Leistungsbeschreibung

Proof of Concept Collaborate Workspace in einer europäischen Microsoft Cloud

für

Senat der Freien und Hansestadt Hamburg
– Senatskanzlei –
Amt für IT und Digitalisierung
Rathausmarkt 1
20095 Hamburg

nachfolgend Auftraggeber

Fachlicher Ansprechpartner	[redacted]-Dataport [redacted] – Dataport
Datum	16.12.2020

Inhalt

1 Einleitung

Im 2018 Jahr hat Dataport im Auftrag der Trägerländer einen Proof of Concept (PoC) im Kontext Collaborative Workspace durchgeführt.

In dem PoC wurden die Anforderungen an den Umgang mit geschäftsrelevanten Dokumenten außerhalb von elektronischen Akten und Fachanwendungen gegen eine im Dataport-RZ betriebene OnPremise Lösung abgeglichen. Zur besseren Vergleichbarkeit von Ergebnissen wünschte das Amt für IT und Digitalisierung (ITD) die Durchführung eines zweiten PoC in einer Public-Cloud-Lösung.

Die Kundenanfrage fokussiert sich auf einen Teilaspekt des File-Service – dieser wird im BASIS Kontext genutzt für

- Gruppenlaufwerke
- Home-Laufwerke
- Servergespeicherte Profile der Benutzer
-

Im PoC liegt der Fokus darauf, die Gruppenlaufwerke durch einen Public-Cloud-basierten Service abzubilden, die Ablösung von Home-Laufwerken und Profilen wird nicht betrachtet.

Da insbesondere die User Experience (Stichwort Bedienbarkeit und Benutzererlebnis) eine hohe Priorität besitzt, wird der PoC nicht in einer gekapselten Laborumgebung abgebildet, sondern erfolgt unter Einbeziehung eines Teilbereiches des ITD und der Behörde für Arbeit, Soziales, Familie und Integration (BASFI) auf der Grundlage von ausgewählten Produktivdaten.

Die Abbildung des PoC erfolgt über Microsoft Cloud Dienste (hier Office 365) aus europäischen Rechenzentren (Niederlande, Irland).

In 2019 hat eine intensive Befassung und Abstimmung über Umfang und Ausprägung des PoC zwischen Auftragnehmer und Auftraggeber stattgefunden, die Ergebnisse finden sich in der Anlage „*Entscheidungsgrundlage Nutzung von Cloudservices*“.

Zudem wurden Konzepte erarbeitet, auf deren Grundlage die initiale Einrichtung und Konfiguration der PoC-Umgebung erfolgt. Erste Schritte wie …

- Bereitstellung eine Tenants und Zuweisung der notwendigen Lizenzen
- Aufbau einer Infrastruktur zur Synchronisation der notwendigen Objekte (Benutzerkonten, Gruppen, Computerkonten) in das Azure Active Directory

.. wurden in 2019 erfolgreich durchgeführt.

1.1 Allgemeine Leistungsabgrenzung

Der PoC fokussiert sich auf die Nutzung einzelner Services aus Office 365 (Sharepoint Online (SPO), Office 365 Pro, Online Office) im Kontext Abbildung eines Gruppenlaufwerks.

Neben der Abbildung eines Gruppenlaufwerks, welches die Organisationsstruktur abbildet, soll auch Teams für Projekte und Aufgaben bezogene Zusammenarbeit getestet werden. Im Rahmen des PoC wird Teams den PoC Benutzern zur Verfügung gestellt, wobei möglicherweise nicht alle Funktionen nutzbar sind.

Ein umfängliche Analyse und Konfiguration von Teams und den damit verbundenen Diensten (z.B. Exchange, OD4B, Planer, …) ist optionaler Bestandteil des Angebots.

Die Ausweitung auf weitere Funktionen aus der euMC erfordert ggf. eine separate Beauftragung bzw. eine Anpassung des Auftrags.

Die Nutzungsmöglichkeit eines Tenant ist an die Laufzeit der genutzten Subscriptionen gebunden. Auf Wunsch des Auftraggebers wurden die für die Abbildung des PoC notwendigen Subscriptionen als AddOn zum bestehenden Enterprise Agreement (EA) Vertrag mit Microsoft beschafft. AddOns zum EA haben eine Laufzeit bis zum Ende des EAs. Eine vorzeitige Kündigung ist nicht möglich. Der aktuelle EA-Vertrag hat eine Laufzeit bis zum 31.12.2021.

Letzter Schritt des PoC ist die Überführung der Produktivdaten aus OneDrive for Business in den dann aktuellen File Service. Sollte der Tenant über die Laufzeit des PoC hinweg genutzt werden, ist für den weiterführenden Betrieb eine separate Beauftragung nötig.

Die Konzeption einer alternativen File-Service-Lösung ist nicht Bestandteil dieses Angebots.

2 Vertragsgegenstand

2.1 Projektsteuerung

Bestandteil dieser Vertragsvereinbarung ist die Bereitstellung einer Projektsteuerung durch den Auftragnehmer.

Hierin enthalten sind folgende Leistungen:

Abstimmung und Koordination

- Zeitliche und inhaltliche Abstimmung mit dem Auftraggeber
- Vorbereitung und Teilnahme an regelmäßigen Jour-Fixe-Sitzungen
- Steuerung der internen Abläufe beim Auftragnehmer, u.a. Vorbereitung und Durchführung interner Abstimmungsgespräche
- Steuerung externer Dienstleister

Berichtswesen / Dokumentation

- Bereitstellung und Administration einer SharePoint-Seite auf dem Kundenportal, welche über die Projektlaufzeit zur Ablage der Projektdokumentation dient
- Pflege einer Offenen-Punkte-Liste
- Qualitätssicherung der Projektdokumentation

Projektplanung

- Erstellen und Pflege eines Projektplans
- Controlling des Projektverlaufs (Termine, Abbildung bzw. Anpassung der Anforderungen)
- Einleiten von Korrekturmaßnahmen, ggf. Einleiten von Eskalationen

2.2 Arbeitspakete

2.2.1 Konzeptreview und PoC-Dokumentation

Übergreifend über alle Phasen des PoC (siehe auch folgende Kapitel) erfolgt ein Review der vorliