wird vereinbart:

10 Versicherung

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

11 Sonstige Vereinbarungen

11.1. Die Allgemeinen Vertragsbedingungen und die Dataport Datenschutz-Leitlinie sind im Internet unter www.dataport.de veröffentlicht.

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

11.3. Werden die gem. Nr. 5.1 vereinbarten Obergrenzen erreicht, werden sich die Vertragspartner unverzüglich zum weiteren Vorgehen abstimmen und entsprechende Vereinbarungen zur Fortführung der relevanten Leistungen im Rahmen eines EVB-IT Änderungsverfahren treffen.

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

11.5. Dieser Vertrag beginnt am 01.10.2013 und gilt gemäß Absprache zwischen Auftragnehmer und Auftraggeber bis 31.12.2014. Zum 01.01.2015 erfolgt die Übergabe des Gesamtsystems an die zuständige Fachbehörde.

11.6. Der Aufwand für den Betrieb von Ubuntu im Rechenzentrum wird jährlich evaluiert. Ist eine Anpassung der gem. Nr. 5.2 vereinbarten Leistungen und Entgelte erforderlich, werden sich die Vertragspartner unverzüglich zum weiteren Vorgehen abstimmen und entsprechende Vereinbarungen zur Fortführung der relevanten Leistungen im Rahmen eines EVB-IT Änderungsverfahren treffen.

Hamburg, 18.11.2013 Hamburg, 21.11.2013

[redacted]

Anlage 1 zum EVB-IT Dienstvertrag V7272/2900000

Entgeltübersicht

Hamburger Transparenzgesetz
Such- und Suchvorbereitungssystem
(Entwicklung, Testmanagement und Betrieb)

Inhaltsverzeichnis

1 Einmalige Entgelte 3
1.1 Entwicklungsunterstützung 3
1.2 Testmanagement 3
1.3 Betrieb 3

1 Einmalige Entgelte

Bei den nachfolgenden Berechnungen handelt es sich um eine Darstellung nach **Aufwand**.

1.1 Entwicklungsunterstützung[1]

Pos.	SAP-Artikel-Nr.	PM[2]	Std.	Std.-Satz	Summe
01	21010345	[redacted]	[redacted]	[redacted] €	91.200,00 €
				Summe	**91.200,00 €**

1.2 Testmanagement

Pos.	SAP-Artikel-Nr.	Std.	Std.-Satz	Summe
	Test Online-Portal	[redacted]		
02	21010345	[redacted]	[redacted] €	6.992,00 €
03	21010347	[redacted]	[redacted] €	11.592,00 €
			Zwischensumme	***18.584,00 €***
	Test von [redacted] Harvestern (je [redacted] Std)	[redacted]		
04	21010345	[redacted]	[redacted] €	27.360,00 €
05	21010347	[redacted]	[redacted] €	45.360,00 €
			Zwischensumme	***72.720,00 €***
			Summe	**91.304,00 €**

Jedes weitere Liefersystem wird zu folgenden Konditionen getestet:

Test von 1 Liefersystem (inkl. automatischer Zulieferung)

Pos.	SAP-Artikel-Nr.	Std.	Std.-Satz	Summe
		[redacted]		
06	21010345	[redacted]	[redacted] €	1.368,00 €
07	21010347	[redacted]	[redacted] €	2.268,00 €
			Summe	**3.636,00 €**

1.3 Betrieb

Pos.	SAP-Artikel-Nr.	Std.	Std.-Satz	Summe
	Technisches Sollkonzept			
08	21010345	[redacted]	[redacted] €	19.000,00 €
			Zwischensumme	***19.000,00 €***

Pos.	SAP-Artikel-Nr.	Stk.	Einzelpreis	Summe
	TVM-Konzepte u. Erstimplementationen			
09	21000139	[redacted]	[redacted] €	71.000,00 €
			Zwischensumme	***71.000,00 €***
			Summe	**90.000,00 €**

[1] Es wird eine Realisierung von [redacted] Harvestern geschätzt [redacted] PT für die ersten [redacted] Harvester und [redacted] PT für jeden weiteren Harvester).
[2] PM (Personenmonate)

Hamburger Transparenzgesetz - Entwicklung und Betrieb Such- und Suchvorbereitungssystem

Leistungsbeschreibung -Testleistungen

Stand: 20.09.2013

Inhaltsverzeichnis

Leistungsbeschreibung

1 Leistungsgegenstand 1
2 Leistungszeitraum 1
3 Entgelt 1

Leistungsbeschreibung

1 Leistungsgegenstand

Der Auftrag umfasst den Test der Komponenten, die für Entwicklung und Betrieb des Such- und Suchvorbereitungssystems (CKAN und IPS – inkl. Harvester) benötigt werden.

2 Leistungszeitraum

Die Leistungserbringung erfolgt in folgendem Leistungszeitraum: Oktober 2013 bis einschließlich September 2014.

Nach Beauftragung wird vom Auftragnehmer ein Zeitplan erstellt. Der Zeitplan wird dem Auftraggeber vor der Leistungserbringung zur Abstimmung schriftlich mitgeteilt.

Nach Freigabe des Zeitplans ist eine Verlängerung, Verkürzung oder Verschiebung des Leistungszeitraums rechtzeitig bekanntzugeben und unter beiderseitigem Einverständnis schriftlich festzuhalten.

3 Entgelt

Die beschriebenen Leistungen können mit einem geschätzten Arbeitsaufwand von [redacted] Stunden (Obergrenze) erbracht werden. Zusätzlich fällt pro entwickeltem Harvester ein Arbeitsaufwand von [redacted] Stunden (Obergrenze) an.

Der Stundensatz für die Leistungen beträgt [redacted] €, sofern die Aufwände im Bereich Testmanagement oder Testanalyse anfallen und [redacted] € bei Aufwänden, die im Bereich Testdurchführung erbracht werden. Erfahrungsgemäß entfallen [redacted] der erbrachten Leistungen auf Testmanagement und Testanalyse und [redacted] auf die Testdurchführung.

Übersicht Arbeitspakete

Arbeitspaket	geschätzter Aufwand
1. Test Online-Portal	[redacted] Std

Beschreibung:

Das Arbeitspaket umfasst den funktionalen Test des Online-Portals:

- Korrekte Anzeige von generierten Webseiten
- Suchfunktion

Es wird davon ausgegangen, dass Testeingangsdaten zur Verfügung stehen und nicht selbst erstellt werden müssen.

Inhalt:

- Erstellung einer Risikoanalyse
- Erstellung eines Testkonzeptes
- Durchführung einer Testanalyse sowie daraus abgeleitet die Erstellung von Testfallbeschreibungen
- Durchführung des Testes anhand der zuvor ausgearbeiteten Beschreibungen
- Exploratives Testen

Arbeitspaket	geschätzter Aufwand
2. Test Harvester	[redacted] Std

Das Arbeitspaket umfasst den funktionalen Test eines Harvesters zur Anbindung weiterer Systeme (z.B. Fachverfahren). Der Test beschränkt sich dabei darauf, zu überprüfen, ob die Ein- und Ausgabe des Harvesters korrekt funktioniert und die betroffenen Daten danach in der Suche auffindbar sind (im Index enthalten).

Inhalt:

- Anteilig Erstellung einer Risikoanalyse (zur Priorisierung des Tests)
- Durchführung einer Testanalyse sowie daraus abgeleitet die Erstellung von Testfallbeschreibungen
- Durchführung des Testes anhand der zuvor ausgearbeiteten Beschreibungen

Hamburger Transparenzgesetz - Entwicklung und Betrieb Such- und Suchvorbereitungssystem

Leistungsbeschreibung für die Entwicklung/Betrieb des CKAN

Stand: 19.11.2013

Inhaltsverzeichnis

Leistungsbeschreibung

1 Leistungsgegenstand 1

Leistungsbeschreibung

1 Leistungsgegenstand

Übernahme der durch HITeC entwickelten Harverster sowie Pflege und Entwicklung von Harvestern. Weitere Dienstleistungen im Kontext der ckan Entwicklung gem. Abstimmung und Beauftragung durch den Auftraggeber.

Das Dokument wird entsprechend des Projektfortschritts fortgeschrieben und in der aktuellen Fassung dem Auftraggeber bereitgestellt.

dataport

Service Level Agreement

Bereitstellung der Infrastruktur und Betrieb *des Verfahrens CKAN (Hamburgisches Transparenzgesetz)* im Rechenzentrum

Allgemeiner Teil (Teil A)

für

Finanzbehörde

Große Bleichen 27

20354 Hamburg

nachfolgend Auftraggeber

Version: 2.1
Stand: 14.06.2013

Inhaltsverzeichnis

1 Einleitung ... 4

1.1 Aufbau des Dokumentes ... 4

1.2 Leistungsgegenstand ... 4

2 Rahmenbedingungen ... 5

2.1 Beschreibung des Fachverfahrens ... 5

2.2 Changemanagement ... 5

2.2.1 Changes mit vorab gegebener Zustimmung ... 5

2.2.2 Changes mit Zustimmung des Auftraggebers ... 6

2.2.3 Freigabe ... 6

2.3 Mitwirkungsrechte und –pflichten ... 6

2.4 Kündigungsmodalitäten ... 7

3 Leistungsbeschreibung ... 8

3.1 Infrastruktur ... 8

3.1.1 Rechenzentrum ... 8

3.1.2 Netzwerk-Anbindung und Firewall ... 9

3.1.3 Serverbasierte Leistungen Windows und Unix ... 9

3.1.4 Technisches Design ... 10

3.2 Bereitstellung ... 10

3.2.1 Systeme im Rechenzentrum ... 10

3.2.2 Systeme in den Räumlichkeiten des Auftraggebers ... 10

3.3 Betrieb und Administration ... 11

3.3.1 Basisbetrieb ... 11

3.3.2 Backup & Recovery ... 11

3.3.3 User – Administration ... 11

3.3.4 Datenbank und Middleware Administration ... 12

3.3.5 Applikations-Betrieb und Administration ... 12

3.3.6 Batch-Betrieb ... 13

3.3.7 Erneuerung und Ergänzung ... 13

3.3.8 Wartung und Pflege ... 13

3.3.9 Fernzugriff und Fernwartung, Fernunterstützung und Fernbedienung ... 14

3.3.10 Kommunikationsanbindung zum RZ ... 15

4 Leistungskennzahlen ... 16

4.1 Definition ... 16

4.1.1 Begriffsfestlegungen 16
4.2 Leistungsausprägung 16
4.3 Vereinbarte Leistungskennzahlen 17
4.4 Reporting 18
5 Erläuterungen 19
5.1 Erläuterung VDBI 19

1 Einleitung

Der Auftragnehmer stellt dem Auftraggeber IT Ressourcen einschließlich Hardware und systemnaher Software sowie IT Dienstleistungen mit dem vereinbarten Leistungsumfang bedarfsgerecht zur Verfügung (im Folgenden als Verfahren bezeichnet). Mit dieser Leistungsvereinbarung (Service Level Agreement, SLA) wird der Leistungsgegenstand geregelt. Darüber hinaus beschreibt das Dokument die Systemumgebung, die Aufgaben und Zuständigkeiten vom Auftragnehmer und vom Auftraggeber, sowie die vereinbarten Leistungskennzahlen (Service Levels).

1.1 Aufbau des Dokumentes

Diese Anlage enthält die folgenden Kapitel:

Rahmenbedingungen (Kapitel 2): Regelung von allgemeinen Rechten und Pflichten von Auftraggeber und Dienstleister, Bestimmungen zur Laufzeit, Änderung bzw. Kündigung der Vereinbarung sowie Übergangsbestimmungen.

Leistungsbeschreibungen (Kapitel 3): Inhaltliche Beschreibung der bereitgestellten Rechenzentrumsleistungen sowie der für einen reibungslosen Betrieb erforderlichen Dienstleistungen. Bestandteil der Leistungsbeschreibungen ist die in diesem Dokument beschriebene Verteilung von Aufgaben und Zuständigkeiten zwischen Auftraggeber und Dienstleister (VDBI – Erläuterungen s. Pkt. 5.1).

Leistungskennzahlen (Kapitel 4): Definition von Leistungskennzahlen und ihrer Messverfahren (z. B. Verfügbarkeit oder Reaktionszeiten), Festlegung von Betriebs- und Servicezeiten und Vereinbarungen über die zu erreichende Leistungsqualität (Service Level Objectives).

Erläuterungen (Kapitel 5)

1.2 Leistungsgegenstand

Gegenstand dieses Service Level Agreements ist die Bereitstellung der Dienstleistungen im Rechenzentrum.

Die allgemeinen Leistungen werden hinsichtlich der Leistungsqualität und des Leistungsumfangs im Kapitel 3 beschrieben. Die verfahrensspezifischen Leistungen werden im Teil B beschrieben.

2 Rahmenbedingungen

2.1 Beschreibung des Fachverfahrens

Die Beschreibung des Fachverfahrens und der zu Grunde liegenden Lösung erfolgt im Teil B.

2.2 Changemanagement

Das Changemanagement erfolgt in einem geregelten Prozess. Es ist die Aufgabe des Changemanagements sicherzustellen, dass standardisierte Vorgehensweisen zur Durchführung von Veränderungen existieren und effizient genutzt werden.

Der Auftragnehmer erbringt folgende Leistungen im Rahmen des Changemanagements für den Rechenzentrumsbetrieb.

2.2.1 Changes mit vorab gegebener Zustimmung

Der Auftraggeber stimmt mit Abschluss dieses Vertrages allen Änderungen an der Hardware, am Betriebssystem oder in den systemnahen Diensten, die die Integrität oder Verfügbarkeit des Verfahrens- oder des Services nicht berühren zu.

Aufgaben und Zuständigkeiten	Auftrag-nehmer	Auftrag-geber
Prüfung des Änderungsbedarfs	**V, D**	**I, B**
Durchführung in einer Testumgebung einschließlich der Dokumentation, wenn im Leistungsumfang enthalten.	**V, D**	**I, B**
Umsetzung der in der Testumgebung getesteten Änderungen in der Produktionsumgebung im vertraglich festgelegten Wartungsfenster und Ergänzung der Systemdokumentation	**V, D**	**I, B**
Anpassung der Verfahrensdokumentation, soweit dies durch eine Änderung erforderlich wird	**V, D**	**I, B**

2.2.2 Changes mit Zustimmung des Auftraggebers

Der Auftragnehmer holt für alle Änderungen, die die Integrität oder Verfügbarkeit des Verfahrens- oder des Services berühren die jeweilige Zustimmung des Auftraggebers ein. Dies gilt auch für Änderungen an den Verfahren und Services selbst.

Aufgaben und Zuständigkeiten	Auftrag-nehmer	Auftrag-geber
Ermittlung des Änderungsbedarfs durch den Auftragnehmer oder Beauftragung durch den Auftraggeber.	**V, D**	**V, D**
Bei Ermittlung des Änderungsbedarfs durch den Auftragnehmer wird dem Auftraggeber oder seinen Beauftragten ein Änderungsantrag schriftlich oder per E-Mail zur Zustimmung übermittelt.	**V, D**	**I, B**
Durchführung von genehmigten Änderungen in einer Testumgebung (sofern beauftragt) einschließlich der Dokumentation des Auftraggebers unter Berücksichtigung der in Beauftragung enthaltenen Dringlichkeitsangabe.	**V, D**	**I, B**
Mitteilung der Testergebnisse (Testdokumentation und Stellungnahme) an den Auftraggeber oder seinen Beauftragten.	**V, D**	**I, B**
Der Auftraggeber führt den Test in der Testumgebung (sofern beauftragt) durch und beauftragt die Umsetzung der Änderungen in der Produktionsumgebung schriftlich oder per E-Mail.	**I, B**	**V, D**
Abstimmung des Umsetzungszeitpunktes und ggf. notwendigen Wartungsfensters mit dem Auftraggeber oder seinen Beauftragten.	**V, D**	**I, B**
Durchführung der Änderungen in der Produktionsumgebung und Ergänzung der Systemdokumentation.	**V, D**	**I, B**
Der Auftraggeber führt Tests in der Produktionsumgebung durch und erklärt die Freigabe der Änderungen in der Produktionsumgebung schriftlich in Papierform oder in Textform (Fax, E-Mail, etc.).	**I, B**	**V, D**
Anpassung der Verfahrensdokumentation, soweit dies durch eine Änderung erforderlich wird.	**V, D**	**I, B**

2.2.3 Freigabe

Mit der Freigabe des bezeichneten Freigabegegenstandes wird vereinbart, dass das System in der existierenden Form genutzt werden soll. Für Test und Freigabe von Verfahren ist der Auftraggeber verantwortlich. Automatisierte Verfahren, die der Auftragnehmer in eigener Verantwortung betreibt, werden vor ihrem erstmaligen Einsatz oder nach Änderungen getestet und freigegeben.

Die Freigabe von Test-, Schulungs- oder Produktivsystemen kann sowohl in Papier- als auch in Textform (Fax, E-Mail, etc.) erfolgen. Im Falle von umfangreicheren Systemen kann ein Freigabeprotokoll neben dem reinen Einverständnis zudem z.B. folgende Parameter festhalten:

- Konfigurationsstände
- Zusammenstellung und Bezeichnung der Datenbanken
- Benutzerhandbücher, technische Dokumentation

2.3 Mitwirkungsrechte und –pflichten

Die vom Auftragnehmer zugesagten Leistungen erfolgen auf Anforderung des Auftraggebers. Es sind Mitwirkungs- und Bereitstellungsleistungen des Auftraggebers erforderlich, die grundsätzlich in einer besonderen Anlage geregelt sind.

2.4 Kündigungsmodalitäten

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

Dazu gehören unter anderem:

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

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

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

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

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

3 Leistungsbeschreibung

Für den Betrieb des Verfahrens werden die im Teil B beschriebenen IT-Services durch den Auftragnehmer erbracht. Dies beinhaltet die anteilige Nutzung der erforderlichen Systemkonfiguration (Host, Server, Betriebssystem, betriebssystemnahe Software, Platten etc.) und alle notwendigen Services zur Sicherstellung eines reibungslosen Betriebs.

3.1 Infrastruktur

Die Leistung des Auftragnehmers erfolgt ausschließlich auf unterstützten Plattformen, die durch Hersteller freigegebenen sind. Daraus ergibt sich regelmäßig eine Veränderung der Infrastruktur / Plattform. Um den laufenden Betrieb zu sichern, werden diese Veränderungen für den zentralen Teil nach Maßgabe des Auftragnehmers realisiert. Dies wird im Rahmen der Regelkündigungsfristen angekündigt. Der Auftraggeber ist verpflichtet, die in seinem Auftrag gehostenen Verfahren und Komponenten rechtzeitig an diese veränderten Anforderungen anzupassen.

3.1.1 Rechenzentrum

Der Auftragnehmer stellt für den Betrieb der Rechnersysteme, die Bestandteil dieses Vertrages sind, entsprechende Fläche und Infrastruktur in den Standorten des Rechenzentrums (RZ) zur Verfügung. Die RZ Infrastruktur weist folgende Charakteristika auf:

1. Aufstellung im Rechenzentrum des Auftragnehmers
2. Betrieb in gesicherter Rechenzentrumsumgebung mit Zutrittschutz und Zugangsschutz
3. Brandschutzmaßnahmen (für die Systemräume Feuerschutz- Isolierung, Brandmeldezentrale, Durchschaltung zur Feuerwehr, Löschvorrichtungen)
4. Zutrittskontrolle und Überwachung in allen Gebäudebereichen, Personenvereinzelungsanlage im Rechenzentrum, Einbruchmeldeanlage, Wachdienst (7x24) vor Ort
5. Redundante unterbrechungsfreie Stromversorgung, Notstrom und Klimatisierung
6. Bereitstellung der Server
7. Installation und Konfiguration der System-Software
8. Bereitstellung, Betrieb und Wartung der erforderlichen Server
9. Tägliche Datensicherung
10. Sachgerechte Lagerung der gesicherten Daten (Datensicherung, Diebstahl- u. Brandschutz)
11. Rücksichern / Wiederherstellen von Daten/Datenbank im Schadensfall
12. Nutzung zentraler Sicherungsinfrastruktur, Magnetbandarchiv
13. Bereitstellung und Verwalten von Speichermedien
14. System- und Applikationsmonitoring mit aktiver Prozessüberwachung
15. Problemanalyse und Störungsbearbeitung
16. Einbindung der Infrastruktur in das LAN/WAN, Firewall
17. Automatische Überwachung über Netzwerk-Management
18. Patchmanagement
19. Virenschutz

3.1.2 Netzwerk-Anbindung und Firewall

Bestandteil der Leistung ist die Anbindung der für die Leistungserbringung erforderlichen Komponenten an das LAN des Rechenzentrums bis zum Übergabepunkt des WAN- bzw. Internet Providers.

Aufgaben und Zuständigkeiten	Auftrag-nehmer	Auftrag-geber
Spezifikation der für die Netzwerkkommunikation erforderlichen Protokolle und Kommunikations-Ports (Kommunikations-Matrix)	**B, I**	**V, D**
Beauftragung und Umsetzung der Netzwerkfreischaltungen für Netzverbindungen, die in der Verantwortung des Auftragnehmers liegen	**V, D**	**I**
Beauftragung von Netzfreischaltungen für Netzverbindungen, die nicht in der Verantwortung des Auftragnehmers liegen	**B, I**	**V, D**

3.1.3 Serverbasierte Leistungen Windows und Unix

Der Auftragnehmer stellt für die im Teil B spezifizierten Services zugesicherte Ressourcen bereit. Zugesicherte Ressourcen werden durch Leistungsparameter beschrieben.

Es werden zwei verschiedene Konfigurationen der Plattform unterschieden (gilt auch für virtuelle Systeme):

- Fest zugewiesene Systemressourcen: Dem Auftraggeber stehen die Systemressourcen zur ausschließlichen Nutzung zur Verfügung. Die Dimensionierung muss dabei den geplanten Spitzen-Belastungen entsprechen. Die Konfiguration und Ressourcen der einzelnen Systeme sind im Anhang angegeben und stehen dem Auftraggeber exklusiv zur Verfügung.
- Gemeinsam genutzte Systemressourcen: Hardware und ggf. Software wird von mehreren Auftraggebern genutzt. Für den Spitzenlastausgleich können die Lastprofile aller beteiligten Auftraggeber ganzheitlich betrachtet werden.

Zugesicherte Ressourcen für Windows und UNIX
Die Leistungsbeschreibung beschreibt die jeweils bereitgestellten zugesicherten Ressourcen auf Basis normalisierter Leistungseinheiten.

Leistungseinheiten zu zugesicherten Serverleistungen
- Höhe der zugesicherten Leistung (CPU-Kerne)
- Zugesicherter RAM Hauptspeicher
- Zugesicherte Speicherleistung (für Daten und Programme)

Leistungseinheiten zu zugesicherten Datenbankleistungen
- Höhe der zugesicherten Leistungen (CPU-Kerne)
- Zugesicherter Hauptspeicher
- Anzahl Instanzen
- Anzahl Datenbanken
- Zugesicherte Speicherleistung (für die Datenbanken)

Leistungseinheiten zu zugesicherten Speicherleistungen
- Bereitgestelle Speicherleistung in GB pro Jahr

3.1.4 Technisches Design

Der Auftragnehmer entwickelt eine technische Architektur und stimmt diese mit den Anforderungen des Auftraggebers ab.

Die einzelnen Aufgaben und die Verteilung der Zuständigkeiten sind wie folgt geregelt:

Aufgaben und Zuständigkeiten	Auftrag-nehmer	Auftrag-geber
Informationsbereitstellung von relevanten Normen, Anwendungsarchitekturen und Projektinitiativen	**I, B**	**V, D**
Abstimmung der applikationsrelevanten Teile des Technologieplans mit dem Auftraggeber (initial und bei erforderlicher Änderung)	**V, D**	**I**

3.2 Bereitstellung

Bereitstellung umfasst alle Maßnahmen im Zusammenhang mit der Installation neuer oder erneuerter Hardware- bzw. Systemsoftware-Komponenten.

Die einzelnen Aufgaben und die Verteilung der Zuständigkeiten sind wie folgt geregelt:

3.2.1 Systeme im Rechenzentrum

Aufgaben und Zuständigkeiten	Auftrag-nehmer	Auftrag-geber
Erweiterungen der technischen Infrastruktur	**V, D, B**	**I**
Bereitstellung der neuen / zusätzlichen Ressourcen (Server, Platten etc.) gemäß Teil B	**V, D**	**I**
Installation und Konfiguration von Hardware, Betriebssystem und betriebssystem naher Software (z.B. Middleware) inkl. Einrichtung notwendiger User-Profile und Zugriffsmechanismen, Installation von Komponenten zur Überwachung und Steuerung des Systems und für die Ausgestaltung des Backup	**V, D**	**I**
Durchführung der Datenmigration im Zusammenhang dem Austausch von Systemkomponenten. Ausgenommen sind Datenmigrationen in Folge einer Neuimplementierung oder Plattformmigration.	**V, D**	**I**
Durchführung geeigneter Tests bei allen Installationen, Umzügen, Erweiterungen, Veränderungen der systemtechnischen Infrastruktur	**V, D**	**I**

3.2.2 Systeme in den Räumlichkeiten des Auftraggebers

Die Aufstellung von Systemen in den Räumlichkeiten des Auftraggebers ist möglich. Die inhaltliche Ausgestaltung kann dem Teil B entnommen werden.

3.3 Betrieb und Administration

Leistungen für Betrieb und Administration sind alle Maßnahmen, die im Zusammenhang mit der laufenden Verwaltung installierter Systeme und Softwareumgebungen (Betriebssystem, systemnahe Software) erbracht werden, um einen reibungslosen Betrieb sicherzustellen. Darunter fallen auch die Aufgaben zum Backup & Recovery. Die Aufgaben und Zuständigkeiten sind nachfolgend geregelt.

3.3.1 Basisbetrieb

Aufgaben und Zuständigkeiten	Auftrag-nehmer	Auftrag-geber
Erstellung, Pflege und Bereitstellung Betriebshandbuch (BSI-Grundschutz)	**V, D**	**B, I**
Inhaltliche Abstimmung des Betriebshandbuchs mit dem Auftraggeber	**V, D**	**B, I**
Steuerung und Überwachung der Systeme. Proaktives Erkennen und Vermeiden von Störungen	**V, D**	**I**
Überwachung der einzelnen Komponenten auf wesentliche Kenngrößen wie CPU Auslastung, Performance, Speicherressourcen und Störanzeichen durch Einsatz entsprechender System Monitoring Tools.	**V, D**	**I**
Sammlung und Übermittlung von Kenngrößen für die Anfertigung von Berichten	**V, D**	**I**
Beseitigung von Störungen, Restart / Recovery von Systemkomponenten unter Einhaltung der Eskalationsverfahren	**V, D**	**I**
Antwort auf Anfragen zu Störungen und Problemen beim Kunden	**V, D**	**I**
Durchführung von Diagnoseprozeduren entsprechend der Betriebsanweisungen	**V, D**	**I**
Benennung möglicher Produktveränderungen zur Leistungsoptimierung oder Kostensenkung für den Auftraggeber	**V, D**	**I**
Durchführung und Koordination von Konfigurationsmanagement und Change Management für alle betriebsrelevanten Bereiche	**V, D**	**I**

3.3.2 Backup & Recovery

Abhängig von der gewählten SLA-Klasse wird eine Zuordnung der Aufgaben und Zuständigkeiten im Teil B beschrieben.

Aufgaben und Zuständigkeiten	Auftrag-nehmer	Auftrag-geber
Definition von Backup Anforderungen und Aufbewahrungszeiträumen	**I**	**V, D**
Definition von Backup mit Zeitplänen, Vorgehensweisen, Parametern	**V, D**	**I**
Implementierung der System- und Datenbanksicherung	**V, D**	**B, I**
Durchführung der Datensicherung von System- und Applikationsdaten entsprechend der festgelegten Verfahrensweise (dezentral mit Unterstützung des Auftraggebers)	**V, D**	**I**
Durchführung von Recovery Maßnahmen entsprechend der bestehenden Richtlinien	**V, D**	**I**

3.3.3 User – Administration

Aufgaben und Zuständigkeiten	Auftrag-nehmer	Auftrag-geber
Bereitstellung der Auftraggeber relevanten Informationen und Vorgehensweisen, die für das Berechtigungskonzept erforderlich sind	**I, B**	**V, D**
Definition von Richtlinien für Administration (Berechtigungskonzept)	**V, D**	**I**

Aufgaben und Zuständigkeiten	Auftrag-nehmer	Auftrag-geber
Beauftragung von Berechtigungsänderungen mit Bereitstellung der im Rahmen des Berechtigungskonzeptes definierten administrativen Daten (z. B. Personalnummer, erforderliche Berechtigungsstufe) bei neuen, geänderten und ausscheidenden Benutzern.	**D**	**V**
Einrichten und Verwaltung von Zugriffsberechtigungen von Anwendern für die einzelnen Systeme	**D**	**V**
Anfertigung von Berichten zu administrativen Tätigkeiten nach Abstimmung (z. B. Statistik User neu, geändert, gesamt für verschiedene Systeme / Plattformen)	**V, D**	**I, B**

3.3.4 Datenbank und Middleware Administration

Aufgaben und Zuständigkeiten	Auftrag-nehmer	Auftrag-geber
Bereitstellung der Vorgaben für das Anlegen, Upgrade und Refresh von Datenbanken und Middleware Komponenten	**V, D**	**I**
Bereitstellung aller erforderlichen Informationen und Quellen (Datenträger) zur Installation und Wiederherstellung der Datenbank- und Middlewarekomponenten	**I, B**	**V, D**
Erstinstallation, Upgrade und Refresh von Datenbanken und Middleware	**V, D**	**I**
Pflege von Betriebsdokumentationen	**V, D**	
Überwachung und Steuerung der Datenbank-Systeme, Transaktionsmonitore und Middleware-Komponenten	**V, D**	
Speicherplatzüberwachung der Datenbanken und Middleware	**V, D**	
Mitteilung bei erforderlichen Speicherplatzerweiterungen mit finanziellen Auswirkungen an den Auftraggeber	**V, D**	**I**
Beseitigung von Störungen bei auftretenden Datenbankproblemen im Betrieb und Ergreifen von Gegenmaßnahmen im Störfall	**V, D**	**B**
Einleitung des vereinbarten Eskalationsprozesses	**V, D**	**I**
Einspielen von Patches	**V, D**	**I**
Wartung der Datenbank	**V, D**	

3.3.5 Applikations-Betrieb und Administration

Grundsätzlich liegt das technische Verfahrensmanagement beim Auftragnehmer. Das technische Verfahrensmanagement beinhaltet die systemtechnische Installation, die Konfiguration und das Patchmanagement des Verfahrens, gemäß der vom Auftraggeber (oder von ihm beauftragten Dritten) vorgegebenen und bereitgestellten Installationspakete und Anweisungen (z. B. Ausführung von Setupprogrammen und Konfigurationen nach Checklisten).

- Das Technische Verfahrensmanagement ist erfüllt, wenn die Fachanwendung und ggf. definierte Programmteile starten.
- Ggf. notwendige Vor-Ort-Einsätze des Software-Herstellers (z. B. wenn die oben genannten Voraussetzungen nicht erfüllt sind) werden vom Auftraggeber gesondert beauftragt. Die dabei entstehenden Aufwände trägt der Auftraggeber.
- Installationsleistungen im Rechenzentrum des Auftragnehmers durch Mitarbeiter von Fremdfirmen oder des Auftraggebers müssen von einem Mitarbeiter des Auftragnehmers begleitet werden. Die Begleitung durch einen Mitarbeiter des Auftragnehmers wird gesondert in Rechnung gestellt.

Weitere Leistungen für den Applikations-Betrieb und der Administration werden im Teil B beschrieben.

3.3.6 Batch-Betrieb

Sofern diese Leistungen anfallen, werde diese im Teil B beschrieben.

3.3.7 Erneuerung und Ergänzung

Technologische Erneuerungs- und Ergänzungsleistungen sind alle Maßnahmen im Zusammenhang mit der routinemäßigen Modernisierung der IT-Infrastruktur, mit deren Hilfe sichergestellt wird, dass alle Systemkomponenten auf dem aktuellen Stand der technischen Entwicklung für branchenübliche Technologieplattformen erhalten werden. Die einzelnen Aufgaben und die Verteilung der Zuständigkeiten sind wie folgt geregelt:

Aufgaben und Zuständigkeiten	Auftrag-nehmer	Auftrag-geber
Einführung von Richtlinien und Verfahrensweisen für Erneuerungen und Ergänzung einschließlich Vorgaben für Erneuerungszyklen für eingesetzte Hardware- und Softwarekomponenten	**V, D**	**I, B**
Zustimmung zu den erstellten Richtlinien für Erneuerung und Ergänzung	**I, B**	**V, D**
Ersatz/Nachrüstung von Hardware und Software unter Verwendung geeigneter neuer Technologien	**V, D**	**I, B**

3.3.8 Wartung und Pflege

Um sämtliche Hardware-Systeme und die eingesetzte Software zum Betrieb der Infrastruktur im Rechenzentrum in einem – auch vom Hersteller unterstützten – Zustand zu halten, führt der Auftragnehmer kontinuierlich Verbesserungen und Änderungen durch. Dazu gehören:

Wartungsarbeiten:
Diese dienen der Erhaltung der Betriebsfähigkeit der eingesetzten Hardware. Der Auftragnehmer betreibt grundsätzlich Systeme, deren Komponenten (Betriebssystem, Datenbanken, etc) beim Hersteller unter Wartung sind.

Softwarepflege:
Die Softwarepflege dient der Verbesserung eines Softwareproduktes in Bezug auf die Funktionalität und Performance (*Release*) oder auf Grund von Fehlerbehebung (*Patch*).
Arbeiten, die im Rahmen der Wartung oder Softwarepflege vom Auftragnehmer erbracht werden, führt der Auftragnehmer innerhalb der normalen Büroarbeitszeiten bzw. innerhalb der vereinbarten Wartungszeitfenster durch. Dies gilt für Eingriffe, die die Nutzung des Service nicht übermäßig beeinträchtigen. Der Auftragnehmer entscheidet eigenständig über den Einsatz von Releases oder Patches, die vom Hersteller angeboten werden.

Arbeiten in der RZ-Umgebung, die mit Einschränkungen für den Auftraggeber verbunden sind, werden in den vereinbarten Wartungsfenstern vorgenommen und mit dem Auftraggeber abgestimmt.
Widerspricht der Auftraggeber einer vom Auftragnehmer empfohlenen Wartungsmaßnahme und entstehen dadurch Mehraufwände, so sind diese vom Auftraggeber zu tragen.

Die Verantwortlichkeiten für die einzelnen Wartungsaufgaben sind wie folgt geregelt:

Aufgaben und Zuständigkeiten	Auftrag-nehmer	Auftrag-geber
Definition von Richtlinien und Verfahrensweisen für Wartung und Reparatur, Einspielen von Patches und Releasewechsel	**V, D**	**I**
Prüfung der Relevanz von veröffentlichten Service Packs, Firmware, Patches etc.	**V, D**	**I**

Aufgaben und Zuständigkeiten	Auftrag-nehmer	Auftrag-geber
Planung von systemspezifischen Wartungsarbeiten	V, D	I
Durchführung von exemplarischen Tests vor der Ausführung systemspezifischer Wartungsarbeiten	V, D	I
Ausführung systemspezifischer Wartungsarbeiten (z. B. Installation von Service Packs, Firmware, Patches und Software Maintenance Releases)	V, D	I
Planung und Abstimmung von Releasewechseln mit dem Auftraggeber (insbesondere Applikationsexperten etc.)	V, D	B
Genehmigung von Releasewechseln hinsichtlich der Kompatibilität mit Systemen / Anwendungen, die unter Verantwortung des Auftraggebers betrieben werden.	V	B
Durchführung der Software-Distribution bei Release-wechsel; Versionskontrolle aller installierten Software Produkte einschließlich Anpassung der Schnittstellen der betroffenen Anwendungen, die vom Auftragnehmer betreut werden	V, D	I
Vorbeugende HW-Wartung entsprechend der Herstellerempfehlungen	V, D	I

3.3.9 Fernzugriff und Fernwartung, Fernunterstützung und Fernbedienung

Ein Fernzugriff liegt vor, wenn Mitarbeiter des Auftragsnehmers oder beauftragte Dritte von einem System auf ein anderes System zu Wartungs-, Reparatur-, Bedienungs- oder Unterstützungszwecken, über nicht-dedizierte Kommunikationskanäle zugreifen.

„Fernzugriff“ ist der Oberbegriff für die im Folgenden dargestellten Fallarten:

- Fernwartung
  Eine Fernwartung setzt eine administrative Tätigkeit von einem externen System auf ein internes System voraus.
  Eine administrative Tätigkeit liegt vor, wenn die Tätigkeit der Verwaltung der Nutzbarmachung des IT-Fachverfahrens dient und nicht ausschließlich der Nutzung eines IT-Fachverfahrens oder dem Support aus Nutzersicht.
- Fernunterstützung
  Die Fernunterstützung stellt einen „nur sehenden“ Fernzugriff, ohne direkte Kontrollmöglichkeit des Systems, dar.
- Fernbedienung
  Mit Einverständnis des Nutzers kann die Fernunterstützung auch in Form einer Fernbedienung erfolgen. Der Zugreifende übernimmt die aktive Steuerung wahlweise mit dem Rechteprofil des Nutzers oder – nach dessen Abmeldung – mit einem auf dem Zielsystem hinterlegtem Fernbedienungs-Account.

Der Fernzugriff von Mitarbeiter des Auftragsnehmers auf zu betreuende Systeme erfolgt in Übereinstimmung mit einem grundschutzkonformen Sicherheitskonzept am Maßstab eines hohen Schutzbedarfs.

Der Fernzugriff von beauftragten Dritten kann ausschließlich über eine vom Auftragnehmer vorgegebene Kommunikations-, Zugriff- und Infrastrukturlösung in Übereinstimmung mit einem grundschutzkonformen Sicherheitskonzept am Maßstab eines hohen Schutzbedarfs erfolgen.
Voraussetzung für die Einrichtung eines Fernzugriffs für Dritte ist der Nachweis, dass durch den Zugriff Dritter keine Gefahr für die Sicherheit der Daten und Ressourcen hinsichtlich der Vertraulichkeit, Integrität und Verfügbarkeit entstehen.

Prüfung und Freigabe des Nachweises erfolgt durch den ITSB des Auftragnehmers.

Details zum Fernzugriff und zur Fernwartung, Fernunterstützung und Fernbedienung sind ggf. im Teil B geregelt.

3.3.10 Kommunikationsanbindung zum RZ

Der Auftraggeber gewährleistet, dass die Anwender des zentralen Verfahrens über einen Zugang zum Landesnetz oder einen mit dem Auftragnehmer abgestimmten, gleichwertigen Anschluss verfügen.

Der Auftraggeber stellt eine für den laufenden Betrieb ausreichend performante Netzanbindung sicher.

4 Leistungskennzahlen

4.1 Definition

Eine Leistungskennzahl ist eine Maßzahl, die zur Qualifizierung einer Leistung dient und der eine Vorschrift zur quantitativen reproduzierbaren Messung einer Größe oder Vorgangs zu Grunde liegt.

4.1.1 Begriffsfestlegungen

Betriebsmodus	Begriffsdefinition
Betriebszeit (unbetreuter Betrieb)	Die Betriebszeit ist der Zeitraum, in der die vereinbarten Ressourcen vom Auftragnehmer zur Verfügung gestellt und automatisiert überwacht werden.
Servicezeit	Servicezeiten beschreiben Zeiträume, in denen definierte Services zur Verfügung steht.
Supportzeit (betreuter Betrieb)	Die Servicezeit „Supportzeit (betreuter Betrieb)“ beschreibt die Zeiträume, in denen die Ressourcen vom Auftragnehmer bedient und Störungen und Anfragen bearbeitet werden.
Wartungsfenster	Regelmäßiges Zeitfenster für Wartungsarbeiten an den Systemen, in dem die Systeme nicht oder nur eingeschränkt für den Auftraggeber nutzbar sind. Sollte in Sonderfällen ein größeres oder weiteres Wartungszeitfenster beansprucht werden, so erfolgt dies in direkter Absprache mit dem Auftraggeber. Der Auftraggeber wird nur in begründeten Fällen die Durchführung von Wartungsmaßnahmen einschränken. Der Auftragnehmer wird in diesen Fällen unverzüglich über sich ggf. daraus ergebenden Mehraufwand und Folgen informieren.
Verfügbarkeit	Prozentualer Anteil an einer zugesagten Servicezeit (z. B. „Supportzeit betreuter Betrieb“) innerhalb eines Messzeitraumes, in der die beschriebenen Komponenten für den Auftraggeber nutzbar sind. $\text{Verfügbarkeit} = 1 - \frac{\sum \text{ungeplante Ausfallzeiten } [h]}{\text{Supportzeit (betreuter Betrieb) im Messzeitraum (Jahr) } [h]}$
Ausfallzeit	Die Ausfallzeit ist die Zeitspanne, die nach Eintritt der Nichtverfügbarkeit während der zugesagten Servicezeit vergeht, bis ein System (bzw. Systemcluster) mit allen Komponenten wieder für den Regelbetrieb zur Verfügung steht. Gemessen wird die Ausfallzeit in Stunden innerhalb der vereinbarten Servicezeiten.
Reaktionszeit	Die Reaktionszeit ist die Zeitspanne innerhalb der vereinbarten Servicezeiten zwischen der Feststellung einer Störung durch den Dienstleister bzw. Meldung einer Störung durch den Auftraggeber über den vereinbarten Weg (Service Desk) bis zum Beginn der Störungsbeseitigung. Die Reaktionszeit beginnt mit der Aufnahme der Störung in das Ticketsystem des Auftragnehmers.
Messzeitraum	Der Zeitraum, auf den sich eine Leistungskennzahl bezieht und in dem die tatsächlich erbrachte Qualität der Leistung gemessen wird. Sofern nicht anders angegeben beziehen sich alle angegebenen Metriken jeweils auf einen Messzeitraum von einem Kalenderjahr.

4.2 Leistungsausprägung

Die beschriebenen Leistungen sind jeweils in verschiedenen Ausprägungen mit unterschiedlichen Qualitätskriterien und Preisen verfügbar, um entsprechend den Anforderungen auf Kundenseite eine optimale Anpassung zwischen benötigter Leistung und Preis erreichen zu können.

[redacted].

Leistungsausprägung	Einsatzgebiet
Typ 1 (Höchstverfügbar) Premium Plus Premium Plus	Höchste Anforderungen bezüglich Verfügbarkeit und Priorität bei der Bereitstellung, Wartung und Störungsbeseitigung für den Betrieb besonders geschäftskritischer Systeme.
Typ 2 (Hochverfügbar) Premium	Hohe Anforderungen bezüglich Verfügbarkeit und Priorität bei der Bereitstellung, Wartung und Störungsbeseitigung für den Betrieb von geschäftskritischen Systemen.
Typ 3 (normale Verfügbarkeit) Standard	Durchschnittliche Anforderungen bezüglich Verfügbarkeit und mittlere Priorität bei der Bereitstellung, Wartung und Störungsbeseitigung für den Produktivbetrieb von Systemen, die nicht geschäftskritisch sind.
Typ 4 (einfache Verfügbarkeit) Economy	Niedrige Anforderungen bezüglich Verfügbarkeit und Priorität bei Bereitstellung, Wartung und Störungsbeseitigung für sonstige Systeme

Die Feststellung der Anforderungen an die Verfügbarkeit eines Systems und die Eingruppierung in eine Typklasse erfolgt vom Auftragnehmer gemeinsam mit dem Auftraggeber und wird im Teil B festgeschrieben.

4.3 Vereinbarte Leistungskennzahlen

Leistungskennzahlen für Betriebsleistungen.

SLA Klassen	1 Premium Plus	2 Premium	3 Standard	4 Economy
Betriebszeit (unbetreuter Betrieb)	7 Tage x 24 Stunden			
Supportzeit (betreuter Betrieb)	Mo-Do 08:00 - 17:00 Uhr Fr 8.00 – 15.00 Uhr			
Wartungsfenster	Di. 19:00 – Mi. 06:00 Uhr; Ausnahmen nach Vereinbarung			
Reaktionszeit im Störungsfall	30 Minuten		60 Minuten	120 Minuten
Zielverfügbarkeit des definierten Services	[redacted]	[redacted]	[redacted]	[redacted]
Storage-Verfügbarkeitsklassen (Obligatorisch bei RDBMS- Service)	Premium	Premium	Standard	Standard

Die Verfügbarkeit wird für zentrale Anwendungen bis zur Datenübergabeschnittstelle ans WAN / Internet garantiert, für dezentrale Anwendungen gilt die Gewährleistung am Erbringungsort.

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

Verfügbarkeitsklassen	Beschreibung
Premium	Für die Verfügbarkeitsklasse Premium werden gespiegelte Speichersysteme eingesetzt. Solche Systeme sind in sich mehrfach redundant aufgebaut, um höchste Verfügbarkeit zu gewährleisten. Ein Ausfall einer Einzelkomponente betrifft damit nur einen sehr geringen Teil des Gesamtsystems. Der Großteil steht ohne Funktions- oder Performanceeinbußen weiter zur Verfügung. Durch entsprechende redundante Anbindung eines Serversystems wird, je nach Anforderung an die Verfügbarkeit, auch dieser Fehlerfall vollständig abgefangen. Die Speichersysteme stehen auch während Software-Upgrades, Erweiterungen oder Konfigurationsänderungen unterbrechungsfrei zur Verfügung. Die Speichersysteme der Verfügbarkeitsklasse Premium sind für die SLA-Klassen Premium Plus und Premium Voraussetzung. Es gibt sie in den Konfigurationen Schutzbedarf „Normal“ und Schutzbedarf „Hoch“.
Standard	Für die Verfügbarkeitsklasse Standard kommen ungespiegelte Speichersysteme zum Einsatz. Alle Komponenten dieser Systeme sind mindestens doppelt ausgelegt, um bei Ausfall einer Komponente den weiteren Betrieb sicherzustellen. Durch entsprechende redundante Anbindung eines Serversystems wird, je nach Anforderung an die Verfügbarkeit, auch dieser Fehlerfall vollständig abgefangen. Software-Upgrades und Erweiterungen haben i.d.R. keine Auswirkungen auf den Betrieb. Midrangesysteme können für die SLA-Klassen Standard und Economy eingesetzt werden. Es gibt sie in den Konfigurationen Schutzbedarf „Normal“ und Schutzbedarf „Hoch“.

4.4 Reporting

Über die Auswertungen bzgl. der Einhaltung der Service Level erbringt der Auftragnehmer einen monatlichen Nachweis über die erbrachten Leistungen.

Der Nachweis umfasst folgende Bereiche:

- Gegenüberstellung zwischen den Messwerten der erbrachten Leistungskennzahlen und den definierten Sollwerten (Service Level Performance)
- Trendbewertung für vereinbarte Systemen bzgl. Auslastung, Performance, Kapazität entsprechend der definierten Richtlinien und daraus abgeleiteten Handlungsempfehlungen

5 Erläuterungen

5.1 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.

dataport

Service Level Agreement

Bereitstellung der Infrastruktur und Betrieb *des Verfahrens CKAN (Hamburgisches Transparenzgesetz)* im Rechenzentrum

Verfahrensspezifischer Teil (Teil B)

für

Finanzbehörde

Große Bleichen 27

20354 Hamburg

nachfolgend Auftraggeber

Version: 1.0
Stand: 11.10.2013

dataport

Inhaltsverzeichnis

1 Einleitung ... 3

1.1 Aufbau des Dokumentes ... 3

1.2 Leistungsgegenstand ... 3

1.3 Ergänzende Informationen/Abgrenzungen zum SLA Teil A Allgemeiner Teil ... 3

1.3.1 Ergänzende Informationen ... 3

1.3.2 Abgrenzungen ... 4

2 Rahmenbedingungen ... 5

2.1 Mitwirkungsrechte und –pflichten ... 5

3 Leistungsbeschreibung ... 6

3.1 Infrastrukturleistungen ... 6

3.1.1 Netzwerk-Anbindung und Firewall ... 6

3.1.2 Serverbasierte Leistungen Windows und UNIX ... 6

3.1.2.1 Applikationsservice ... 6

3.1.2.2 Webservice ... 7

3.1.2.3 Datenbankservice ... 7

3.2 Betrieb und Administration ... 8

3.2.1 Backup & Recovery ... 8

3.2.2 Besondere Leistungsvereinbarungen für den Betrieb von UBUNTU ... 8

3.3 Lizenzleistungen ... 9

3.3.1 Lizenzleistungen aus Landesverträgen / Rahmenverträgen ... 9

4 Leistungskennzahlen ... 10

4.1 Leistungsausprägung ... 10

4.1.1 Betriebszeiten ... 10

4.1.1.1 Onlineverfügbarkeit ... 10

4.1.1.2 Servicezeit - Betreuter Betrieb ... 10

4.1.1.3 Servicezeit - Überwachter Betrieb ... 10

4.1.2 Wartungsarbeiten ... 10

4.1.3 Support ... 10

4.1.4 Störungsannahme ... 11

4.1.5 Incident-Management ... 11

5 Erläuterungen ... 13

5.1 Erläuterung VDBI ... 13

1 Einleitung

Der Auftragnehmer stellt dem Auftraggeber IT Ressourcen einschließlich Hardware und systemnaher Software sowie IT Dienstleistungen mit dem vereinbarten Leistungsumfang bedarfsgerecht zur Verfügung (im Folgenden als Verfahren bezeichnet). Mit dieser Leistungsvereinbarung (Service Level Agreement, SLA) wird der Leistungsgegenstand geregelt.

1.1 Aufbau des Dokumentes

Diese Anlage enthält die folgenden Kapitel:

Rahmenbedingungen (Kapitel 2): Individuelle Regelung von Rechten und Pflichten von Auftraggeber und Dienstleister, Bestimmungen zur Laufzeit, Änderung bzw. Kündigung der Vereinbarung sowie Übergangsbestimmungen.

Leistungsbeschreibungen (Kapitel 3): Individuelle inhaltliche Beschreibung der bereitgestellten Rechenzentrumsleistungen sowie individuelle Vereinbarungen von für einen reibungslosen Betrieb erforderlichen Dienstleistungen.

Leistungskennzahlen (Kapitel 4): Individuelle Definition von Leistungskennzahlen und ihrer Messverfahren (z. B. Verfügbarkeit oder Reaktionszeiten), Festlegung von Betriebs- und Servicezeiten und Vereinbarungen über die zu erreichende Leistungsqualität (Service Level Objectives).

Erläuterungen (Kapitel 5)

1.2 Leistungsgegenstand

Gegenstand dieses Service Level Agreements ist die Bereitstellung der Dienstleistungen im Rechenzentrum.

Die allgemeinen Leistungen werden hinsichtlich der Leistungsqualität und des Leistungsumfangs im Teil A beschrieben. Die verfahrensspezifischen Leistungen werden im Teil B beschrieben.

1.3 Ergänzende Informationen/Abgrenzungen zum SLA Teil A Allgemeiner Teil

1.3.1 Ergänzende Informationen

- Punkt 3.2.2: Eine Aufstellung in den Räumen des Auftraggebers erfordert immer eine gesonderte detaillierte Prüfung der Gegebenheiten vor Ort. Ggfs. sind Bereitstellungsleistungen des Auftraggebers erforderlich, die dann in Punkt 3 dieses SLAs geregelt werden.
- Punkt 3.3.1: Produktveränderungen zur Leistungsoptimierung oder Kostensenkung für den Auftraggeber werden unter Berücksichtigung der aktuell geltenden RZ Standards zwischen Produktverantwortlichem, Architektur und dem Auftraggeber abgestimmt

1.3.2 Abgrenzungen

Die hier im Folgenden aufgeführten in Teil A definierten Services können teilweise erst mit dem Umzug der hier betroffenen Fachverfahren und zugehörigen Services in die neuen Dataport Rechenzentren (RZ²) reportet werden. Der Umzug erfolgt im Rahmen der Transitionen des Projekts RZ².

- Punkt 3.3.1: Sammlung und Übermittlung von Kenngrößen für die Anfertigung von Berichten
- Punkt 3.3.1: „Erstellung und Abstimmung von Betriebsführungshandbüchern nach BSI_Grundschutz“
- Punkt 3.3.3: „Anfertigung von Berichten zu administrativen Tätigkeiten nach Abstimmung (z. B. Statistik User neu, geändert, gesamt für verschiedene Systeme / Plattformen)“
- Punkt 3.3.7: „Einführung von Richtlinien und Verfahrensweisen für Erneuerungen und Ergänzung einschließlich Vorgaben für Erneuerungszyklen für eingesetzte Hardware- und Softwarekomponenten“
- Punkt 4.4: „Reporting“

2 Rahmenbedingungen

2.1 Mitwirkungsrechte und –pflichten

Die vom Auftragnehmer zugesagten Leistungen erfolgen auf Anforderung des Auftraggebers. Es sind Mitwirkungs- und Bereitstellungsleistungen des Auftraggebers erforderlich.

Ergibt sich aus der Unterlassung von Mitwirkungspflichten und Nichtbeistellung des Auftraggebers von festgelegten Informationen / Daten eine Auswirkung auf die Möglichkeit der Einhaltung der Service Level, entlastet dies den Auftragnehmer von der Einhaltung der vereinbarten Service Level ohne Einfluss auf die Leistungsvergütung für die bereitgestellten Ressourcen.

3 Leistungsbeschreibung

3.1 Infrastrukturleistungen

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

3.1.1 Netzwerk-Anbindung und Firewall

Für Dienststellen der Verwaltung des Landes Schleswig-Holstein wird ein Zugang zum Landesnetz Schleswig-Holstein vorausgesetzt.

Für Dienststellen der Freien und Hansestadt Hamburg wird ein Zugang zum Hamburgischen Landesnetzes (FHHNetz) vorausgesetzt.

3.1.2 Serverbasierte Leistungen Windows und UNIX

3.1.2.1 Applikationsservice

Es werden zugesicherte Ressourcen für die nachfolgend spezifizierten Services bereitgestellt.

CKAN Applikationsservice

Betriebssystem

UBUNTU

Produktionsstufen		SLA-Klasse		SAN und Backup	
Produktion	x	Economy	[redacted]	SAN Highend	
QS / Stage	x	Standard		SAN Midrange	
Test	x	Premium		Backup 30 Tage	
Entwicklung		Premium Plus			
Schulung					

Zugesicherte Ressourcen

Anzahl	Servicebezeichnung	zugesicherte CPU-Kerne	zugesicherter RAM	zugesicherte Speicher-leistung in GB
[redacted]	**Applikationsservice Standard Produktion Allocated L**	[redacted]	[redacted]	
	Applikationsservice IPS Standard Produktion Allocated L			
	Applikationsservice Standard QS Allocated M			
	Applikationsservice IPS Standard QS Allocated M			
	Applikationsservice Standard Test Allocated M			
	Applikationsservice IPS Standard Test Allocated M			

Ergänzungen / Bemerkungen

3.1.2.2 Webservice

Es werden zugesicherte Ressourcen für die nachfolgend spezifizierten Services bereitgestellt.

CKAN Webservice

Betriebssystem

UBUNTU

Produktionsstufen		SLA-Klasse		SAN und Backup	
Produktion	x	Economy	[redacted]	SAN Highend	
QS / Stage		Standard		SAN Midrange	
Test		Premium		Backup 30 Tage	
Entwicklung		Premium Plus			
Schulung					

Zugesicherte Ressourcen

Anzahl	Servicebezeichnung	zugesicherte CPU-Kerne	zugesicherter RAM	zugesicherte Speicher-leistung in GB
[redacted]	**Webservice Standard Produktion Allocated L**	[redacted]	[redacted]	
	Webservice Standard QS Allocated M			

Ergänzungen / Bemerkungen

3.1.2.3 Datenbankservice

Es werden zugesicherte Ressourcen für die nachfolgend spezifizierten Services bereitgestellt.

CKAN Datenbankservice

RDBMS

PostgreSQL

Betriebssystem

UBUNTU

Produktionsstufen		SLA-Klasse		SAN und Backup	
Produktion	x	Economy	[redacted]	SAN Highend	[redacted]
QS / Stage	x	Standard		SAN Midrange	
Test	x	Premium		Backup 30 Tage	
Entwicklung		Premium Plus			
Schulung					

Zugesicherte Ressourcen

Anzahl	Servicebezeichnung	zugesicherte CPU-Kerne	zugesicherter RAM	zugesicherte Speicher-leistung in GB
[redacted]	**Datenbank Standard Dedicated XL Produktion**	[redacted]	[redacted]	[redacted]
	Datenbank Standard QS Allocated L			
	Datenbank Standard Test Allocated L			

Ergänzungen / Bemerkungen

Die zugesicherte Speicherleistung verteilt sich auf DATA und LOG.

3.2 Betrieb und Administration

3.2.1 Einmalige Leistungen

Für die Erstellung eines technischen Soll-Konzepts der Verfahrensinfrastruktur werden einmalig [redacted] Personenstunden veranschlagt.

3.2.2 Backup & Recovery

Die Datensicherung umfasst die Sicherung sämtlicher Daten, die zur Ausführung und für den Betrieb der Verfahren notwendig sind. Diese wird gemäß Anforderung des Auftraggebers eingerichtet.

Programm-Dateien, Konfigurations-Dateien und Nutzdaten-Dateien. Verfahrensdaten, die in der Registry abgelegt sind, gehören zu den Systemdaten, die durch die Systemsicherung entsprechend zu sichern sind. Die Systemsicherung wird vom Auftragnehmer standardmäßig eingerichtet.

Gemäß Standard im Dataport Rechenzentrum erfolgt für Applikations-, Web- und Terminalservices einmal wöchentlich eine Vollsicherung sowie eine tägliche inkrementelle Sicherung.

Für Datenbankservices wird einmal tägliche eine Vollsicherung durchgeführt, dazwischen erfolgt alle drei Stunden eine Logsicherung.

Die gesicherten Daten werden 30 Tage aufbewahrt.

Im Fehlerfall bzw. auf Anforderung des Auftraggebers erfolgt eine Wiederherstellung der Daten.

Entsprechend den Anforderungen des Auftraggebers kann von den Standard-Sicherungszyklen abgewichen werden. Dies ist im Einzelfall auch unter Berücksichtigung der technischen Möglichkeiten abzustimmen.

3.2.3 Besondere Leistungsvereinbarungen für den Betrieb von UBUNTU

Hinsichtlich der Einführung eines für den Auftragnehmer im standardisierten Rechenzentrumsbetrieb neuen Betriebssystems UBUNTU wird derzeit davon ausgegangen, dass die vorhanden Services (Patchmanagement, Monitoring, Virenschutz etc.) installier- und betreibbar sind.

Insofern sich bei den Realisierungen hierzu Abweichungen oder anderslautende Erkenntnisse ergeben, kann dies Auswirkungen auf das SLA haben.
Dieses ist bis zur abgeschlossenen Einführung daher als vorläufig zu betrachten.

3.3 Lizenzleistungen

Die Lizenzleistungen sind zwischen Auftraggeber und Auftragnehmer wie nachfolgend beschrieben vereinbart.

Aufgaben und Zuständigkeiten	Auftrag-nehmer	Auftrag-geber
Betriebssystemlizenzen inklusive Wartung, Assurance, UBUNTU		**V,D**
Lizenzen für zentrale RZ-Dienste wie Datensicherung, Systemmanagement, Netzwerküberwachung	**V,D**	
Virenschutz auf allen Systemen, die der Auftragnehmer als Bestandteil dieses SLAs bereitstellt	**V,D**	
Fachanwendung		**V,D**
RDBMS (PostgreSQL)		**V,D**
Lizenzleistungen aus Landesverträgen des Auftraggebers		**V, D**

3.3.1 Lizenzleistungen aus Landesverträgen / Rahmenverträgen

Lizenzleistungen, die der Auftraggeber durch Vereinbarungen außerhalb der hier vorliegenden Leistungsvereinbarung nutzen kann (z. B. aus Landesverträgen, Rahmenverträgen etc.), sind im Rahmen dieser Leistungsvereinbarung eine **Beistellungsleistung des Auftraggebers**.

Erlischt deren Nutzbarkeit für den Auftraggeber, ist der Auftraggeber verpflichtet, eine im Sinne des Lizenzrechts des Lizenzgebers gleichwertige Lizenzleistung beizubringen oder beim Auftragnehmer eine im Sinne des Lizenzrechts des Lizenzgebers gleichwertige Lizenzleistung zu beauftragen.

Die nachfolgend stehenden Lizenzen werden im Rahmen dieser Leistungsvereinbarung als Beistellungsleistung des Auftraggebers vom Auftragnehmer genutzt:

Lizenz	Lizenztyp	Anzahl	inklusiv...	Bemerkungen / Ergänzungen
	☐ Clientlizenz ☐ Serverlizenz ☐ CPU-Lizenz		☐ Wartung ☐ ☐	
	☐ Clientlizenz ☐ Serverlizenz ☐ CPU-Lizenz		☐ Wartung ☐ ☐	
	☐ Clientlizenz ☐ Serverlizenz ☐ CPU-Lizenz		☐ Wartung ☐ ☐	
	☐ Clientlizenz ☐ Serverlizenz ☐ CPU-Lizenz		☐ Wartung ☐ ☐	

4 Leistungskennzahlen

4.1 Leistungsausprägung

4.1.1 Betriebszeiten

4.1.1.1 Onlineverfügbarkeit

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

4.1.1.2 Servicezeit - Betreuter Betrieb[1]

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

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

4.1.1.3 Servicezeit - Überwachter Betrieb

- alle Zeiten außerhalb des betreuten Betriebes

Auch außerhalb des betreuten Betriebes stehen die Systeme den Anwendern grundsätzlich zur Verfügung. Die Systeme werden automatisiert überwacht. Festgestellte Fehler werden automatisch in einem Trouble-Ticket-System hinterlegt. Ansprechpartner stehen während des überwachten Betriebes nicht zur Verfügung.

4.1.2 Wartungsarbeiten

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

4.1.3 Support

Der Auftragnehmer übernimmt den Support für die vom Auftragnehmer angebotenen Leistungen. Der Auftragnehmer übernimmt keine verfahrensbezogenen fachlichen Supportleistungen. Ggf. notwendige Vor-Ort-Einsätze des Software-Herstellers für technische oder fachliche Supportleistungen werden vom Auftraggeber beauftragt und die entstehenden Aufwände trägt der Auftraggeber.

[1] Gilt nicht für gesetzliche Feiertage, sowie 24.12. und 31.12.

- Support für den Betrieb erfolgt durch die Annahme von Störungsmeldungen und die Einleitung der Behebung des zugrunde liegenden Problems.
- Support für Verfahren sowohl vom Auftragnehmer als auch von anderen Herstellern ist nicht Bestandteil der Leistung und kann optional beauftragt werden.

4.1.4 Störungsannahme[2]

Die Störungsannahme erfolgt grundsätzlich über das Call-Center/den Userhelpdesk des Auftragnehmers.

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

4.1.5 Incident-Management

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

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

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

Priorität	Auswirkung	Dringlichkeit	Bearbeitung
Niedrig (bisher 4)	Incident betrifft einzelne Benutzer. Die Geschäftstätigkeit ist nicht eingeschränkt.	Ersatz steht zur Verfügung und kann genutzt werden, oder das betroffene System muss aktuell nicht genutzt werden. Tätigkeiten, deren Durchführung durch den Incident behindert wird, können später erfolgen.	Priorität Niedrig führt zur Bearbeitung durch den Auftragnehmer und unterliegt der Überwachung des Lösungsfortschritts. Die Reaktionszeit (Beginn der Bearbeitung oder qualifizierter Rückruf) ergibt sich aus der Serviceklasse.
Mittel (bisher 3)	Wenige Anwender sind von dem Incident betroffen. Geschäftskritische Systeme sind nicht betroffen. Die Geschäftstätigkeit kann mit leichten Einschränkungen aufrechterhalten werden.	Ersatz steht nicht für alle betroffenen Nutzer zur Verfügung. Die Tätigkeit, bei der der Incident auftrat, kann später oder auf anderem Wege evtl. mit mehr Aufwand durchgeführt werden.	Priorität Mittel führt zur standardmäßigen Bearbeitung durch den Auftragnehmer und unterliegt der Überwachung des Lösungsfortschritts. Die Reaktionszeit (Beginn der Bearbeitung oder qualifizierter Rückruf ergibt sich aus der Serviceklasse.
Hoch (bisher 2)	Viele Anwender sind betroffen. Geschäftskritische	Ersatz steht kurzfristig nicht zur Verfügung. Die Tätigkeit, bei der der Incident auftrat,	Priorität Hoch führt zur bevorzugten Bearbeitung durch den Auftragnehmer und

[2] Gilt nicht für gesetzliche Feiertage, sowie 24.12. und 31.12.

	Systeme sind betroffen. Die Geschäftstätigkeit kann eingeschränkt aufrechterhalten werden.	muss kurzfristig durchgeführt werden.	unterliegt besonderer Überwachung des Lösungsfortschritts. Die Reaktionszeit (Beginn der Bearbeitung oder qualifizierter Rückruf ergibt sich aus der Serviceklasse.
Kritisch (bisher 1)	Viele Anwender sind betroffen. Geschäftskritische Systeme sind betroffen. Die Geschäftstätigkeit kann nicht aufrechterhalten werden.	Ersatz steht nicht zur Verfügung. Die Tätigkeit, bei der der Incident auftrat, kann nicht verschoben oder anders durchgeführt werden.	Priorität Kritisch führt zur umgehenden Bearbeitung durch den Auftragnehmer und unterliegt intensiver Überwachung des Lösungsfortschritts. Die Reaktionszeit (Beginn der Bearbeitung oder qualifizierter Rückruf ergibt sich aus der Serviceklasse.

5 Erläuterungen

5.1 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.

dataport

Service Level Agreement

Technisches Verfahrensmanagement

allgemeiner Teil (Teil A)

zum IT-Verfahren CKAN (Hamburgisches Transparenzgesetz)

für

Finanzbehörde
Große Bleichen 27
20354 Hamburg
nachfolgend Auftraggeber

Version: 1.1
Stand: 17.06.2013

Inhaltsverzeichnis

1 Einleitung 3

1 Einleitung

Das Dokument wird entsprechend des Projektfortschritts fortgeschrieben und in der aktuellen Fassung dem Auftraggeber bereitgestellt.

dataport

Service Level Agreement

Technisches Verfahrensmanagement

verfahrensspezifischer Teil (Teil B)

zum IT-Verfahren CKAN (Hamburgisches Transparenzgesetz)

für

Finanzbehörde

Große Bleichen 27

20354 Hamburg

nachfolgend Auftraggeber

Version: 1.1
Stand: 10.06.2013

Inhaltsverzeichnis

1 Einleitung 3

1 Einleitung

Das Dokument wird entsprechend des Projektfortschritts fortgeschrieben und in der aktuellen Fassung dem Auftraggeber bereitgestellt.

HmbTG-IT-System

Beschreibung der Anforderungen

Version/Zustand (1.0 / in Bearbeitung/vorgelegt/fertig gestellt)

21.08.2013

Änderungsverzeichnis

Änderung			Geänderte Kapitel	Beschreibung der Änderung	Autor
Nr.	Datum	Version			
1	19.07.2013	0.1	1,2 und 3 Ausgenommen 3.2.2	Einarbeitung von Anmerkungen des FHH-Projektes bis zum 17.07.13	[redacted]
2	22.07.2013	0.1.1	3.2.	Einleitung 3.2 geändert	[redacted]
3	22.07.2013	0.1.2	3.2.2 und 3.2.3	Einarbeitung von Anmerkungen des FHH-Projektes bis zum 17.07.13	[redacted]
4	23.07.2013	0.1.3	3.2	Neugliederung des Kapitels, Redaktionelle Überarbeitung des gesamten Kapitels	[redacted]
5	28.07.2013	0.1.4	3.2	Anpassung und Ergänzung der Anforderungsbeschreibungen	[redacted]
6	02.08.2013	0.1.5	alle	Redaktionelle Anpassungen / Überarbeitungen eingepflegt	[redacted]
7	21.08.2013	1.0	Neuer Zuschnitt	Extraktion der die Anforderungen betreffenden Kapitel und entsprechende Umwidmung des Dokuments	[redacted]

Inhaltsverzeichnis

Änderungsverzeichnis 2
Inhaltsverzeichnis 3
1 Zweck dieses Dokumentes 4
2 Organisatorischer Rahmen 4
3 Anforderungen HmbTG-IT-System 4
3.1 Terminliche Anforderungen 4
3.1.1 Terminziel „Informationsregister ist online“ 4
3.1.2 Terminziel „Produktionsbereitschaft für Veröffentlichung“ 5
3.1.3 Terminziel „Test- und Schulungsbereitschaft“ 5
3.2 Anforderungen an die bereitzustellende IT 7
3.2.1 Übergreifende Anforderungen an die bereitzustellende IT 8
3.2.2 Zulieferungen 10
3.2.3 Zentraler Metadatenspeicher 16
3.2.4 Zentraler Datenspeicher 20
3.2.5 Suchkomponente für verteilte Informationshaltung 23
3.2.6 Portal 26
3.3 Rahmenvorgaben 27
3.3.1 Quellen 27
3.3.2 Sicherheitsanforderungen 28
3.3.3 Anforderungen an Software- und Systemarchitektur 29
3.3.4 Anforderungen Lösungsarchitektur 29
3.3.5 Wirtschaftlichkeit 29

1 Zweck dieses Dokumentes

Dieses Dokument spezifiziert die Anforderungen der FHH an das für die Umsetzung des Hamburgischen Transparenzgesetzes zu schaffende IT-System („HmbTG-IT-System“).

2 Organisatorischer Rahmen

Die Staatsräte der Behörde für Justiz und Gleichstellung[1], Finanzbehörde[2] und Kulturbehörde[3] haben zum 01.10.2012 das behördenübergreifende Projekt „Umsetzung des HmbTG“ mit dem Ziel „Termingerechte Schaffung der Voraussetzungen für die Umsetzung des HmbTG“ eingerichtet (im Folgenden kurz: „FHH-Projekt“ genannt).

Aufgabe dieses Projektes ist insbesondere die Schaffung der informationstechnischen Voraussetzungen zur Veröffentlichung von Informationen für veröffentlichungspflichtige Stellen („HmbTG-IT-System“) und die Unterstützung dieser Stellen bei der Nutzung dieser IT bzw. Unterstützung bei der Anbindung ggf. vorhandener, von ihnen selbst verantworteter, IT-Fachverfahren („Liefersysteme“).

Nachfolgend werden die Anforderungen an das HmbTG-IT-System dargelegt.

3 Anforderungen HmbTG-IT-System

3.1 Terminliche Anforderungen

3.1.1 Terminziel „Informationsregister ist online“

Anforderung

Spätestens am 06. Oktober 2014 müssen die IT-Anteile der technischen Voraussetzungen für die Umsetzung des HmbTG („HmbTG-IT-System“) für die produktive Nutzung bereitstehen und alle nach dem Gesetz erforderlichen Inhalte proaktiv veröffentlicht sein.

Aus diesem Grund muss das Informationsregister, samt den gesetzlich vorgeschriebenen Inhalten, online zur Verfügung stehen.

Begründung

§ 18 Abs. 1 ...Die technischen Voraussetzungen für die Umsetzung dieses Gesetzes sind innerhalb von zwei Jahren nach dem Inkrafttreten dieses Gesetzes herzustellen...“ und

§ 18 Abs. 3... Das Gesetz tritt drei Monate nach seiner Verkündung in Kraft. ...

(Verkündung des Gesetzes am 06.07.2012)

---

[1] Behörde für Justiz und Gleichstellung, www.hamburg.de/justizbehoerde/
[2] Finanzbehörde, www.hamburg.de/finanzbehoerde/
[3] Kulturbehörde (insb. Staatsarchiv), www.hamburg.de/kulturbehoerde/

3.1.2 Terminziel „Produktionsbereitschaft für Veröffentlichung“

Anforderung

Im Mai 2014 müssen die Komponenten für die manuelle und automatisierte Zulieferung von Informationsobjekten zum Informationsregister für die produktive Nutzung bereitstehen.

D.h. insbesondere die unter 3.2.2 beschriebenen Prozesse sowie der zentrale Informationsspeicher müssen zur Zulieferung und Informationsaufnahme bereitstehen.

Begründung

Seit dem 06.10.2012 gemerkte Dokumente müssen bis zum 06.10.2014 in das Informationsregister eingepflegt werden.

3.1.3 Terminziel „Test- und Schulungsbereitschaft“

Anforderung

Im ersten Quartal 2014 soll die erste Version in den Testbetrieb gehen und als Grundlage für das Produktivsystem dienen. Eine Ansicht der Oberfläche zur Gestaltung der Schulungsunterlagen wird bis spätestens Februar 2014 benötigt.

Begründung

Diese Anforderung resultiert aus der Planvorgabe des FHH-Projektes, u. a. in der Präsentation vom 03. April 2013 („Vorgehensvorschlag zum Thema „Schwärzen“ von Dokumenten“)[4]. Des Weiteren wird zu diesem Zeitpunkt die Anwenderschulung durch das ZAF vorbereitet.

Zudem ist der Zeitplan aus der Meilensteinplanung vom 27.05.2013[5] ersichtlich:

[4] Vgl. Präsentation „Vorgehensvorschlag zum Thema „Schwärzen“ von Dokumenten“, Stand 03. April 2013, Folie 6
[5] Quelle: „Meilensteinplan_HmbTG_FINAL.pdf“, Abruf am 14.06.2013

[redacted]

3.2 Anforderungen an die bereitzustellende IT

Das folgende Kapitel behandelt die Anforderungen an das HmbTG-IT-System. Es gliedert sich in Anforderungen systemübergreifender Art (Kapitel 3.2.1), Anforderungen an die unterschiedlichen Formen der Zulieferung (Kapitel 3.2.2) sowie Anforderungen an Metadaten- und Datenspeicher, Such- und Portalkomponente.

Die Struktur dieses Kapitels richtet sich nach den abstrakten Komponenten einer Grobarchitektur, welche aus der folgenden Abbildung ersichtlich ist.

[redacted]

Gleichlautende Anforderungen können sich an mehreren Stellen wiederfinden. In diesem Fall sind die Anforderungen ggf. durch mehrere, möglicherweise zu koppelnde Komponenten gleichartig zu erfüllen.

3.2.1 Übergreifende Anforderungen an die bereitzustellende IT

Übergreifende Anforderungen beschreiben solche Anforderungen, die das HmbTG-IT-System als Ganzes erfüllen soll.

3.2.1.1 Anforderung „Verfügbarkeit für Informationen Suchen und Abrufen“

Anforderung

Das Gesamtsystem soll, bezogen auf die Geschäftsprozesse „*Informationen suchen* und *abrufen*“, eine Verfügbarkeit von etwa 98% pro Jahr (auf 24/7-Basis) aufweisen.[6]

Die exakten Anforderungen an die Verfügbarkeit werden für alle einzelnen (unabhängig) betreibbaren Komponenten festgelegt, aus denen das Gesamtsystem besteht und die an den entsprechenden Geschäftsprozessen beteiligt sind.

Diese Bausteine umfassen neben den zentral betriebenen Komponenten des HmbTG-IT-Systems auch dezentrale Systeme, insbesondere die Liefersysteme, die über Harvesting von Metadaten oder eine Metasuche verfügbar gemacht werden sollen.

Aus welchen Komponenten mit welchem Aufgabenspektrum das HmbTG-IT-System genau besteht, spezifiziert das Dokument „HmbTG-IT-System: Lösungsarchitektur“.

Die exakten Verfügbarkeiten von Bausteinen werden mit den jeweiligen Betreibern der Komponenten in Abwägung zu den Kosten in Form von Service Level Agreements (SLA) vereinbart. Beispielsweise gibt es für Komponenten, die bei Dataport betrieben werden sollen, gestufte Standard-SLAs des technischen Verfahrensbetriebes.

3.2.1.2 Anforderung „Antwortzeiten“

Anforderung

Die Architektur des HmbTG-IT-Systems ist so zu gestalten, dass Benutzeranfragen in den Dialoganwendungen des Portals innerhalb von einer Sekunde beantwortet werden können. Die Antwort ist dabei nicht näher spezifiziert. Insbesondere wird nicht erwartet, dass innerhalb einer Sekunde das Ergebnis einer umfassenden Suche zur Verfügung steht. Anforderung 3.2.1.4 ist zu beachten.

3.2.1.3 Anforderung „Verfügbarkeit für Zuliefervorgänge“

Anforderung

Das Gesamtsystem soll bezogen auf die Zuliefervorgänge eine Verfügbarkeit von jeweils [redacted] pro Jahr (auf 24/7-Basis) aufweisen.

---

[6] Das bedeutet schlimmstenfalls eine Ausfallzeit von ca. sieben aufeinander folgenden Tagen pro Jahr.

Die exakten Anforderungen an die Verfügbarkeit werden für alle einzelnen (unabhängig) betreibbaren Komponenten festgelegt, aus denen das Gesamtsystem besteht und die an den entsprechenden Geschäftsprozessen beteiligt sind.

Diese Bausteine umfassen neben den zentral betriebenen Komponenten des HmbTG-IT-Systems aber auch dezentrale Systeme, insbesondere die Liefersysteme, die die zentralen Speicherkomponenten beliefern.

Aus welchen Komponenten, mit welchem Aufgabenspektrum, das HmbTG-IT-System genau besteht, spezifiziert das Dokument „HmbTG-IT-System: Lösungsarchitektur".

Die exakten Verfügbarkeiten von Bausteinen werden mit den jeweiligen Betreiber der Komponenten in Abwägung zu den Kosten in Form von Service Level Agreements (SLA) vereinbart. Beispielsweise gibt es für Komponenten, die bei Dataport betrieben werden sollen, gestufte Standard-SLAs des technischen Verfahrensbetriebes.

3.2.1.4 Anforderung „Leistung des Backend-Systems"

Anforderung

Die Architektur des Backend-Systems, bestehend aus zentralem Daten- und Metadatenspeicher sowie den Suchkomponenten, ist so zu dimensionieren, dass die Vorgänge zum Aufbau der Indexstrukturen aller angeschlossenen Liefersysteme in akzeptabler Zeit abgeschlossen werden können. So sollte z. B. sichergestellt sein, dass diese Aufgaben über Nacht oder kontinuierlich auf einem Indexierungsserver parallel zum Produktivsystem durchgeführt werden können. Da die endgültige Anzahl der angeschlossenen Liefersysteme bislang nicht bekannt ist, kann die Anforderung noch nicht detaillierter formuliert werden. Insofern ist Anforderung 3.2.1.5 zu beachten.

3.2.1.5 Anforderung „Skalierbarkeit"

Anforderung

Das System muss sowohl in Bezug auf Performance als auch auf Speicherkapazität möglichst leicht skalierbar sein.

Begründung

Beim HmbTG-IT-System handelt es sich um ein ständig wachsendes System, wodurch sich leicht Lastverschiebungen ergeben können. Auf diese Lastverschiebungen muss möglichst einfach reagiert werden können.

3.2.1.6 Anforderung „Schutz vor Viren und Schadsoftware"

Anforderung

Es muss sichergestellt sein, dass das HmbTG-System vor Viren und Schadsoftware geschützt ist.

Begründung

3.2.2 Zulieferungen

In § 3 Abs. 1 HmbTG werden 15 Informationsgegenstände (z.T. mit weiteren Untergliederungen) benannt, Abs. 2 enthält zwei weitere Gegenstände sowie eine Öffnungsklausel.

Damit sind unterschiedlichste Stellen, die über unterschiedlichste IT-Unterstützung für ihre Arbeit verfügen, durch das HmbTG zur Veröffentlichung dieser Informationsgegenstände verpflichtet.

Um die dazu notwendigen Anpassungen ihrer Verwaltungsabläufe (insbesondere der schon automatisierten) möglichst gering zu halten, muss das HmbTG-IT-System diese Stellen unterstützen. Es soll dazu für verschiedene Arbeitsschritte Funktionalitäten bieten, die leicht in die bisherigen Abläufe der Stellen integrierbar sind.

3.2.2.1 Allgemeine Anforderungen an die Zulieferung

Dieses Unterkapitel befasst sich mit den übergreifenden Anforderungen für die Zulieferung von Informationen zum Informationsregister.

3.2.2.1.1 Anforderung „Bereitstellung einer Transportinfrastruktur für Liefersysteme innerhalb des FHHNET“

Anforderung

Das HmbTG-IT-System stellt eine Infrastruktur bereit, um den Transport der Informationen von den vorgelagerten Liefersystemen in den zentralen Datenspeicher zu gewährleisten. Die Liefersysteme befinden sich innerhalb des FHHNET. Die von den Liefersystemen verwendete Transportinfrastruktur ist nach Möglichkeit wiederzuverwenden. Es ist sicherzustellen, dass das liefernde System eine Empfangsbestätigung vom HmbTG-IT-System erhält, sofern es diese verarbeiten kann.

Begründung

Die Anforderung ergibt sich aus der Notwendigkeit, Daten von angeschlossenen Liefersystemen in das Informationsregister zu übertragen. Ein Transport ist erforderlich, da ein direkter anonymer Zugriff aus dem Internet auf die Fachsysteme in der Regel aus Datenschutz- und Sicherheitsgründen nicht zulässig ist.

3.2.2.1.2 Anforderung „Bereitstellung einer Transportinfrastruktur für externe Stellen“

Anforderung

Das HmbTG-IT-System stellt eine Möglichkeit bereit, die Informationen von Liefersystemen außerhalb des FHHNET an den zentralen Datenspeicher zu übertragen. Es ist sicherzustellen, dass das liefernde System eine Empfangsbestätigung vom HmbTG-IT-System erhält, sofern es diese verarbeiten kann.

Begründung

Die Anforderung ergibt sich aus der Notwendigkeit, Daten von externen Liefersystemen (z.B. aus Beteiligungsunternehmen) von außerhalb des FHHNET in das Informationsregister zu übertragen.

3.2.2.1.3 Anforderung „Bereitstellung einer Indexierungskomponente“

Anforderung

Das HmbTG-IT-System verfügt über eine Komponente zum Aufbau von Indexstrukturen. Die Komponente unterstützt verschiedene Datenformate. Insbesondere wird die Volltextindizierung von Dateien in den Formaten PDF/A und Office Open XML (z. B. Excel-Dateien) unterstützt.

Begründung

Die Recherche in großen Datenbeständen setzt die Verwendung von Indexstrukturen voraus, um die Zugriffspfade zu den einzelnen gespeicherten Objekten zu verkürzen. Nach § 10 Abs. 1 HmbTG sind die Informationen „(…) im Volltext, in elektronischer Form im Informationsregister zu veröffentlichen". Darüber hinaus müssen nach § 10 Abs. 1 HmbTG alle Dokumente „leicht auffindbar (und) maschinell durchsuchbar" sein. Da nicht nur PDF/A-Dokumente, sondern auch strukturierte Daten z.B. im Format Office Open XML enthalten sein werden, muss diese Anforderung unbedingt erfüllt werden.

3.2.2.1.4 Anforderung „Schutz von personenbezogenen Daten sowie Betriebs- und Geschäftsgeheimnissen"

Anforderung

Es muss sichergestellt werden, dass ausschließlich Informationen in das Informationsregister übertragen werden, bei denen gewährleistet ist, dass die Anforderungen des Transparenzgesetzes in Bezug auf die Ausnahmetatbestände §§ 4-7 HmbTG, insb. Schutz personenbezogener Daten und Betriebs- und Geschäftsgeheimnissen, Berücksichtigung finden. Die Einhaltung wird nicht bei der Speicherung im Informationsregister geprüft, sondern durch Maßnahmen in vorgelagerten Prozessschritten gewährleistet.

Begründung

Die Begründung der Anforderung ergibt sich aus den §§ 4-7 HmbTG.

3.2.2.1.5 Anforderung „Versionierung der veröffentlichten Informationen"

Anforderung

Nach § 10 Abs. 7 HmbTG muss „bei Änderung veröffentlichter Informationen (…) neben der Änderung die jeweilige Fassung für jeden Zeitpunkt abrufbar sein". Es wird nicht gefordert, dass die Unterschiede der verschiedenen Versionen gekennzeichnet sein müssen. Das HmbTG-IT-System soll eine Funktionalität bieten, die Beziehungen zwischen verschiedenen Versionen einer Datei herstellt, sofern dies durch technische Maßnahmen in vorgelagerten Prozessschritten unterstützt wird. Als technische Maßnahme gilt z.B. die Kennzeichnung einer Datei als Nachfolgeversion einer bestehenden Datei.

Begründung

Die Begründung der Anforderung ergibt sich aus § 10 Abs. 7 HmbTG „Bei Änderungen veröffentlichter Informationen muss ...Fassung für jeden Zeitpunkt abrufbar sein."

Anmerkung

Eine Historie für veröffentlichte Daten aus Liefersystemen wird im Informationsregister nur abgebildet, wenn das jeweilige Liefersystem diese Historie zur Verfügung stellt.[7]

---

[7] Quelle: Protokoll „Projektmanagementausschuss (PMA) HmbTG", 6. Sitzung (Termin vom 19.04.2013, 10:00 – 13:00 Uhr)

3.2.2.2 Manuelle Zulieferung

Nachfolgendes Kapitel befasst sich mit der manuellen Zulieferung von Informationen zum Informationsregister.

3.2.2.2.1 Allgemeine Anforderungen an die manuelle Zulieferung

In diesem Kapitel werden Anforderungen beschrieben, die für alle manuellen Zulieferungen gelten sollen.

3.2.2.2.1.1 Anforderung „Manuelle Metadatenbearbeitung“

Anforderung

Das HmbTG-IT-System muss eine Funktionalität bieten, die es erlaubt, bei der Zulieferung von Informationsobjekten Metadaten, die nicht automatisch generiert werden sollen oder können (wie z.B. das Veröffentlichungsdatum), in einem unterstützten Dialog (z.B. mittels Auswahllisten) zu erfassen und zu ändern. Einige Metadaten müssen bei der manuellen Veröffentlichung verpflichtend eingegeben werden, damit eine Information im Informationsregister gefunden werden kann. Die Eingabe einiger weiterer Metadaten wird nach derzeitigem Stand optional sein.

Begründung

Die Begründung der Anforderung ergibt sich aus § 10 Abs. 5 HmbTG, nach dem „alle Dokumente (…) leicht auffindbar“ sein müssen.

3.2.2.2.2 Manuelle Zulieferung aus der Kernverwaltung (Veröffentlichungs-Workflow: Dokumente über die E-Akte)

Die folgenden Anforderungen befassen sich mit der Zulieferung von Dokumenten, die im Rahmen der Verwaltungstätigkeit der Kernverwaltung entstehen und gemäß HmbTG einer Veröffentlichungspflicht unterliegen.

3.2.2.2.2.1 Anforderung „Anbindung des Veröffentlichungs-Workflows zur E-Akte“

Anforderung

Der in Hamburg etablierte „E-Akten-Workflow“ (ELDORADO) soll an das Informationsregister angebunden werden, damit Dokumente bei Veröffentlichungsrelevanz gemäß HmbTG ohne „Werkzeugwechsel“ automatisiert im Informationsregister veröffentlicht werden können. Dazu ist die Erweiterung des E-Akten-Workflows notwendig. Der gesamte Prozess zur manuellen Zulieferung von Dokumenten im Anschluss an die E-Akte wird im folgenden Veröffentlichungs-Workflow genannt.

Die detaillierten Anforderungen sind im durch das FHH-Projekt erarbeiteten Lastenheft „Veröffentlichungs-Workflow“ spezifiziert.

Begründung

Für die revisionssichere Archivierung und elektronische Dokumentenverwaltung („E-Akte“) wird in Hamburg das System ELDORADO eingesetzt. Durch Erweiterung des „E-Akten-Workflows“ werden auch die technischen Voraussetzungen geschaffen, bezüglich HmbTG relevante Dokumente gesetzeskonform zu verarbeiten.

3.2.2.2.2.2 Anforderung „Schwärzung“

Anforderung

Das HmbTG-IT-System muss eine Funktionalität bieten, die es Behörden ermöglicht, nicht zur Veröffentlichung geeignete Teile in Dokumenten im Verlauf des Veröffentlichungs-Workflows unkenntlich zu machen. Zu diesem Zweck muss eine Funktionalität geboten werden, die es erlaubt, Textdokumente mit revisionssicher geschwärzten Passagen im PDF/A-Format zu erzeugen.

Begründung

Die Begründung der Anforderung ergibt sich u.a. aus § 4 Abs. 1 HmbTG, nach dem „personenbezogene Daten (…) bei der Veröffentlichung im Informationsregister unkenntlich zu machen“ sind. Dasselbe gilt für andere Ausnahmen, z.B. § 7.

3.2.2.2.2.3 Anforderung „OCR“

Anforderung

Das HmbTG-IT-System muss für den Veröffentlichungs-Workflow eine OCR-Komponente vorsehen, die vor Start des Veröffentlichungs-Workflows aus ELDORADO zugelieferte PDF-Dateien daraufhin überprüft, ob deren Inhalte textbasiert sind. Handelt es sich um gescannte Dateien, bei denen der Inhalt als Bild im PDF vorliegt, muss eine OCR-Erkennung und anschließende Umwandlung in eine textbasierte PDF/A-1 Datei vorgenommen werden.

Handelt es sich bei der übermittelten Datei bereits um ein textbasiertes PDF-Dokument, soll keine OCR-Erkennung stattfinden, um das Aufkommen im OCR-Modul so gering wie möglich zu halten.

Begründung

Bild-PDFs können nach aktuellem Kenntnisstand nicht gemäß Anforderung 3.2.2.2.2.2 (Anforderung „Schwärzung“) verarbeitet werden. Daher müssen sie vorab in ein geeignetes Format überführt werden.

Zudem sind veröffentlichte Dokumente im Volltext durchsuchbar zu machen (siehe Anforderung 3.2.5.6 „Volltextsuche“).

3.2.2.2.3 Manuelle Zulieferung aus der Kernverwaltung („strukturierte Daten“)

Die nachstehenden Anforderungen beschäftigen sich mit der Zulieferung von strukturierten Daten, z.B. im Excel- oder CSV[8]-Format, die nicht über den Veröffentlichungs-Workflow nach der E-Akte eingesteuert werden können.

3.2.2.2.3.1 Anforderung „Veröffentlichungs-Dialoganwendung für strukturierte Datenformate“

Anforderung

Das HmbTG-IT-System soll eine Dialoganwendung umfassen, die es der Kernverwaltung ermöglicht, Daten in Form strukturierter Formate zusammen mit den zugehörigen Metadaten in das Informationsregister einzustellen.

[8] Comma-separated values / Character-separated values

Es wird davon ausgegangen, dass die Daten zuvor gesetzeskonform aufbereitet wurden und u.a. keine personenbezogenen Daten oder Betriebs- und Geschäftsgeheimnisse mehr enthalten.

Die spezifischen Anforderungen an die Veröffentlichungs-Dialoganwendungen werden von Dataport in einem eigenen Dokument beschrieben.

3.2.2.2.4 Manuelle Zulieferung von externen Stellen (z.B. Unternehmen)

Nach § 2 Abs. 3 HmbTG sind auch natürliche und juristische Personen des Privatrechts, soweit sie öffentliche Aufgaben, insbesondere der Daseinsvorsorge, wahrnehmen oder öffentliche Dienstleistungen erbringen und dabei der Kontrolle der FHH oder einer unter ihrer Aufsicht stehenden juristischen Personen des öffentlichen Rechts unterliegen, zur Veröffentlichung im Informationsregister verpflichtet. Aus technischer Sicht unterscheiden sich diese Stellen von der Verwaltung dadurch, dass sie nicht Bestandteil des FHHNet sind und daher über zusätzliche Kanäle an das Informationsregister angebunden werden müssen.

3.2.2.2.4.1 Anforderung „Veröffentlichungs-Dialoganwendung für externe Stellen“

Anforderung

Das HmbTG-IT-System soll eine Dialoganwendung umfassen, die insbesondere externen Stellen die Veröffentlichung von Dokumenten sowie strukturierten Datenformaten (Dateien) im Informationsregister ermöglicht.

Es wird davon ausgegangen, dass die Daten zuvor gesetzeskonform aufbereitet wurden und u. a. keine personenbezogenen Daten oder Geschäftsgeheimnisse mehr enthalten.

Die spezifischen Anforderungen an die Veröffentlichungs-Dialoganwendung werden von Dataport in einem eigenen Dokument beschrieben.

Begründung

Die Anforderung ergibt sich aus der Notwendigkeit, gemäß § 2 Abs. 3 HmbTG Informationen von externen Stellen in das Informationsregister zu übertragen, die nicht über ein angebundenes Liefersystem eingesteuert werden können.

3.2.2.3 Automatisierte Zulieferung

Unter die automatisierte Zulieferung fallen alle Arten der Zulieferung, die ohne manuelle Eingriffe erfolgen und auch keine manuelle Nachbearbeitung der Metadaten vorsehen. Die Einhaltung der gesetzlichen Anforderungen bzgl. des Schutzes personenbezogener Daten sowie von Betriebs- und Geschäftsgeheimnissen wird für jedes Liefersystem in vorgelagerten Entscheidungsprozessen geprüft und kann daher bei der Anbindung vorausgesetzt werden.

3.2.2.3.1 Allgemeine Anforderungen an die automatisierte Zulieferung

In diesem Kapitel werden Anforderungen beschrieben, die alle automatisierten Zulieferprozesse erfüllen müssen.

3.2.2.3.1.1 Anforderung „Metadaten-Mapping“

Anforderung

Das HmbTG-IT-System muss eine Funktionalität bieten, die die Metadatenschemata eines Liefersystems auf das Metadatenmodell des HmbTG-IT-Systems abbildet.

Begründung

3.2.2.3.2 Anbindung von Systemen durch dezentrale Informationshaltung (über Metasuche)

Die folgenden Anforderungen beschreiben die Anbindung von Liefersystemen, die über eigene Such- und Datenhaltungsmechanismen verfügen.

3.2.2.3.2.1 Anforderung „Zugriff auf verteilt gespeicherte Informationen mittels Metasuche“

Anforderung

Das Informationsregister soll verteilte (u.a. bei den Liefersystemen angesiedelte) Informationsspeicher logisch zusammenfassen können. Das HmbTG-IT-System stellt Komponenten zur Verfügung, um Suchanfragen, die an das Informationsregister gestellt werden, an das jeweilige Liefersystem weiterzuleiten und die zurückgelieferte Antwort zu verarbeiten. Die Komponenten sind so aufgebaut, dass die Anbindung für verschiedene Liefersysteme separat konfigurierbar bzw. programmierbar ist. Dieser Zugriff wird dann benötigt, wenn Liefersysteme nicht indexiert werden können.

3.2.2.3.3 Anbindung von Systemen durch dezentrale Datenhaltung, aber zentrale Metadatenhaltung

Die folgenden Anforderungen beschreiben die Anbindung von Liefersystemen, die ihre Informationen bereits im Internet veröffentlichen, so dass auf diese verwiesen werden kann. Die Systeme verfügen jedoch über keine Suchfunktion, die eine Anbindung an die Portalsuche des Informationsregisters erlaubt.

3.2.2.3.3.1 Anforderung „Auffindbarkeit von dezentral gespeicherten Informationen“

Anforderung

Das Informationsregister soll verteilte (u.a. bei den Liefersystemen angesiedelte) Informationsspeicher logisch zusammenfassen können. Das HmbTG-IT-System stellt Komponenten zur Verfügung, um auf die dezentral gespeicherten Informationen zugreifen zu können. Die Metadaten werden im Informationsregister hinterlegt und ermöglichen das Auffinden der Informationen über die Suchfunktion des Informationsregisters. Die Komponenten sind so aufgebaut, dass die Anbindung für verschiedene Liefersysteme separat konfigurierbar bzw. programmierbar ist.

Begründung

Nach § 10 Abs. 1 HmbTG sind die Informationen „(…) im Volltext, in elektronischer Form im Informationsregister zu veröffentlichen“. Darüber hinaus müssen nach § 10 Abs. 1 HmbTG alle Dokumente „leicht auffindbar (und) maschinell durchsuchbar“ sein.

Nach § 2 Abs. 6 HmbTG ist das „Informationsregister (…) ein zentral zu führendes, elektronisches und allgemein zugängliches Register, das alle nach diesem Gesetz veröffentlichten Informationen enthält.“

Hinweis

Zur Indexerstellung kann es erforderlich sein, größere Datenmengen heranzuziehen und temporär zu speichern, z. B. durch Download von Volltextdokumenten zur Volltextindizierung. Dies ist bei der Dimensionierung der Komponenten sowie des Speicherplatzes zu beachten.

3.2.2.3.3.2 Anforderung „Anbindung von Informationsportalen über ihre Metadaten“

Anforderung

Als Abgrenzung zu Anforderung 3.2.2.3.3.1 soll das HmbTG-IT-System keine Suchfunktion für Liefersysteme bereitstellen, wenn diese als eigenständige Portale den Zugriff auf die gespeicherten Informationen selbst steuern und im Informationsregister keine eindeutigen Treffer erzeugen. Im Informationsregister werden jedoch Metadaten zu diesen Liefersystemen hinterlegt, so dass bei einer passenden Suchanfrage Verweise auf die Liefersysteme erzeugt werden.

Begründung

Die Begründung der Anforderung ergibt sich aus § 10 Abs. 5 HmbTG, nach dem „alle Dokumente (…) leicht auffindbar“ sein müssen.

3.2.2.3.4 Anbindung von Systemen durch zentrale Informationshaltung

Die folgenden Anforderungen beschreiben die Anbindung von Liefersystemen, die ihre Informationen nicht im Internet veröffentlichen und daher auch über keine öffentlich zugängliche Suchfunktion verfügen, die eine Anbindung an die Metasuche des Informationsregisters erlaubt. Das fachliche Liefersystem muss seine Daten inklusive Metadaten an einer Schnittstelle bereitstellen.

3.2.2.3.4.1 Anforderung „Dateibasierte Zulieferung“

Anforderung

Von den angeschlossenen Liefersystemen werden die Informationen dateibasiert geliefert. Zu jeder Dateilieferung gehören passende Metadaten.

Einige Metadaten müssen bei der Veröffentlichung verpflichtend hinterlegt werden.

3.2.3 Zentraler Metadatenspeicher

Der zentrale Metadatenspeicher beschreibt eine abstrakte Architekturkomponente, die sich mit der Speicherung von Metadaten gemäß dem vereinbarten Metadatenmodell und dazugehörigen Funktionalitäten befasst. Die Dokumentation des Metadatenmodells ist zu beachten. Nachfolgendes Kapitel befasst sich mit den Anforderungen an eine solche Komponente.

3.2.3.1 Anforderung „Automatisierte Metadatenanreicherung durch den Empfänger“

Anforderung

Das HmbTG-IT-System muss eine Funktionalität bieten, die bestimmte automatisch erzeugbare Metadaten (z.B. Veröffentlichungszeitpunkt, Absender, ...) zu einem Informationssatz im Zuge des Veröffentlichungsvorganges generiert und dem veröffentlichten Informationssatz zuordnet.

Einige Metadaten müssen bei der Veröffentlichung verpflichtend hinterlegt werden.

3.2.3.2 Anforderung „Automatisierte Zulieferung“

Anforderung

Das HmbTG-IT-System soll Funktionalitäten bieten, die es ermöglichen, IT-Systeme als so genannte Liefersysteme für eine Zulieferung von Informationen an das zentrale Informationsregister anzubinden.

Über diese Anbindung der Liefersysteme sollen alle Arten von Informationsobjekten und/oder zugehörige Metadaten zu Informationsobjekten automatisiert an das Informationsregister übergeben werden können.

In diesem Sinne *automatisiert zuliefern* sollen sowohl die Liefersysteme der Kernverwaltungen und externen Stellen als auch der ebenfalls zum HmbTG-IT-System gehörige *Veröffentlichungs-Workflow* und weitere *Veröffentlichungsdialoganwendungen* (siehe Kap. 3.2.2.2.3 und Kap. 3.2.2.2.4). Mit letzteren sollen externe Stellen Dokumente veröffentlichen bzw. die Kernverwaltung selbst E-Akten-fremde, strukturierte Daten in Form von Dateien (wie z.B. Excel, CSV etc.) veröffentlichen können.

Zur detaillierten Darstellung der Zulieferungen siehe Kap. 3.2.2 „Zulieferungen“.

3.2.3.3 Anforderung „Erleichterung der automatisierten Zulieferung“

Anforderung

Das HmbTG-IT-System soll Funktionalitäten bieten, die die Anbindung zuliefernder Systeme an die in 3.2.3.2 beschriebene Systemfunktionalität erleichtert.

Dazu gehören insbesondere Funktionalitäten, die es erleichtern bestimmte Sicherheitsmaßnahmen zu ergreifen und spezifische netztechnische Verbindungen zu nutzen.

Die Grundsätze von Integrität und Authentizität müssen gewahrt bleiben. Dies ist durch technische Richtlinien umzusetzen, die sich in der Architektur (Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.**) wiederfinden.

3.2.3.4 Anforderung „Protokollierung von Veröffentlichungsvorgängen“

Anforderung

Das HmbTG-IT-System soll geeignete Protokollierungsmechanismen zur Verfügung stellen:

- Lieferung/Änderung von Daten und Metadaten: Wer, was, wann
- Lieferung/Änderung von Dokumenten und Metadaten: Wer, was, wann
- Korrektur von veröffentlichten Daten und Metadaten: Wer, was, wann
- Korrektur von veröffentlichen Dokumenten und Metadaten: Wer, was , wann
- Löschen von veröffentlichten Daten und Metadaten: Wer, was, wann
- Löschen von veröffentlichen Dokumenten und Metadaten: Wer, was , wann

3.2.3.5 Anforderung „Quittierung von Veröffentlichungsvorgängen“

Anforderung

Das HmbTG-IT-System soll geeignete Quittierungsmechanismen zur Verfügung stellen:

- Lieferung/Änderung von Daten und Metadaten: Wer, was, wann

- Lieferung/Änderung von Dokumenten und Metadaten: Wer, was, wann
- Ggf. Korrektur von veröffentlichten Daten und Metadaten: Wer, was, wann
- Ggf. Korrektur von veröffentlichen Dokumenten und Metadaten: Wer, was , wann
- Ggf. Löschen von veröffentlichten Daten und Metadaten: Wer, was, wann
- Ggf. Löschen von veröffentlichen Dokumenten und Metadaten: Wer, was , wann

3.2.3.6 Anforderung „Metadatensuche - relational“

Anforderung

Informationen im Informationsregister sollen durch relationale Suchanfragen auf die Metadaten-Daten des Informationsregisters gefunden werden können.

Begründung

§10 Abs. 1 ...leicht auffindbar, maschinell durchsuchbar...

3.2.3.7 Anforderung „Metadatenvolltextsuche“

Anforderung

Informationen im Informationsregister sollen durch Volltextsuchanfragen auf die Metadaten des Informationsregisters gefunden werden können.

Begründung

§10 Abs. 1 ...leicht auffindbar, maschinell durchsuchbar...

3.2.3.8 Anforderung „Mindestens zehn Jahre Aufbewahrung“

Anforderung

Alle Informationen, die im Informationsregister veröffentlicht wurden, müssen für mindestens zehn Jahre gefunden und abgerufen werden können. Die gilt unabhängig davon, welcher der verteilten Datenspeicher des Informationsregisters genutzt wird.

Begründung

§ 10 Abs. 6 (6) „Die Informationen im Informationsregister müssen mindestens zehn Jahre nach ihrer letzten Änderung vorgehalten werden.“

3.2.3.9 Anforderung „Korrektur“

Anforderung

Das HmbTG-IT-System muss eine Funktionalität bieten, die es ermöglicht, fehlerhafte Metadaten zu einer Information im zentralen (Meta-)Datenspeicher zu korrigieren.

3.2.3.10 Anforderung „manuelle Löschung im Fehlerfall (Metadaten)“

Anforderung

Das HmbTG-IT-System muss eine Funktionalität bieten, Daten/Dokumente und Metadaten zu einer veröffentlichten Information im Fehlerfall aus dem zentralen Metadaten- und ggf. dem zentralen Datenspeicher zu löschen. Dabei soll sichergestellt werden, dass die Löschung keine Inkonsistenzen in anderen Komponenten verursacht. Wird ein Metadatensatz gelöscht, zu dem

eine Ressource im zentralen Datenspeicher liegt, so muss diese Ressource auch gelöscht werden. Liegen Ressourcen zu einem gelöschten Metadatensatz in dezentralen Speichern, so erfolgt darauf kein Zugriff.

3.2.3.11 Anforderung „Löschung“ (nach gesetzlicher Veröffentlichungsfrist)

Anforderung

Das HmbTG-IT-System soll eine Funktionalität bieten, die realisiert, dass im Informationsregister veröffentlichte Informationen zu einem Zeitpunkt, der >= zehn Jahre nach dem Veröffentlichungstermin liegt, automatisch gelöscht werden (das heißt, dass die Information anschließend weder durch Suchen gefunden noch anderweitig abgerufen werden kann).

Das Standardvorgehen ist die Löschung nach einem Verbleib von zehn Jahren im Informationsregister. Eine verlängerte Veröffentlichungsdauer kann über ein Datum oder über einen Wert „ohne Enddatum“ definiert werden. Dabei soll sichergestellt werden, dass die Löschung keine Inkonsistenzen in anderen Komponenten verursacht. Bei der automatischen Löschung soll evtl. ein zeitlicher Puffer eingeplant werden.

Begründung

§ 10 Abs. 6

3.2.3.12 Anforderung „Einbindung in andere Open-Data-Portale“

Anforderung

Das HmbTG-IT-System soll Funktionalitäten bieten, über die andere Portale aus dem Open Data/Open Government Kontext auf den Datenbestand des Informationsregisters zugreifen können. Dabei ist insbesondere auf die Einhaltung geltender Standards zu achten.

Begründung

Das Open Data Portal Hamburg mit den dazugehörigen Prozessen soll in das im Rahmen des HmbTG neu zu konzipierende Informationsregister integriert werden, um möglichst keine redundanten Strukturen aufzubauen.[9]

Dazu gehört es, die bestehenden Möglichkeiten des Datenabrufes (Harvesting) für andere Portale (insbesondere das Open Data Portal des Bundes govdata.de) zu erhalten.

Im bisherigen Open-Data-Portal wird das Produkt *CKAN* bereits verwendet und entsprechende Harvesting-Module anderer Open-Data-Portale sind bereits im Einsatz. Die zugrunde liegende API stellt der CKAN zur Verfügung.

[9] Vgl. Projektmanagementausschuss (PMA) HmbTG, 2. Sitzung vom 09.11.2012, 10:00 – 11:00 Uhr

3.2.4 Zentraler Datenspeicher

Der zentrale Datenspeicher beschreibt eine abstrakte Architekturkomponente, die mit der Speicherung der eigentlichen Daten der Informationsgegenstände betraut ist. Nachfolgend werden entsprechende Anforderungen spezifiziert.

3.2.4.1 Anforderung „Zentrale Speicherbarkeit von Informationen“

Anforderung

Das Informationsregister soll über eine Funktionalität verfügen, zugelieferte Informationen persistent zentral zu speichern.

Begründung

Nicht alle im HmbTG aufgeführten Liefersysteme und Behörden können die Anforderungen insbesondere zu den Aspekten 3.2.1.1 („Anforderung „Verfügbarkeit für Informationen Suchen und Abrufen“), 3.2.1.3 („Anforderung „Verfügbarkeit für Zuliefervorgänge“), 3.2.4.8 („Anforderung „Mindestens zehn Jahre Aufbewahrung“) und 3.2.3.4 (Anforderung „Protokollierung von Veröffentlichungsvorgängen“) mit eigenen dezentralen Systemen selbst erfüllen.

3.2.4.2 Anforderung „Automatisierte Zulieferung“

Anforderung

Das HmbTG-IT-System soll Funktionalitäten bieten, die es ermöglichen, andere IT-Systeme als so genannte Liefersysteme für eine Zulieferung von Informationen an das zentrale Informationsregister anzubinden.

Über diese Anbindung der Liefersysteme sollen alle Arten von Informationsobjekten und/oder zugehörige Metadaten zu Informationsobjekten automatisiert an das Informationsregister übergeben werden können.

In diesem Sinne *automatisiert zuliefern* sollen sowohl die Liefersysteme der Kernverwaltungen und externen Stellen als auch der ebenfalls zum HmbTG-IT-System gehörige *Veröffentlichungs-Workflow* und weitere *Veröffentlichungsdialoganwendungen* (siehe Kap. 3.2.2.2.3 und Kap. 3.2.2.2.4). Mit letzteren sollen externe Stellen Dokumente veröffentlichen bzw. die Kernverwaltung selbst E-Akten-fremde, strukturierte Daten in Form von Dateien (wie z.B. Excel, CSV, etc.) veröffentlichen können.

Zur detaillierten Darstellung der Zulieferungen siehe Kap. 3.2.2 „Zulieferungen“.

3.2.4.3 Anforderung „Erleichterung der automatisierten Zulieferung“

Anforderung

Das HmbTG-IT-System soll Funktionalitäten bieten, die die Anbindung zuliefernder Systeme an die in 3.2.4.2 beschriebene Systemfunktionalität erleichtert.

Dazu gehören insbesondere Funktionalitäten, die es erleichtern, bestimmte Sicherheitsmaßnahmen zu ergreifen und spezifische netztechnische Verbindungen zu nutzen.

Die Grundsätze von Integrität und Authentizität müssen gewahrt bleiben. Dies ist durch technische Richtlinien umzusetzen, die sich in der Architektur („HmbTG-IT-System: Lösungsarchitektur“) wiederfinden.

3.2.4.4 Anforderung „Protokollierung von Veröffentlichungsvorgängen“

Anforderung

Das HmbTG-IT-System soll geeignete Protokollierungsmechanismen zur Verfügung stellen:

- Lieferung/Änderung von Daten und Metadaten: Wer, was, wann
- Lieferung/Änderung von Dokumenten und Metadaten: Wer, was, wann
- Korrektur von veröffentlichten Daten und Metadaten: Wer, was, wann
- Korrektur von veröffentlichen Dokumenten und Metadaten: Wer, was , wann
- Löschen von veröffentlichten Daten und Metadaten: Wer, was, wann
- Löschen von veröffentlichen Dokumenten und Metadaten: Wer, was , wann

3.2.4.5 Anforderung „Quittierung von Veröffentlichungsvorgängen“

Anforderung

Das HmbTG-IT-System soll geeignete Quittierungsmechanismen zur Verfügung stellen:

- Lieferung/Änderung von Daten und Metadaten: Wer, was, wann
- Lieferung/Änderung von Dokumenten und Metadaten: Wer, was, wann
- Ggf. Korrektur von veröffentlichten Daten und Metadaten: Wer, was, wann
- Ggf. Korrektur von veröffentlichen Dokumenten und Metadaten: Wer, was , wann
- Ggf. Löschen von veröffentlichten Daten und Metadaten: Wer, was, wann
- Ggf. Löschen von veröffentlichen Dokumenten und Metadaten: Wer, was , wann

3.2.4.6 Anforderung „Dateiformate“

Anforderung

Es wird eine definierte Liste von Dateiformaten geben, die für Informationsobjekte im Informationsregister empfohlen werden (z.B. PDF/A).

Begründung

§ 10 Abs. 5

3.2.4.7 Anforderung „Dateiformate und exotische Dateiformate“

Anforderung

Das Informationsregister des HmbTG-IT-System soll auch „exotische“ Dateiformate verarbeiten können, d.h. solche, die nicht in einem Format gemäß der in 3.2.4.6 geforderten Liste formatiert sind.

Ist es einem anzubindenden Liefersystem nicht möglich, Datei-Exporte in einem akzeptablen Format für die Zulieferung an das Informationsregister zu realisieren, soll es eine Funktion geben, die es ermöglicht, den Output dieses Systems in empfohlene Dateiformate umzuformatieren (z.B. Word-Dateien in PDF/A-1). Diese Funktionalität ist optional und nicht zwingend im 1. Release vorzusehen.

Begründung

Vermerk Datenformate HmbTG vom 5.2.2013[10].

Bürgerschaftsdrucksache 20/4466, Seite 21: „Alle Prozesse der Verwaltung sind so zu gestalten, dass bei der Veröffentlichung der Daten kein unnötiger Aufwand entsteht."

3.2.4.8 Anforderung „Mindestens zehn Jahre Aufbewahrung"

Anforderung

Alle Informationen, die im Informationsregister veröffentlicht wurden, müssen bei geeigneter Suche mindestens zehn Jahre gefunden und abgerufen werden können. Die gilt unabhängig davon, welcher der verteilten Datenspeicher des Informationsregisters genutzt wird.

Begründung

§ 10 Abs. 6 (6) „Die Informationen im Informationsregister müssen mindestens zehn Jahre nach ihrer letzten Änderung vorgehalten werden."

3.2.4.9 Anforderung „Korrektur"

Anforderung

Das HmbTG-IT-System muss eine Funktionalität bieten, die es ermöglicht, fehlerhafte Metadaten zu einer Information im zentralen (Meta-)Datenspeicher zu korrigieren.

3.2.4.10 Anforderung „manuelle Löschung im Fehlerfall (Datenspeicher)"

Anforderung

Das HmbTG-IT-System muss eine Funktionalität bieten, Daten/Dokumente und Metadaten zu einer veröffentlichten Information im Fehlerfall aus dem zentralen Metadaten- und ggf. dem zentralen Datenspeicher zu löschen. Dabei soll sichergestellt werden, dass die Löschung keine Inkonsistenzen in anderen Komponenten verursacht.

Wird eine Ressource im zentralen Datenspeicher gelöscht, muss der zugehörige Metadatensatz gelöscht werden, falls keine weiteren zu diesem Metadatensatz zugehörigen Ressourcen vorliegen. Bleibt der Metadatensatz wegen weiterer zugehöriger Ressourcen bestehen, muss darin der Link zur gelöschten Ressource entfernt werden.

3.2.4.11 Anforderung „Löschung" (nach gesetzlicher Veröffentlichungsfrist)

Anforderung

Das HmbTG-IT-System soll eine Funktionalität bieten, die realisiert, dass im Informationsregister veröffentlichte Informationen zu einem Zeitpunkt, der >= zehn Jahre nach dem Veröffentlichungstermin liegt, automatisch gelöscht werden (das heißt, dass die Information anschließend weder durch Suchen gefunden noch anderweitig abgerufen werden kann).

---

[10] http://fhhportal.stadt.hamburg.de/websites/1021/Projekt/Unterlagen%20Beirat/2.%20Sitzung%20am%2007.02.2012/Vermerk%20-%20Datenformate%20FB_Februar2013.pdf

Das Standardvorgehen ist die Löschung nach einem Verbleib von zehn Jahren im Informationsregister. Eine verlängerte Veröffentlichungsdauer kann über ein Datum oder über einen Wert „ohne Enddatum“ definiert werden. Dabei soll sichergestellt werden, dass die Löschung keine Inkonsistenzen in anderen Komponenten verursacht. Bei der automatischen Löschung soll evtl. ein zeitlicher Puffer eingeplant werden.

Begründung

§ 10 Abs. 6

3.2.5 Suchkomponente für verteilte Informationshaltung

Nachfolgendes Kapitel benennt die Anforderungen an die Suchkomponente für die verteilte Informationshaltung des HmbTG-IT-Systems.

3.2.5.1 Anforderung „Metasuche“

Wie unter 3.2.2.3.2.1 Anforderung „Zugriff auf verteilt gespeicherte Informationen mittels Metasuche“ gefordert, soll das Informationsregister verteilte Datenhaltung unterstützen. D.h. sowohl die Informationsobjekte, als auch die zugehörigen Metadaten können verteilt an mehreren Orten gespeichert sein (insbesondere auch in externen Liefersystemen).

Anforderung

Die in den folgenden Kapiteln 3.2.5.2, 3.2.5.3, 3.2.5.4, 3.2.5.5, 3.2.5.6 und 3.2.5.7 gestellten Anforderungen an die Suchmechanismen sollen auch auf externe Teile des Informationsspeichers des Informationsregisters wirken oder genauere Teilsuchen an diese delegieren.

Begründung

Um der Anforderung 3.2.6.1 Anforderung „Zentraler Zugriffspunkt“ zu genügen, sind Suchmechanismen nötig, die diese verteilte Datenhaltung - für Suchende nicht wahrnehmbar - kompensieren. Suchen sollen auf Metaebene („oberhalb“ des realen Speicherortes) durchgeführt werden können.

3.2.5.2 Anforderung „Kurzsuche“

Anforderung

Das HmbTG-IT-System soll die Möglichkeit einer „Kurzsuche“ bieten.

Die Kurzsuche ermöglicht die Angabe von Suchbegriffen in einem Einzeleingabefeld und daraufhin eine Suche über alle Metadatenfelder und alle Liefersysteme.

Begründung

Die Infrastrukturen für das Open Data Portal sollen in das neu zu konzipierende Informationsregister im Rahmen des HmbTG integriert und möglichst keine redundanten

Strukturen aufgebaut werden.[11] D.h., dass auch ein analoger Funktionsumfang vorgesehen werden muss.

§ 2 Abs.6

3.2.5.3 Anforderung „Erweiterte Suche“

Anforderung

Das HmbTG-IT-System soll die Möglichkeit einer „Erweiterten Suche“ bieten.

Erweiterte Suche bedeutet, dass die Angabe von Suchbegriffen in unterschiedlichen Feldern möglich sein soll und eine Suche in genau diesen Feldern und ggf. in ausgewählten Liefersystemen erfolgt.

3.2.5.4 Anforderung "Filterfunktionalität"

Anforderung

Das Portal soll eine facettierte Suche in Form von definierten Filteroptionen anbieten, mit denen es möglich ist, die Ergebnisse einer vorangegangenen Kurz- oder erweiterten Suche schrittweise einzuschränken.

3.2.5.5 Anforderung „Metadatensuche - relational“

Anforderung

Informationen im Informationsregister, sollen durch relationale Suchanfragen auf die Metadaten des Informationsregisters gefunden werden können.

Begründung

§10 Abs. 1 ...leicht auffindbar, maschinell durchsuchbar...

3.2.5.6 Anforderung „Volltextsuche“

Anforderung

Informationen im Informationsregister, die in Textform vorliegen, sollen unabhängig von ihrer Formatierung im Volltext durchsuchbar gemacht werden.

Begründung

§10 Abs. 1 ...im Volltext, in elektronischer Form ...leicht auffindbar, maschinell durchsuchbar und druckbar...“

3.2.5.7 Anforderung „Metadatenvolltextsuche“

Anforderung

---

[11] Vgl. Projektmanagementausschuss (PMA) HmbTG, 2. Sitzung vom 09.11.2012, 10:00 – 11:00 Uhr

Informationen im Informationsregister, sollen durch Volltextsuchanfragen auf die Metadaten des Informationsregisters gefunden werden können

Begründung

§10 Abs. 1 ...leicht auffindbar, maschinell durchsuchbar...

3.2.5.8 Anforderung „Maschinelle Durchsuchbarkeit“

Anforderung

Während Suchmöglichkeiten auf dem Portal direkt unter Berücksichtigung von Software-Benutzungsaspekten (Usability) angeboten werden sollen, sind für die Datenexporte dokumentierte Schnittstellen (in Form einer API) bereit zu stellen.

Begründung:

Das Portal soll verschiedene Nutzergruppen ansprechen. Es sind sowohl maschinenlesbare Daten als auch Benutzeroberflächen für den interessierten Bürger bereit zu stellen.

3.2.5.9 Anforderung „Suchergebnisse in Kurzansicht“

Anforderung

Das HmbTG-IT-System soll Suchergebnisse in Kurzansicht darstellen können. D.h. in der Ergebnisliste nach einer Suche soll zu jedem Treffer ein zu definierender Teilausschnitt des Metadatensets des jeweiligen Ergebnisses dargestellt werden.

3.2.5.10 Anforderung „Suchergebnisse in Langansicht“

Anforderung

Das HmbTG-IT-System soll Suchergebnisse in Langansicht darstellen können. Wird ein Treffer aus einer Ergebnisliste ausgewählt, soll dieser in einer detaillierten Ansicht mit einem erweiterten noch zu definierenden Set der zugehörigen Metadaten inkl. Hyperlinks zu den Informationsobjekten (zum Download) dargestellt werden.

3.2.5.11 Anforderung „Abrufbarkeit fortgeschriebener Informationen“

Anforderung

Informationen, die durch Veröffentlichung von Fortschreibungen (3.2.2.1.5 „Anforderung „Versionierung der veröffentlichten Informationen““) einer Information historisch werden, also nicht mehr aktuell sind, müssen weiterhin zum Abruf angeboten werden, wenn eine aktuellere Fortschreibung im Suchergebnis auftaucht.

Begründung

§ 10 Abs. 7 Bei Änderungen veröffentlichter Informationen muss ...Fassung für jeden Zeitpunkt abrufbar sein.

Anmerkung

Eine Historie für veröffentlichte Daten aus Liefersystemen wird im Informationsregister nur abgebildet, wenn das jeweilige Liefersystem diese Historie zur Verfügung stellt.[12]

3.2.6 Portal

Nachfolgendes Kapitel beschreibt Anforderungen an ein für das HmbTG-IT-System zu konzipierendes Portal. Zu den speziellen Anforderungen an die Suchkomponente des Portals siehe Kap. 3.2.5.

3.2.6.1 Anforderung „Zentraler Zugriffspunkt“

Anforderung

Der Zugang zu allen Informationen des Informationsregisters soll an einem zentralen Zugriffspunkt möglich sein.

Begründung

§ 2 Abs. 6

3.2.6.2 Anforderung „Anonyme Nutzung“

Anforderung

Der Zugang zu den Informationen des Informationsregisters muss anonym möglich sein.

Begründung

§ 10 Abs. 4

3.2.6.3 Anforderung "Kostenlose Nutzung"

Anforderung

Der Zugang zu den Informationen des Informationsregisters muss kostenlos möglich sein.

Begründung

§ 10 Abs. 4

3.2.6.4 Anforderung „Format abrufbarer Information“ (keine zusätzliche Visualisierung)

Anforderung

Informationen sollen im gleichen Format abgerufenen werden können, in dem sie dem Informationsregister zugeliefert werden. Eine darüber hinausgehende Aufbereitung (z.B.

[12] Quelle: Protokoll „Projektmanagementausschuss (PMA) HmbTG“, 6. Sitzung (Termin vom 19.04.2013, 10:00 – 13:00 Uhr)

Visualisierung) ist nicht erforderlich. Die Anforderungen zu den Formaten bei der Veröffentlichung sind spezifiziert unter 3.2.4.6.

3.2.6.5 Anforderung „Protokollierung von Informationssuchen und -abrufen“

Anforderung

Das HmbTG-IT-System soll geeignete Protokollierungsmechanismen zur Verfügung stellen, um den Datenzugriff zu analysieren.

- Zur Analyse der Zugriffszahlen auf das Portal
- Zur Analyse der Suchanfragen insgesamt sowie nach bestimmten Informationsobjekten oder Gruppen von Informationsobjekten
- Zur Analyse der Zugriffszahlen auf Detaildarstellungen für bestimmte Informationsobjekte oder Gruppen von Informationsobjekten
- Zur Analyse der Downloadzugriffe

Begründung

Nach Projektabschluss soll eine Evaluation erfolgen.

Ergebnisse der Analysen sollen zudem für die Fachliche Leitstelle Informationsregister einen Anhaltspunkt darstellen, um die Weiterentwicklung des Portals an den Bedürfnissen der Zielgruppen ausrichten zu können.

3.2.6.6 Anforderung „Orientierung an Layout und Usability von hamburg.de“

Anforderung

Die Nutzeroberfläche des Informationsregisters soll sich in das Design von hamburg.de einfügen. Die Architektur des HmbTG-IT-Systems soll die Einbindung des Informationsregisters in das bestehende hamburg.de Portal berücksichtigen.

Die konkrete Ausgestaltung erfolgt in einem gesonderten Konzept, das vom FHH-Projekt erstellt wird.

Das Konzept zur Ausgestaltung wird durch Analyse der Anforderungen unterschiedlicher Nutzergruppen, wie z.B. interessierte Bürger, die Dokumente bzgl. ihres Stadtteils oder IT-Firmen, die die zur Verfügung gestellten Daten für neue Web- oder Mobilanwendungen verwenden wollen, ermittelt. Daher wird die Nutzbarkeit des Portals im Wesentlichen durch Suchmöglichkeiten und Exportschnittstellen für Dokumente und Daten gewährleistet werden.

3.3 Rahmenvorgaben

Nachfolgendes Kapitel behandelt Rahmenvorgaben, die ebenfalls für das HmbTG-IT-System Berücksichtigung finden müssen.

3.3.1 Quellen

Neben den unter 3.2 aufgeführten „direkten“ Anforderungen an das HmbTG-IT-System sind insbesondere die folgenden allgemeinen Vorgaben für IT-Systeme in Hamburg zu beachten.

3.3.1.1 Hamburgisches Datenschutzgesetz

Insbesondere zu beachten sind hier die Hinweise zur Risikoanalyse und Vorabkontrolle nach dem Hamburgischen Datenschutzgesetz.

3.3.1.2 Rahmenanforderungen an Software- und Systemarchitektur

Zu beachten sind die von der Finanzbehörde vorgegebenen „Rahmenanforderungen an Software- und Systemarchitektur" in der gültigen Version (aktuell V3.0 vom 27.06.2012).

3.3.2 Sicherheitsanforderungen

3.3.2.1 Anforderung „Vorverarbeitung bei jedem Schutzbedarf"

Anforderung

Damit die realisierte Funktionalität für die Vorverarbeitung der Quellinformation, bis zur Veröffentlichungsfähigkeit von *allen* Stellen – unabhängig vom speziellen Schutzbedarf für ihre Quellinformationen – möglichst leicht genutzt werden kann, ist diese *so* zu realisieren, dass auch bei ihrem Einsatz im Rahmen der Anpassung der Verwaltungsabläufe das erforderliche Sicherheitsniveau ohne großen Zusatzaufwand erhalten werden kann. D.h. bei Konzeption dieser Funktionalität sind auch Bereiche zu berücksichtigen, in denen hoher Schutzbedarf besteht, unter der Voraussetzung, dass dies mit vertretbarem Aufwand möglich ist.

Begründung

Die zur Veröffentlichung verpflichteten Stellen haben bei der Verarbeitung ihrer Quellinformationen im Allgemeinen einen unterschiedlich hohen Schutzbedarf.

Falls die datenverarbeitenden Stellen bei der Vorverarbeitung von Quellinformation eine Funktionalität des HmbTG-IT-Systems nutzen wollen, sind die datenverarbeitenden Stellen nach Hamburgischen Datenschutzgesetz zur Risikoanalyse und Vorabkontrolle verpflichtet. Sie müssen begründen, dass der Einsatz dieser Funktionalität den vorhandenen Schutzbedarf nicht gefährdet.

Wenn die genutzten Module für sich betrachtet hohen Sicherheitskriterien entsprechen, erleichtert das i.d.R. diese Argumentationen.

3.3.2.2 Anforderung „Authentizitäts- und Integritätsschutz"

Anforderung

Bei der Konzeption des Informationsregisters sind Sicherheitsmaßnahmen vorzusehen, die die Verletzung von Authentizität und Integrität der veröffentlichten Informationen verhindern.

Begründung

Informationen, die im Informationsregister veröffentlicht wurden, bleiben in der Verantwortung der Stelle die veröffentlicht hat. Speicherung und das Anbieten dieser Informationen geschieht im Rahmen von Auftragsdatenverarbeitung.

Für im Informationsregister veröffentlichte Informationen besteht ein deutlich geringerer Schutzbedarf als für die Informationen, aus denen sie durch Schwärzung oder Filterung erzeugt wurden. Es besteht insbesondere keine Anforderung bzgl. Vertraulichkeit, da diese Informationen definitionsgemäß für jedermann anonym und frei zugänglich sein sollen.

Obwohl es sich um Daten handelt, die frei zugänglich sind, haben die veröffentlichen Stellen ein Interesse daran, dass Authentizität (Datenursprung/Sicherstellung des Absenders) und Integrität (Korrektheit/Unversehrtheit von Daten) gewahrt bleiben.

3.3.3 Anforderungen an Software- und Systemarchitektur

Sofern nicht ausdrücklich in den folgenden Absätzen etwas Abweichendes gefordert wird, soll das System die als „Rahmenanforderungen an Software- und Systemarchitektur" in der gültigen Version (aktuell V3.0 vom 27.06.2012) festgelegten Anforderungen erfüllen. Bei Abweichungen von diesen Anforderungen sind diese explizit zu erwähnen und ausführlich zu begründen.

3.3.3.1 Spezielle Vorgaben Softwarearchitektur

3.3.3.2 Spezielle Vorgaben Systemarchitektur

Die zum Einsatz kommenden Komponenten für u.a. Indizierung, Metasuche, Datenspeicher und Webportal werden voraussichtlich als getrennte Komponenten zum Einsatz kommen, die auf unterschiedlichen Servern laufen. Die Kommunikation zwischen diesen Komponenten, z.B. über Port-Schnittstellen zwischen den Servern, muss daher gewährleistet sein.

3.3.4 Anforderungen Lösungsarchitektur

3.3.4.1 Nutzung von vorhandenen Lösungen und Infrastrukturen

Um Realisierungs-, Einführungs- aber insbesondere auch Betriebskosten zu minimieren, sollen nach Möglichkeit bereits existierende bzw. betriebene Infrastrukturkomponenten mitgenutzt werden.

Insbesondere soll möglichst auf bereits existierenden Standards und Lösungen der Hamburger Verwaltung aufgebaut werden - nicht zuletzt um den Aufwand (z.B. auch für Schulungsmaßnahmen) zu minimieren.

Dies bezieht sich insbesondere auf

- Open Data-Infrastrukturen (Open Data Portal ,CKAN,...)
- E-Akten-Workflow zur Archivierung in ELDORADO
- Solr-Index für die Indexierung
- „IPS Library" für die Metasuche

3.3.5 Wirtschaftlichkeit

Auch wenn die zuvor genannten Rahmenbedingungen nicht zuletzt zur Erfüllung des Ziels Wirtschaftlichkeit gesetzt wurden, soll der bei der Konzeption des zu schaffenden IT-Systems verbleibende Spielraum optimal genutzt werden, um ein kostenminimales System zu schaffen.

dataport

HmbTG-IT-System

Lösungsarchitektur

Version 1.0 /Zustand (in Bearbeitung/vorgelegt/fertig gestellt)

Datum letzte Änderung 26.09.2013

Änderungsverzeichnis

Änderung			Geänderte Kapitel	Beschreibung der Änderung	Autor
Nr.	Datum	Version			
1	08.08.2013	0.0.1	alle	Ersterstellung	Dataport
2	09.08.2013	0.0.2		Liveänderungen aus Workshop am 9.8. übertragen	Dataport
3	11.08.2013	0.0.3	3	Tabellen um Leerspalten ergänzt Untergliederungsebenen getauscht	Dataport
4	12.08.2013	branch	3.1 und 3.3	Konkrete Architektur	HITeC/Dataport
5	13.08.2013	branch	3.2	Konkrete Architektur	Dataport
6	13.08.2013	0.0.6		branches zusammengeführt	Dataport
7	15.08.2013	0.0.7	3.1	CKAN Architektur	HITeC
8	19.08.2013	0.0.8	alle außer 3.1	Form und Bezug zu Anforderungspapier	Dataport
9	19.08.2013	0.0.9	3.1 und 2.2.1	Suchanforderungen und CKAN Architektur	HITeC
10	20.08.2013	0.0.10	alle außer 3.1	Redaktionelles und Übersicht konkrete Architektur ergänzt, Konsistenz von 2.2 zur Anforderungsspezifikation, Systemarchitektur ZSp-MDB	Dataport
11	20.08.2013	0.0.11	Alle	Redaktionelles, Erklärungstext	HITeC
12	21.08.2013	0.1.0	alle	Redaktionelles, Bilderklärungen	Dataport
13	23.08.2013	0.9.1	alle	Ergänzungstexte Einleitung, Prozesse, Komponenten	Dataport, [redacted]
14	26-27.08.2013	0.9.2	alle	Anpassung Struktur und Übernahme Inhalte aus Vorgängerversion	FB
15	30.08.2013	1.0	alle	Endredaktion	FB
16	19.09.2013	1.0	alle	Ergänzungen auf Basis der Rückmeldung von [redacted]	Dataport
17	26.09.2013	1.0	2.5.2	Update der Komponenten für	FB

				den Veröffentlichungs-WF (Upload)	

Prüfverzeichnis

Die folgende Tabelle zeigt einen Überblick über alle Prüfungen, die das vorliegende Dokument in den Zustand „fertig gestellt“ überführt haben.

Datum	Geprüfte Version	Anmerkungen	Prüfer

Inhaltsverzeichnis

1 Einleitung 6
1.1 Zweck des Dokuments 6
1.2 Bezug zur Anforderungsspezifikation 7

2 Aufbau der Lösungsarchitektur und abgeleitete IT-Komponenten für HmbTG 7
2.1 Vorgehensweise 7
2.2 Anforderungsszenario 7
2.3 Abstrakte Lösungsarchitektur 8
2.3.1 Zuständigkeiten der Teilsysteme 10
2.4 Konkrete Lösungsarchitektur 10
2.5 Dezentrale und zentrale Liefersysteme 11
2.5.1 Veröffentlichungs-Workflow (ELDORADO) 11
2.5.1.1 Kurzbeschreibung „Veröffentlichungs-Workflow (ELDORADO)“ 11
2.5.1.2 Systemarchitektur „Veröffentlichungs-Workflow (ELDORADO)“ 11
2.5.1.3 Softwarearchitektur „Veröffentlichungs-Workflow (ELDORADO)“ 13
2.5.1.4 Anforderungen „Veröffentlichungs-Workflow (ELDORADO)“ 13
2.5.2 Veröffentlichungs-Workflow (Upload) 13
2.5.2.1 Kurzbeschreibung „Veröffentlichungs-Workflow (Upload)“ 13
2.5.2.2 Systemarchitektur „Veröffentlichungs-Workflow (Upload)“ 14
2.5.2.3 Softwarearchitektur „Veröffentlichungs-Workflow (Upload)“ 15
2.5.2.4 Anforderungen „Veröffentlichungs-Workflow (Upload)“ 16
2.5.3 Automatisierte Zulieferung 16
2.5.3.1 „Systemarchitektur „Automatisierte Zulieferung“ 16
2.5.3.2 Softwarearchitektur „Automatisierte Zulieferung“ 19
2.5.3.3 Anforderungen „Automatisierte Zulieferung“ 19
2.6 Zentrales Speichersystem (ZSp-MDB) 19
2.6.1 Kurzbeschreibung „Zentrales Speichersystem (ZSp-MDB)“ 19
2.6.2 Systemarchitektur „Zentrales Speichersystem (ZSp-MDB)“ 19
2.6.3 Softwarearchitektur „Zentrales Speichersystem (ZSp-MDB)“ 20
2.6.4 Anforderungen „Zentrales Speichersystem (ZSp-MDB)“ 21
2.7 Suchvorbereitungs- und Suchsystemkomponenten 21
2.7.1 Kurzbeschreibung „Suchvorbereitungs- und Suchsystemkomponenten“ 21
2.7.2 Systemarchitektur „Suchvorbereitungs- und Suchsystemkomponenten“ 22
2.7.3 Softwarearchitektur „Suchvorbereitungs- und Suchsystemkomponenten“ 24
2.7.4 Anforderungen „Suchvorbereitungs- und Suchsystemkomponenten“ 25
2.7.5 Portal 25
2.8 Zusammenwirken der Teilsysteme untereinander und mit externen Systemen 26
2.8.1 Abstrakte Schnittstellen 28
2.8.2 Zusammenwirken bei Aufbereitung von Veröffentlichungen für Suchen („Harvesting“) 29
2.8.3 Zusammenwirken bei zentraler Speicherung 30
2.8.4 Zusammenwirken bei Herausgabe von Veröffentlichungen aus verteilten Speichern 31
2.8.5 Zusammenwirken mit externen Systemen und Komponenten 32

3 Überblick über Komponenten und Angebote HmbTG-System 33
3.1 Prozesse und Komponenten im Überblick 33
3.2 Dataport Angebotserstellung für die Komponenten im Überblick 34

4 Anhang 35
4.1 Realisierungsansätze und deren Bewertungen 35
4.1.1 Umsetzung „Veröffentlichungs-Workflow (ELDORADO)“ 35
4.1.2 Umsetzung der Schnittstellen „Veröffentlichungs-Workflow (ELDORADO)“ 36

4.1.3 Umsetzung „Veröffentlichungs-Workflow (Upload)“ 36
4.1.4 Umsetzung der Schnittstellen „Veröffentlichungs-Workflow (Upload)“ 37
4.1.5 Umsetzung „Automatisierte Zulieferung“ 38
4.1.6 Umsetzung „Zentrales Speichersystem (ZSp-MDB)“ 39
4.1.8 Umsetzung „Such- und Suchvorbereitungskomponente“ 43
4.1.9 Umsetzung der Schnittstellen „Such- und Suchvorbereitungskomponente“ 47
4.2 Metadaten aus ELDORADO 47
4.3 Metadaten-Modell für Eingabemasken 48
4.4 Abkürzungsverzeichnis 49

1 Einleitung

Am 13. Juni 2012 ist das Hamburgische Transparenzgesetz (HmbTG) von der Hamburgischen Bürgerschaft beschlossen worden und am 06. Oktober 2012 in Kraft getreten. Zweck des Gesetzes ist es, durch ein umfassendes Informationsrecht die in der Verwaltung der FHH (eingeschlossen die im § 2 HmbTG definierten juristischen Personen des Privatrechts) vorhandenen Informationen unter Wahrung des Schutzes personenbezogener Daten unmittelbar der Allgemeinheit zugänglich zu machen. Ziel ist es, über die bestehenden Informationsmöglichkeiten hinaus die demokratische Meinungs- und Willensbildung zu fördern und eine Kontrolle des staatlichen Handelns zu ermöglichen.

Kern des HmbTG ist die Schaffung eines zentralen Informations- und Suchportals (folgend Informationsregister genannt). Auf dem Hamburger OpenData-Portal (daten.hamburg.de) stehen zwar seit Februar 2013 bereits eine Vielzahl von Informationen zur Verfügung. Hierbei handelt es sich allerdings überwiegend um sog. strukturierte Daten (wie bspw. Geodaten), welche lediglich verlinkt werden.

Das Informationsregister soll jeden Auskunftssuchenden in die Lage versetzen, die im Gesetz genannten Informationsgegenstände einzusehen. Dazu müssen verschiedene Informationsquellen (dezentrale und zentrale Bestände) verknüpft und über eine Suchfunktion zugänglich gemacht werden.

In Kapitel 2 werden der genaue Aufbau der Lösungsarchitektur sowie die sich daraus ergebenden IT-Komponenten beschrieben. Dabei werden auch die mit den IT-Komponenten in Beziehung stehenden Prozesse erläutert.

In Kapitel 3 werden die Komponenten noch einmal in einer Übersicht zusammengefasst und die dafür zu entwickelnden Angebote seitens Dataport aufgeführt. Im Anhang sind alle aus dem Lastenheft (siehe 1.2) enthaltenen Anforderungen aufgeführt. Diese wurden möglichen Realisierungsansätzen gegenübergestellt und bewertet.

1.1 Zweck des Dokuments

Das Dokument beschreibt, welcher Lösungsarchitekturansatz bei der Umsetzung des HmbTG-IT-Systems verfolgt wird. Die in diesem Dokument beschriebene Lösungsarchitektur wurde von einer Expertengruppe, die aus Vertretern der Finanzbehörde, von HITeC und Dataport gebildet wurde, gemeinsam entwickelt.

Die abstrakte Lösungsarchitektur (Kap. 2.3) stellt dar, aus welchen Teilsystemen das HmbTG-IT-System bestehen soll und wie diese zusammenwirken. Insbesondere wird definiert, wie die gestellten Anforderungen an das Gesamtsystem umgesetzt und auf die Teilsysteme verteilt werden sollen.

Die konkrete Lösungsarchitektur (Kap. 2.4) stellt dar, welche konkrete Basis für die Realisierung der abstrakten Lösungsarchitektur gewählt wird. Die Konkretisierung bezieht sich sowohl auf Softwarebestandteile als auch auf die Systemplattformen auf denen diese betrieben werden sollen. Dargelegt wird dabei, mit welchem Ansatz die dem abstrakten Teilsystem zugewiesenen Anforderungen auf der gewählten konkreten Basis realisiert werden sollen.

Die vollständige konkrete Lösungsarchitektur umfasst alle zu realisierenden Anforderungen, die Identifikation eines Realisierungsansatzes, seine Ausarbeitung und die Überprüfung der Umsetzbarkeit.

1.2 Bezug zur Anforderungsspezifikation

Der Lösungsarchitektur wurde das Lastenheft „Anforderungen HmbTG-IT-System.docx“ Version 1.0 vom 21.08.2013 zu Grunde gelegt. Es befindet sich auf dem SharePoint des FHH-Projektes. Zur weiteren Spezifikation der Anforderungen werden zu jedem Prozess bzw. Komponente einzelne Lastenhefte erstellt:

Lastenheft Veröffentlichungs-Workflow (Eldorado)

Lastenheft Veröffentlichungs-Workflow (Upload) Interne/Externe

2 Aufbau der Lösungsarchitektur und abgeleitete IT-Komponenten für HmbTG

2.1 Vorgehensweise

In diesem Kapitel werden der genaue Aufbau der Lösungsarchitektur sowie die sich daraus ergebenden IT-Komponenten beschrieben. Basierend auf der Anforderungsspezifikation (siehe Abschnitt 1.2) wird zunächst in Abschnitt 2.2 das Anforderungsszenario vorgestellt. Dieses wird dann in Abschnitt 2.3 zu einer abstrakten Lösungsarchitektur weiterentwickelt, welche insbesondere die benötigten IT-Teilkomponenten identifiziert. Zur Verdeutlichung dieser Vorgehensweise wird in Abschnitt 2.3.1 dargestellt, welche IT-Komponenten der abstrakten Lösungsarchitektur welche Komponenten und Aspekte des Anforderungsszenarios abdecken. In Abschnitt 2.4 wird schließlich die konkrete Lösungsarchitektur vorgestellt. Danach werden in den Abschnitten die einzelnen IT-Komponenten detailliert beschrieben. Hierbei wird dann u.a. auch darauf eingegangen, in welcher Beziehung die IT-Komponenten zu den Veröffentlichungs-Workflows stehen.

2.2 Anforderungsszenario

Die Abbildung 1 zeigt das Anforderungsszenario, das auf Basis der Anforderungsspezifikation entstanden ist. So sind für die Verfügbarmachung der relevanten Informationen nach HmbTG verschiedene Informationsquellen relevant. Dies sind Fachsysteme, die Informationen entweder automatisiert (z.B. Geodaten) oder manuell durch eine Person (z.B. über ELDORADO) zuliefern können. Ein Teil der in HmbTG genannten Informationsgegenstände werden über ELDORADO in das Informationsregister überführt. Dieser Prozess der manuellen Zulieferung von Dokumenten von intern, d.h. aus der FHH, wird „Veröffentlichungs-Workflow (ELDORADO)“ genannt. Er ist in der nachfolgenden Abbildung mit der Abschnittsnummer 2.5.1 markiert.

Es gibt darüber hinaus noch manuelle Zulieferungen strukturierter Daten aus der Kernverwaltung und von Extern. Zudem können auch Externe Dokumente zuliefern. Alle diese drei Möglichkeiten werden „Veröffentlichungs-Workflow (Upload)“ genannt, da sie zusammen betrachtet werden können. Er ist in der nachfolgenden Abbildung mit der Abschnittsnummer 2.5.2 markiert.

Neben den manuellen Zulieferungen, bei denen immer eine Person beteiligt ist, gibt es auch automatisierte Zulieferungen, bei denen Informationen aus Fachsystemen automatisiert kommen können, wie bspw. bei BACom. Dieser Prozess wird „Automatisierte Zulieferung“ genannt.

Die Zulieferung der Daten hängt maßgeblich von den Metadaten ab. Bei den manuellen Zulieferungen („Veröffentlichungs-Workflow (ELDORADO)“ bzw. „Veröffentlichungs-Workflow (UPLOAD)“) werden die Metadaten größtenteils durch die zuliefernde Person mitgegeben. Bei automatisierten Zulieferungen muss gewährleistet werden, dass die Metadaten mitgeliefert werden und für die Suche zur Verfügung stehen. Die Prozesse der automatisierten Zulieferung sowie die Sicherstellung

der Metadaten ist in der Abbildung unter der Abschnittsnummer 2.5.3 zu finden und in diesem Abschnitt erläutert.

Darüber hinaus wird es einen zentralen Speicher geben, der alle Informationsgegenstände vorhält, die nicht dezentral unter den Anforderungen des Hamburger Transparenzgesetzes gespeichert werden können. Die Speicherkomponente wird unter der Abschnittsnummer 2.6 visualisiert.

Zudem wird auch ein Portal benötigt, über welches die Nutzer Zugang zu den veröffentlichten Informationsgegenständen bekommen. Hier ist insbesondere die Suchfunktionalität von zentraler Bedeutung (siehe Abschnitt 2.7). Auf die Anforderungen des Portals wird im Abschnitt 2.7.5 eingegangen.

2.3 Abstrakte Lösungsarchitektur

Die abstrakte Lösungsarchitektur stellt dar, aus welchen Teilsystemen das HmbTG-IT-System bestehen soll. Insbesondere wird definiert, wie die Umsetzung der an das Gesamtsystem gestellten Anforderungen auf die Teilsysteme verteilt wird und wie die Teilsysteme zusammenwirken.

Abbildung 2: Abstrakte Teilsysteme des Informationsregisters.

Wie aus Abbildung 2 ersichtlich, setzt sich die abstrakte Lösungsarchitektur des HmbTG-IT-Systems aus drei lose miteinander gekoppelten Typen von Teilsystemen zusammen:

1) „Suchvorbereitungssystem und Suchsystem",
2) „Zentrales Speichersystem (ZSp-MDB)" sowie
3) „Dezentrale und zentrale Liefersysteme".

Während es für die ersten beiden Teilsysteme genau ein Szenario gibt (**Suchvorbereitungssystem und Suchsystem:** CKAN/Harvesting für Automatisierte Zulieferungen; **Zentrales Speichersystem:** Speicherung von Daten und Dokumenten, die im Liefersystem nicht konform zu den Vorgaben des Hamburger Transparenzgesetztes gespeichert werden), gibt es beim letzten mehrere. Die Szenarien des dritten Typs sind hier der Veröffentlichungs-Workflow (ELDORADO) sowie der Veröffentlichungs-Workflow (Uploads). Während diese beiden Workflows manuelle Veröffentlichungsprozesse beschreiben, gibt es daneben auch automatisierte Zulieferungen, die ebenfalls Repräsentanten des Teilsystems „Dezentrale und zentrale Liefersysteme" sind. Grundlegend lassen sich bzgl. der Persistenz bei automatisierter Zulieferung folgende zwei Fälle unterscheiden:

- Selbstpersistierende Liefersysteme, d.h. diese Systeme erfüllen selbst die Anforderung der Persistenz von Informationen (Entitäten und Metadaten).
- Nicht-Selbstpersistierende Liefersysteme, d.h. diese Systeme speichern die Daten und Dokumente nicht konform zum Hamburger Transparenzgesetz (Dauer: mindestens 10 Jahre, Historisierung etc.).

Alle in der Anforderungsspezifikation (siehe Abschnitt 1.2) aufgestellten Anforderungen an das HmbTG-IT-System werden von den lose gekoppelten Teilsystemen im Zusammenspiel erfüllt. Dabei werden die Zuständigkeiten für die Erfüllung der Anforderungen, wie in (Abbildung 3: Zuständigkeit der Teilsysteme) dargestellt, beschrieben und auf die Teilsysteme verteilt („separation of concerns").

2.3.1 Zuständigkeiten der Teilsysteme

Abbildung 3 verdeutlicht die Zuständigkeiten der Teilsysteme, indem es diese in Zusammenhang zu dem Anwendungsszenario bringt. Demzufolge bringt die Abbildung 3 die vorangegangenen Abbildung 1 und Abbildung 2 zusammen.

2.4 Konkrete Lösungsarchitektur

Die konkrete Lösungsarchitektur stellt dar, welche konkrete Basis für die Realisierung der abstrakten Lösungsarchitektur gewählt wird. Die Konkretisierung bezieht sich sowohl auf Softwarebestandteile als auch auf die Systemplattformen, auf denen diese betrieben werden sollen. Dargelegt wird dabei, mit welchem Ansatz die dem abstrakten Teilsystem zugewiesenen Anforderungen auf der gewählten konkreten Basis realisiert werden sollen.

Abbildung 4 zeigt, welche der in den folgenden Unterabschnitten beschriebenen konkreten Softwarebestandteile welches abstrakte Teilsystem realisieren.

[redacted]

2.5 Dezentrale und zentrale Liefersysteme

In den folgenden Unterabschnitten wird das Teilsystem „Dezentrale und zentrale Liefersysteme“ beschrieben. Dabei werden in den Abschnitten 2.5.1 und 2.5.2 jeweils die beiden Varianten des Veröffentlichungs-Workflows (manuelle Zulieferungen intern und extern) dargestellt, während der Abschnitt 2.5.3 die automatisierten Zulieferungen beschreibt.

2.5.1 Veröffentlichungs-Workflow (ELDORADO)

2.5.1.1 Kurzbeschreibung „Veröffentlichungs-Workflow (ELDORADO)“

Der Veröffentlichungs-Workflow (ELDORADO) ist für das manuelle Hochladen von internen Dokumenten in das Informationsregister zuständig.

2.5.1.2 Systemarchitektur „Veröffentlichungs-Workflow (ELDORADO)“

In der folgenden Abbildung 5 ist der Prozessablauf visualisiert, wie von dem E-Akte-System ELDORADO Informationsgegenstände in das Informationsregister gelangen:

[redacted]

Der Sachbearbeiter (SB) hat in seinem Arbeitsablauf ein Dokument, welches er in ELDORADO ablegt. Er vermutet, dass die Inhalte des Dokuments transparenzgesetzrelevant sind. SB verfügt das Dokument nach ELDORADO und vergibt dabei ein definiertes Schlagwort. Ein Duplikat des Dokuments liegt dann in einem Filesystem einschließlich ausgewählter Metadaten aus ELDORADO (in XML-Format) vor, auf das der SharePoint-Workflow zugreifen kann. Die Metadaten sind im Anhang unter Abschnitt 4.2 erläutert.

Liegt das Dokument in ELDORADO nicht als zeichenbasiertes PDF-A sondern bildbasiert (z.B. TIFF) im PDF-Mantel vor, erfolgt eine automatisierte Texterkennung mittels Optical Character Recognition (OCR). Anschließend wird das Dokument in PDF-A umgewandelt. Für den OCR-Vorgang soll die Lösung Kofax genutzt werden.

Ist in den Metadaten bei einem Informationsgegenstand bei der Übergabe an den Veröffentlichungs-Workflow das Schlagwort „_HmbTG_Verträge der Daseinsvorsorge“ oder „_HmbTG_Verträge von öffentlich. Interesse“ enthalten, wird vor Beginn des SharePoint-Workflows im Hintergrund eine Kopie von Duplikat und Metadatensatz gemacht und automatisiert an das Projekt Herakles übergeben. Dieser Vorgang wird über einen Webservice erfolgen, den das Projekt HERAKLES zurzeit auf Basis der Dokumente und Metadaten aus ELDORADO definiert.

Im nächsten Schritt erfolgt für relevante Dokumente durch SB eine rechtliche Prüfung. Geprüft wird auf personenbezogene Daten, die nicht veröffentlicht werden dürfen sowie ob Betriebs- und Geschäftsgeheimnisse enthalten sind. Die Konsequenz aus einer positiven Prüfung wäre die Schwärzung. Wie für jeden Workflow-Schritt soll für die Prüfung ggf. mehrere Delegationsebenen ermöglicht werden. Folglich können auch zusätzliche Personen in dem Prozess eingebunden werden. SB oder ein neuer Workflow-Inhaber (Delegation) markiert dazu im PDF die zu schwärzenden Stellen.

Dadurch können vertrauliche Inhalte gelöscht werden. Wird diese Aufgabe delegiert, kann der neue Workflow-Inhaber die Eingaben sehen und Kommentare lesen sowie von einer Markierung zur nächsten springen. Nach der Markierung setzt er die Aufgabe auf erledigt.

SB erhält zur Freigabe für das Informationsregister einen Link, über den das Ergebnis geprüft und freigegeben werden kann. Erst mit Übertragung des Dokuments an das Informationsregister werden die markierten Inhalte über die Serverkomponente Redax Enterprise Server geschwärzt und nicht zu veröffentlichende Metadaten und Kommentare entfernt. Das Duplikat mit zugehörigen Metadaten aus dem Filesystem wird dann gelöscht. Eine Protokolldatei sowie das eingestellte geschwärzte Dokument werden in ELDORADO zum Originaldokument gespeichert.

Verweis: Eine detaillierte Beschreibung dieses Veröffentlichungs-Workflows findet sich im Lastenheft Veröffentlichungs-Workflow (ELDORADO).

2.5.1.3 Softwarearchitektur „Veröffentlichungs-Workflow (ELDORADO)“

Die Workflowkomponente zur Umsetzung der einzelnen Bearbeitungsschritte soll auf Basis des HIM-Workflows umgesetzt werden. Eine detaillierte Beschreibung der Schnittstellen zu ELDORADO, Kofax, Redax und dem Informationsregister ist in Arbeit.

Die detaillierte Verteilung dieser einzelnen Arbeitspakete und damit die Festlegung auf die Infrastruktur erfolgt bei einem Termin mit Vertretern von HIM, Dataport und dem Umsetzungsprojekt am 03.09.2013.

2.5.1.4 Anforderungen „Veröffentlichungs-Workflow (ELDORADO)“

Die Anforderungen werden durch die Komponenten erfüllt. Zu den einzelnen Anforderungen siehe Abschnitt 4.1.1 Umsetzung „Veröffentlichungs-Workflow (ELDORADO)“.

2.5.2 Veröffentlichungs-Workflow (Upload)

2.5.2.1 Kurzbeschreibung „Veröffentlichungs-Workflow (Upload)“

Für die Veröffentlichung strukturierter Daten von Intern sowie für die Veröffentlichung von Dokumenten und strukturierten Daten von Extern müssen weitere Veröffentlichungs-Workflows (Upload) bereitgestellt werden. Der Ablauf ist schematisch für die Veröffentlichung von intern und extern gleich und wird in 2.5.2.2 dargestellt.

2.5.2.2 Systemarchitektur „Veröffentlichungs-Workflow (Upload)“

[redacted]

Der Zulieferer (das „Liefersystem“) ist eine natürliche Person, wenn die veröffentlichende Stelle intern (d.h. innerhalb der FHH) ist. Bei externen veröffentlichenden Stellen ist es dagegen eine juristische Person.

Der Zulieferer muss gewährleisten, dass nur den Ansprüchen des Transparenzgesetztes konforme Dateien zur Veröffentlichung eingereicht werden. Des Weiteren müssen strukturierte Daten unabhängig von ihrer Herkunft in Dateiformaten veröffentlicht werden, die auf verbreiteten und frei zugänglichen Standards basieren (z.B. PDF, Word, Excel etc.) und durch herstellerunabhängige Organisationen unterstützt und gepflegt werden. Zudem müssen die Metadaten dieser Datei frei von personenbezogenen Daten sein. Für die Veröffentlichung externer Dokumente gilt, dass diese bereits geschwärzt und ebenfalls frei von personenbezogenen Metadaten sein müssen.

Im ersten Schritt erfolgt nun das Einreichen der konformen Datei. Hierzu muss das Liefersystem authentifiziert werden, um sicherzustellen, dass es dazu berechtigt ist und um protokollieren zu können, welche Datei von welchem Liefersystem eingestellt wurde. Da der Aspekt der Authentifizierung sowohl davon abhängt, ob das Liefersystem von Intern oder Extern kommt und welche Technologie zur Umsetzung der Veröffentlichungsdialogs zum Einsatz kommt, wird dies separat am Ende dieses Unterabschnitt thematisiert.

Grundsätzlich sind folgende Aspekte beim Einstellen von Dateien zu beachten:

- Dokumente sind vom Liefersystem im Format PDF/A einzustellen. Dies wird, soweit möglich, von der Software-Komponente hinter dem Veröffentlichungsdialog kontrolliert und sichergestellt.
- Strukturierte Daten sind in Dateiformaten einzustellen, die auf verbreiteten und frei zugänglichen Standards basieren und durch herstellerunabhängige Organisationen unterstützt und gepflegt werden, wobei PDF/A für strukturierte Daten nicht genutzt werden sollte.
- Pro Vorgang können nur Dateien eingestellt werden, die insgesamt eine Größe von [redacted] nicht überschreiten

Im zweiten Schritt öffnet sich eine Eingabemaske zur Eingabe der Metadaten. Darin befindet sich u.a. auch das Metadatum „Veröffentlichende Stelle“, welches den Lieferanten identifiziert, um im Zweifel Verursacher nicht ausreichend geschwärzter Dokumente identifizieren zu können. In entsprechender Weise sind Pflichtfelder in der Eingabemaske hinterlegt.

Nach Eintragung der Metadaten werden im dritten Schritt die eingestellten Daten von der Software-Komponente hinter dem Veröffentlichungsdialog in ein passendes Format transformiert und an den zentralen Speicher übergeben. Die Definition für das Format dieser Schnittstelle ist in Arbeit und soll sich an bereits festgelegten Schnittstellen zum Informationsregister orientieren (z.B. der Schnittstelle aus dem Veröffentlichungs-Workflow ELDORADO in das Informationsregister). Der Lieferant erhält eine Quittung über die erfolgreiche Übertragung des Dokuments an das Informationsregister.

2.5.2.3 Softwarearchitektur „Veröffentlichungs-Workflow (Upload)“

Veröffentlichungs-Workflow (Upload) für interne Zulieferer – Lösung mit SharePoint

Die Realisierung soll mit einer reduzierten Version des Veröffentlichungs-Workflows (ELDORADO) auf Basis des HIM-Workflow-Systems, ohne Integration zu Herakles, Redax, OCR und ELDORADO erfolgen. Da keine Übergabe von Dokumenten aus ELDORADO erfolgt, wird ein manueller Einstiegspunkt integriert (z.B. als Uploadfunktion oder per E-Mail an ein Postfach). Darüber hinaus muss sicherstellt sein, dass intern keine Dateien, die eigentlich über ELDORADO veröffentlicht werden müssen hochgeladen werden (z.B. PDF, Word).

Eine Ausarbeitung der Anforderungen an diesen zusätzlichen Workflow ist aktuell in Arbeit und soll bis Anfang KW 40 fertiggestellt sein.

Es werden zwei Risiken gesehen:

1. Die Anforderung, dass die dem Informationsregister zu Verfügung gestellten Dokumente immer entsprechend den rechtlichen Vorgaben geschwärzt sind, muss hier der Nutzer Rechnung tragen. Dazu müssen entsprechende organisatorische Vorgaben erarbeitet werden.
2. Es muss sichergestellt werden, dass bei der Nutzung des Veröffentlichungs-Workflow (Upload) intern keine Umgehung des Veröffentlichungs-Workflows (ELDORADO) erfolgt. Es besteht das Risiko, dass Mitarbeiter ELDORADO umgehen und die Dokumente direkt über den hier erläuterten alternativen Weg hochladen. Dazu müssen entsprechende Vorgaben erarbeitet werden. Außerdem soll der Workflow einen Upload der Formate PDF, DOC. DOCX, PPT und PPTX mit Fehlermeldung abweisen.

Veröffentlichungs-Workflow (Upload) für externe Zulieferer – Lösung mit dem Hamburg-Gateway:

Der Nutzer muss sich am HamburgGateway autorisieren und somit einen Account mit Passwort und Benutzernamen anlegen. Um eine Verbindung zum Einstellen von Dokumenten herstellen zu können und auch später im Prozess eine Rückmeldung über das erfolgreiche Einstellen des Dokuments geben zu können, benötigt der Lieferant einen Account und ein Postfach im Gateway. Hat sich der Lieferant erfolgreich autorisiert, erfolgt im nächsten Schritt die Auswahl der Datei zum Upload und die Erfassung der notwendigen Metadaten, sowie die Freigabe und anschließend die Übertragung an das Informationsregister.

Zu klären ist, welche Sicherheitsstufe für die Accounts zuliefernder externer Stellen gewählt werden muss.

Veröffentlichungs-Workflow (Upload) für externe Zulieferer – Lösung mit ZUVEX und SharePoint:

Alternativ zu der Gateway-Lösung wird momentan die Realisierung über einen weiteren SharePoint-Workflow auf Basis der HIM-Workflow-Technologie mit Zugang von Extern über ZUVEX-Accounts geprüft. Es besteht die Hoffnung, dass der reduzierte Veröffentlichungs-

Workflow (Upload) für intern mit einigen Erweiterungen zu diesem Zwecke verwendet werden kann.

Verweis: Eine detaillierte Beschreibung des Veröffentlichungs-Workflows (Upload) für externe Zulieferer wird derzeit in einem Lastenheft erarbeitet und mit dem Bereich FB 175 abgestimmt. Nach der daraus folgenden Beurteilung und Aufwandsschätzung soll sehr zeitnah die Entscheidung für eine der beiden Varianten getroffen werden.

Die Tendenz im Projekt zeigt in Richtung einer Umsetzung mit SharePoint und ZUVEX, weil in diesem Fall alle anfallenden Workflows für eine manuelle Übertragung von Inhalten an das Informationsregister über die gleiche Infrastruktur gelöst werden könnten.

Zur Gegenüberstellung der beiden beschriebenen Varianten liegt eine Dokumentation auf dem Projekt-SharePoint.

2.5.2.4 Anforderungen „Veröffentlichungs-Workflow (Upload)“

Die Anforderungen werden durch die dargestellten Komponenten erfüllt.

2.5.3 Automatisierte Zulieferung

2.5.3.1 „Systemarchitektur „Automatisierte Zulieferung“

Die Liefersysteme der automatisierten Zulieferungen sind aufgrund unterschiedlicher Informationsinhaltstypen und verschiedenem Veröffentlichungsgrad, Zugriffsmöglichkeiten sowie diverser Daten- und Veröffentlichungsstandards sehr heterogen. Zur Gewährleistung der Informationsverfügbarkeit müssen diese entsprechend unterschiedlich angebunden werden.

Die Anforderungen, die ein Liefersystem idealerweise aufweist, sind: Erreichbarkeit über das Internet, vorhandene Suchfunktion und eine dem Hamburger Transparenzgesetz entsprechende Datenhaltung. Die Liefersysteme werden in der folgenden Abbildung je nach Anforderungen, die sie abdecken, in Kategorien eingeteilt und mit entsprechenden Lösungen versehen, um die Erreichbarkeit auch der referenzierten Informationsobjekte zu gewährleisten.

[redacted]

Selbst-persistierende Systeme halten die Daten und Dokumente entsprechend der vom Transparenzgesetz vorgeschriebenen Anforderungen (bspw. Datenhaltung 10 Jahre, Historisierung etc.) vor. Nicht-persistierende Systeme folglich gewährleisten dies nicht. Die Daten aus letzteren müs-

sen samt Metadaten in den zentralen Speicher gezogen werden. Selbst-persistierende Daten müssen folglich nicht im zentralen Speicher vorgehalten werden.

Selbst-persistierende Liefersysteme:

Diese Liefersysteme werden nun in zwei Unterkategorien eingeteilt. Das **Liefersystem 1** der selbst-persistierenden Liefersysteme steht im Internet und besitzt eine Volltextsuche, besitzt aber nicht das im Informationsregister genutzte Metadatenmodell. Aufgrund dessen muss dafür gesorgt werden, dass die Suche im Informationsregister unter der Verwendung der im Metadatenmodell festgelegten Begriffe mit den Begriffen des Metadatenmodells des Liefersystems 1 funktioniert. Zum Beispiel wird bei der Suche im Informationsregister unter dem Begriff Titel gesucht, im Liefersystem 1 wird dieser Begriff aber unter Thema geführt. Um diese „Übersetzung" zu gewährleisten, wird das System IPS (Information-Portal-Suite) genutzt. Der Sucheintrag aus dem Informationsregister wird zur IPS geschickt. Die IPS fragt mit der „Übersetzung" an das Liefersystem an und übermittelt die Treffer an das Informationsregister zu dem anfragenden Nutzer weiter. Für jedes Liefersystem wird dazu ggf. ein Skript geschrieben, um die „Übersetzung" zu gewährleisten.

Das **Liefersystem 2** hält zwar die Daten entsprechend den Vorgaben des Hamburger Transparenzgesetzes vor und ist auch über das Internet erreichbar, hat aber keine Suchfunktion. In diesem Fall wird die Technologie CKAN (Comprehensive Knowledge Archive Network) und das sog. Harvesting benötigt. Im Folgenden werden zunächst die beiden Technologie-Komponenten und dann der Prozess der Informationslieferung beschrieben:

Das Open-Source-Programm CKAN ist eine mit der Programmiersprache Python geschriebene Software und dient der Sammlung von Metadaten über Datenpakete und andere Ressourcen. Es hat den Vorteil, dass neben dem überschaubaren Datenmodell für die Beschreibung von Datenpaketen beliebig viele Datenelemente ergänzt werden können. Sämtliche strukturierte Daten werden wie in einem Wiki versioniert. Es gibt ein Web-Interface zum Hinzufügen und Editieren von Paketinformationen. Für den maschinellen Zugriff ist eine API (Application Programming Interface) implementiert.

Unter *Harvesting* wird hier das regelmäßige Abernten vorhandener Datenbestände eines Liefersystems über eine entsprechende Schnittstelle verstanden.

Durch das Harvesting werden vom Liefersystem 2 alle Daten, inkl. Metadaten, geholt. Der Volltextindex wird ggf. extrahiert, im CKAN mit den Metadaten abgelegt und im eigenen Index eingelagert. Nachdem das passiert ist, wird die Ressource gelöscht. Entspricht beim Liefersystem 2 das Metadatenmodell dem des Informationsregisters, wird es als Suchergebnis ausgeliefert.

Nicht-persistierende Liefersysteme:

Nicht persistierende Liefersysteme halten die Daten nicht entsprechend den Vorgaben des Hamburger Transparenzgesetzes vor. Somit müssen diese zunächst vorgabengerecht gespeichert werden. Es gibt auch hier zwei Typen von Liefersystemen. Das **Liefersystem 3** hat keinen Zugang zum Internet bzw. ist nicht ständig online und hat keine Volltextsuche, steht aber im FHHNet. Im Unterschied dazu hat das **Liefersystem 4** einen Zugang zum Internet. Die Informationsgegenstände solcher Liefersysteme werden im zentralen Speicher (Mandanten-DB) vorgehalten. Dafür werden geeignete Agenten, wie etwa der Transportagent des Nachrichtenbrokers benötigt. Über geeignete Webservices, wie den XTA-Webservice landen die Daten inklusive Metadaten dann vollständig im Speicher. Der Einsatz des XTA-Webservices wird für jedes einzelne Liefersystem während der Analyse geprüft und entschieden. Zum gegenwärtigen Zeitpunkt ist bereits klar, dass es Liefersysteme gibt, die diesen Webservice aufgrund bereits implementierter Schnittstellen in jedem Fall nutzen werden. Die endgültige Anzahl anzubindender Liefersysteme über XTA und das dabei anfallende Datenvolumen ist allerdings noch nicht absehbar. Es wird ein sukzessives Monitoring bei jeder Anbindung mit Blick auf die verbleibenden Kapazitäten des Nachrichtenbrokers geben.

Der Speicher wird auch durch den CKAN geharvestet und ist somit analog zum Liefersystem 2 zu betrachten (Herausziehen der Metadaten, Indexergänzung und Auslieferung der Suchanfrage).

2.5.3.2 Softwarearchitektur „Automatisierte Zulieferung“

Für eine detaillierte Beschreibung der Softwarekomponenten kann auf das Kapitel 2.7.2 und 2.7.3 verwiesen werden. Dort sind alle oben involvierten Komponenten beschrieben.

2.5.3.3 Anforderungen „Automatisierte Zulieferung“

Die Anforderungen werden durch die Komponenten erfüllt. Zu den einzelnen Anforderungen siehe Abschnitt 4.1.5 Umsetzung „Automatisierte Zulieferung“.

2.6 Zentrales Speichersystem (ZSp-MDB)

2.6.1 Kurzbeschreibung „Zentrales Speichersystem (ZSp-MDB)“

Das zentrale Speichersystem enthält die in der oben aufgeführten Abbildung enthaltenen Komponenten, um Informationsobjekte zu speichern, die in den Liefersystemen nicht entsprechend der Vorgaben des Hamburger Transparenzgesetzes gespeichert werden. Diese Liefersysteme stellen Dateien in einem Zwischenspeicher (über einen Export) zur Verfügung. Für das Holen der Daten aus dem Zwischenspeicher wird sich eines sog. Transportagenten bedient. Über die XTA-Webservice-Schnittstelle werden die Daten in den Speicher geholt und das Original aus dem Zwischenspeicher kann dann gelöscht werden. Neben den Daten bzw. Dokumenten werden so auch die Metadaten gespeichert.

Zusätzlicher Nutzen

In den vorangehenden Absätzen ist dargelegt, wie diese Realisierungsvariante das in der abstrakten Architektur spezifizierte Zentrale Speichersystem umsetzt.

Darüber hinaus bringt diese Variante folgenden Nutzen:

- Schutz vor Schadsoftware
- Adapter- und Dienstepalette des Nachrichtenbrokers für unterschiedlichste Liefersystemanforderungen einsetzbar
- Relationales DBMS als Persistenzkern erleichtert Ergänzung von Standardreportgeneratoren und Datawarehouse-Systemen
- „Webservicefassade“ erlaubt leichte Erweiterung um Spezialdienste

2.6.2 Systemarchitektur „Zentrales Speichersystem (ZSp-MDB)“

Entwicklungsplattform

Weitestgehende Mitnutzung von Entwicklungsplattformen, die für andere Entwicklungen genutzt werden.

QS-Plattform

Der Produktionsplattform ähnliche standardisierte Plattform aus Dataportangebot

Produktionsplattform

Standardisierte bei Bedarf clusterbare Plattformen aus Dataportangebot.

Plattform	Module auf der Plattform	OS
Datenbankserver	• Microsoft SQL-Server	Windows-Server
Applicationserver	• Microsoft IIS	Windows-Server

2.6.3 Softwarearchitektur „Zentrales Speichersystem (ZSp-MDB)“

Technisch umfasst der Speicher eine relationale Datenbank für

- Ressourcen als BLOBs beliebiger MIME-Types
- Metadaten zu Ressourcen
- Protokolle zu authentifizierten CUD-Zugriffen (Create, Update, Delete) und anonymen Get-Ressource-Abfragen
- Referenzen für referentielle Integrität bzgl. Versionierung und Metadaten-Ressource-Beziehungen
- Logisch Isolierte Mandantenbereiche

sowie einen zentralen Speicher-Service (ZSS) für anwendungsspezifische CUD-Datenbanktransaktionen (Data-Access-Layer), einen Leitstellenclient mit Benutzeroberfläche für manuelle Eingriffe insbesondere der Fachlichen Leitstelle und Transportagent für dezentralen Einsatz bei Liefersystemen, die den zentralen XTA-Webservice nicht selbst direkt aufrufen können.

[redacted]

2.6.4 Anforderungen „Zentrales Speichersystem (ZSp-MDB)“

Die Anforderungen werden durch die Komponenten erfüllt. Zu den einzelnen Anforderungen siehe Abschnitt 4.1.6 Umsetzung „Zentrales Speichersystem (ZSp-MDB)“.

2.7 Suchvorbereitungs- und Suchsystemkomponenten

2.7.1 Kurzbeschreibung „Suchvorbereitungs- und Suchsystemkomponenten“

Das Comprehensive Knowledge Archive Network (CKAN) ist ein webbasiertes Datenmanagementsystem zum Sichern und Verteilen von großen Datenmengen. Dazu auf ckan.org:

> *“CKAN, the world’s leading open-source data portal platform.*
>
> *CKAN is a powerful data management system that makes data accessible – by providing tools to streamline publishing, sharing, finding and using data. CKAN is aimed at data publishers (national and regional governments, companies and organizations) wanting to make their data open and available.”*

Die technologische Basis der Grundfunktionalität ist eine auf Solr/Lucene basierende Suche und eine PostgreSQL-Datenbank.

Der CKAN besitzt eine ausführliche RPC-API zugreifbar über http. Alle Kernfunktionalitäten der Webseite des CKAN können durch externe Programme, welche die CKAN-API aufrufen, angesprochen werden. Diese Funktionalität ermöglicht speziell die Verfügbarkeit der Informationsobjekte für Applikationsentwickler.

Die Verwendung des CKAN ermöglicht die Bereitstellung des Suchsystems und des Harvestings (Suchvorbereitung des „Suchvorbereitungs- und Suchsystems“).

Die Suche selbst ist bereits durch die Verwendung der CKAN-OpenSource-Entwicklung realisiert und kann über die CKAN-Webseite oder die CKAN-API angesprochen werden.

Für die Suchvorbereitung müssen pro Liefersystem Harvester geschrieben werden, um die Datenbestände aus jedem Liefersystem ziehen zu können. Diese holen einerseits die Metadaten und die Ressourcen (z.B. Textdokumente, Office-Dateien, Aufrufe von Services). Die Ressourcen werden geparst, um eine Volltextsuche zu ermöglichen. Weiterhin bildet jeder Harvester die Metadaten des Liefersystems auf das Metadatenschema des HmbTG-IT-Systems ab.

Speziell die besondere Abstimmung des CKAN auf die Anforderungen öffentlicher Verwaltungen und Regierungen, die Nähe zur OpenKnowledgeFoundation und OpenData-Anwendungen (gegeben durch die API und ähnliche Metadatenschemata) und der weitverbreitete Einsatz des CKAN im US-amerikanischen wie auch zunehmend im europäischen Raum[1] bestimmt die Wahl des CKAN als Suchvorbereitungs- und Suchsystem im HmbTG-IT-System.

Ähnlich liefert die IPS (Information Portal Suite) erprobte[2] Metasuchfunktionalität, die bei Bedarf eingesetzt werden sollen.

Durch beide zu verwendenden Systeme, CKAN und IPS, sind Abweichungen der notwendigen Infrastruktur (Betriebssystems, Programmiersprachen, Datenbanken) von den Rahmenanforderungen an Software- und Systemarchitektur begründet.

Zusätzlicher Nutzen CKAN

---

[1] http://ckan.org/case-studies/

[2] U.a. http://www.hamburgwissen-digital.de

In den vorangehenden Absätzen ist dargelegt, wie mit CKAN das in der abstrakten Architektur spezifizierte *„Suchvorbereitungs- und Suchsystem“* umsetzt.

Darüber hinaus bringt es in diesem abstrakten Aufgabengebiet folgenden Nutzen:

- Verwendungsmöglichkeiten weiterer CKAN-Extensions (z.B. Geo-Extension, Filestore, Datastore)
- Weiterentwicklung durch eine Open-Source-Community
- Steuerung der CKAN-Entwicklung durch aktive Teilnahme an dieser Community
- Teilnahme an einer Software-Community aus dem E-Government-Bereich,
- Grundlage für Entwicklungen in anderen Bundesländern

2.7.2 Systemarchitektur „Suchvorbereitungs- und Suchsystemkomponenten“

Im folgendem werden beide Architekturvarianten, CKAN und CKAN/IPS, auf Plattformen abgebildet. Jede Plattform kann mit einem virtuellen oder physikalischen Server realisiert werden. Die angegebene Infrastruktur wird für die vom CKAN und der IPS zur Verfügung gestellten Funktionalität notwendig.

Zu beachten ist, dass für die QS-Plattform und für die Produktionsplattform der SOLR-Indexierer und die SOLR-Suche auf getrennten Server laufen sollten. Die Komponenten werden über das Master/Slave-Konzept von SOLR realisiert. Der SOLR-Indexierer bildet den SOLR-Master, welcher regelmäßig auf den SOLR-Slave dupliziert wird. Der SOLR-Slave realisiert die produktive Suche[3]. Für die Entwicklungsplattform ist die Unterscheidung Master/Slave noch nicht notwendig.

[redacted]

2.7.3 Softwarearchitektur „Suchvorbereitungs- und Suchsystemkomponenten“

Falls externe Suche-Server über eine Metasuche angesprochen werden müssen, ist die Entwicklung einer Schnittstelle zwischen CKAN und der Metasuchmaschine Information Portal Suite (IPS) notwendig. Daher soll die Softwarearchitektur für das Suchvorbereitungs- und Suchsystems in zwei Varianten vorbereitet werden: einmal ohne Metasuche (CKAN vgl. Abbildung 9) und einmal mit Metasuche (CKAN/IPS Abbildung 10). Das System CKAN/IPS enthält als zusätzliches Teilsystem die IPS. Alle anderen Teilsysteme (SOLR-Server, CKAN-Applikation und Portal-Server) sind exakt die Teilsysteme des Systems CKAN. Sie sind daher in Abbildung 10 nicht detailliert aufgeführt.

CKAN/IPS wird nur dann zum Einsatz kommen, wenn im Zuge der Analyse der gemeldeten Liefersysteme Fälle auftreten, die nicht geharvestet werden oder an den zentralen Speicher zuliefern, sondern nur mittels einer Suche angesprochen werden können. Dies kann z.B. der Fall sein, wenn a) der Datenumfang des Liefersystems ein Harvesten nicht zulässt oder b) ein direkter Zugriff auf Informationsobjekte des Liefersystems aus Aktualitätsgründen notwendig ist. Diese Systemvariante erfordert eine zusätzliche neue Schnittstelle zwischen der CKAN-Applikation und dem IPS-Server, sowie IPS-Gateways für die Anbindung der Suchmaschinen und der eigenen Suchkomponente im SOLR-Server.

Zum jetzigen Zeitpunkt (Stand 30.08.2013) sind keine Liefersysteme bekannt, die den Einsatz der IPS erfordern.

[redacted]

2.7.4 Anforderungen „Suchvorbereitungs- und Suchsystemkomponenten“

Die Anforderungen werden durch die Komponenten erfüllt. Zu den einzelnen Anforderungen siehe Abschnitt 4.1.8 Umsetzung „Such- und Suchvorbereitungskomponente.

2.7.5 Portal

Es wird ein Portal benötigt, über welches die Nutzer Zugang zu den veröffentlichten Informationsgegenständen bekommen. Hier ist insbesondere die Suchfunktionalität von zentraler Bedeutung.

Um das Portal angemessen nutzen zu können, müssen folgende Qualitätsmerkmale eingehalten werden:

- Durchgängige Erreichbarkeit der Plattform und auch der referenzierten Informationsobjekte
- Stabiler Betrieb auch bei mehr als 1000 Anfragen gleichzeitig
- Volltextsuche für Dokumente
- Informationsobjekte in maschinenlesbarer Form, Standardformate für die Zielgruppe Weiterverarbeiter
- Informationsdarstellung in menschenlesbarer Form
- Versionierung / Historisierung der Informationsobjekte
- Verfügbarkeit der Daten über mindestens 10 Jahre
- Einhaltung des Datenschutzes
- Vollständige Abdeckung der im TG §3 genannten Themenfelder („Informationsgegenstände“)

- Integration des bestehenden Open Data Portals Hamburg

Die oben aufgeführten Komponenten tragen diesen Anforderungen Rechnung.

Verweis: Eine detailliertere Beschreibung der genauen Portalanforderungen wird derzeit in einem eigenen Portalkonzept erarbeitet. Auf dieser Basis erfolgt die Definition der technischen Komponenten für die Umsetzung.

Um die Portaloberfläche für das neue Informationsregister aufzubauen, sind nach gegenwärtigem Stand verschiedene Optionen denkbar, die im Portalkonzept umrissen werden. Grundsätzlich ist dabei die Entscheidung zu treffen, ob die Portaloberfläche in einem CMS abgebildet und per Schnittstelle an den CKAN (als Metadatenregister) angebunden wird, oder ob die CKAN-Oberfläche direkt als Portaloberfläche genutzt werden soll.

Abhängig von dieser Entscheidung fallen im Weiteren nach aktuellem Stand die folgenden Arbeitspakete an:

- Erweiterung der im Rahmen von Open Data bestehenden Schnittstelle (Java-basiert) für die Integration der Portaloberfläche auf Basis des Redaktionssystems von hamburg.de (CoreMedia) mit der API des CKAN-Datenregisters;
- Oder „Theming“ der CKAN-Oberfläche zur Anpassung an das Kommunikationsmuster der FHH auf hamburg.de, um CKAN ganz oder teilweise direkt als Oberfläche für das Informationsregister zu verwenden.

2.8 Zusammenwirken der Teilsysteme untereinander und mit externen Systemen

Auch wenn sie einige Funktionalität allein erbringen, werden einige Anforderungen erst durch das Zusammenwirken der Teilsysteme untereinander und mit externen Systemen erfüllt.

Abbildung 11 zeigt die für das Zusammenwirken nötigen Schnittstellen.

Einleitend beschreibt Abschnitt 2.8.1 die benötigten Schnittstellen. Die Abschnitte 2.8.2 bis 2.8.5 skizzieren anschließend die wichtigsten Szenarien bei Zusammenwirken der Teilsysteme.

2.8.1 Abstrakte Schnittstellen

Mit den abstrakten Schnittstellen werden funktional-semantisch benötigte Zusammenarbeits-Verbindungen zwischen den abstrakten Teilsystemen beschrieben. Insbesondere abstrahieren sie von der Interaktionsform und technischem Format. Letztere werden in Abhängigkeit von der konkreten Umsetzungsform der Teilsysteme passend gewählt (unter Umständen sogar in mehreren Varianten). Abbildung 11 zeigt welche abstrakten Schnittstellen zwischen den Teilsystemen des Informationsregisters und von ihnen zu externe Systemen bestehen. Ihr jeweiliger Zweck wird in den folgenden Unterabschnitten beschrieben.

Abstrakte Schnittstelle „Gather“

Zweck: Übergabe einer ID-Liste aller Objekte (Metadaten+Ressource) eines Objektspeichers („Quellsystems“)

Abstrakte Schnittstelle „Fetch“

Zweck: Übergabe des zu einer ID gehörigen Objektes

Abstrakte Schnittstelle „Fetch-all“

Zweck: Übergabe aller Objekte eines Objektspeichers

Abstrakte Schnittstelle „SignalChange“

Zweck: Hinweis, dass sich Objekte auf die per Index verwiesen wird, geändert (i.S.v. CUD) haben

Abstrakte Schnittstelle „GetRessource“

Zweck: „Upload-artiges“ holen eines Objektes über seine URL

Abstrakte Schnittstelle „PackageSearch“

Zweck: API für die Suchfunktionalität für Applikationsentwickler („Apps“)

Abstrakte Schnittstelle „Link“

Zweck: Referenz auf eine Web-Seite, speziell um das HmbTG-IT-System in hamburg.de einzubinden.

Abstrakte Schnittstelle „Create“

Zweck: Erzeugen eines neuen Objektes in einem Objektspeicher

Abstrakte Schnittstelle „Update“

Zweck: Ändern eines existierenden Objektes in einem Objektspeicher

Abstrakte Schnittstelle „Delete“

Zweck: Entfernen eines Objektes aus einem Objektspeicher

[redacted]

4.2 Metadaten aus ELDORADO

Nach aktuellem Arbeitsstand werden die folgenden Metadatenfelder exportiert:

- „abgebendes/ erstellendes“ Verfahren (für eine spätere Zuordnung)
- ELDORADO-Dokumentennummer (interne Information)
- Erstellungs-Datum
- Betreff
- Aktenzeichen
- Fremdes Aktenzeichen (optional, z.B. wenn ein Papieraktenzeichen mit übergeben werden soll)

- Absender
- Stichworte/Schlagworte
- Adressat für den Veröffentlichungs-Workflow
    - Wird ein Dokument per Druckertreiber nach ELDORADO verfügt und vom Registratur-mitarbeiter im Folgenden kein abweichender Adressat für den Veröffentlichungs-Workflow angegeben, wird die E-Mail-Adresse des verfügenden Benutzers beim Export des Duplikates in den Metadaten als Adressat übernommen.

4.3 Metadaten-Modell für Eingabemasken

Feld aus dem Metadatenmodell für das Informationsregister	Feldname in Veröffentlichungs-WF	Inhalt	Format	Mehrfachnennung	Pflicht	Mapping und Darstellung im Veröffentlichungs-WF
Informationsgegenstand	Informationsgegenstand	Infogegenstände aus dem HmbTG	zu klären: Text oder numerisch	ja	ja	Auswahl aus Liste, ggf. änderbarer Vorschlag auf Basis des gewählten HmbTG-Schlagwortes aus ELDORADO
Titel	Titel	aussagekräftiger Titel des Dokumentes, der Anwendung oder des Datensatzes	Text	Nein	ja	Übernahme aus ELDORADO: Betreff (änderbar) begrenzt auf 70 Zeichen
Schlagwörter	Schlagwörter/Suchbegriff(e)	Schlagwörter zur Beschreibung des Inhaltes. Verwendung eines Thesaurus wird geprüft, ist aber schwierig wegen der sehr unterschiedlichen Inhalte	Text	ja	nein	Übernahme aus ELDORADO: Stichwort, (änderbar)
Veröffentlichende Stelle (intern o. extern)	Veröffentlichende Stelle	Behörde oder Beteiligungsunternehmen, aus der/aus dem der Inhalt kommt	Text	nein	ja	Übernahme aus ELDORADO: Absender (änderbar)
weitere Informationen	Link zu weitergehenden Informationen	URL zu weiterführenden Informationen über den Inhalt, kann auch auf externe Anwendung / externes Portal verlinken	URL	ja	nein	Zu klären: nicht anzeigen oder optional
Offline-Datum	Löschdatum	Datum, zu dem der Inhalt aus dem Inforegister gelöscht werden kann. Kann ggf. länger als 10 Jah-	Datum (oder hier noch Textangabe, das echte „Da-	nein	ja	Default: Veröffentlichungszeitpunkt (im Inforeg.) in 10 Jahren, änderbar auf späteres Datum (x Jahre) oder

		re sein, nicht kürzer. Zusätzliche Option: Aufbewahrungszeit = unendlich	tum“ muss zum Zeitpunkt der Veröffentlichung vom Inforeg. gesetzt werden			"läuft nie ab"
Beschreibung	Inhalt	Beschreibung des Inhaltes, ggf. Kurzbeschreibung in den ersten 180 Zeichen (o.ä.) für die Darstellung in der Trefferliste im Informationsregister	Text	nein	nein	Eingabe Freitext (Anzahl Zeichen?)
Kategorie	Kategorie(n)	Open Data Kategorien (Mehrfachnennung bisher nicht möglich, ist aber gewünscht, Klärung für das Modell im CKAN)	Text	ja	ja	Auswahl aus Liste
Zeitraum von	Gültig ab	Wann beginnt der im Datensatz behandelte Zeitraum	Datum	nein	nein	Übernahme aus ELDORADO: Erstellungsdatum (änderbar, Auswahl aus Kalender?)
Zeitraum bis	Gültig bis	Wann endet der im Datensatz behandelte Zeitraum	Datum	nein	nein	Eingabe Datum (Auswahl aus Kalender?)

Feldfarbe	Bedeutung
	Vorbelegtes Feld mit änderbarem Inhalt
	Leeres Feld

4.4 Abkürzungsverzeichnis

Abkürzung	Beschreibung
API	Application Programming Interface
CKAN	Comprehensive Knowledge Archive Network
IPS	Information-Portal-Suite
IAP	Integrierter Angebotsprozess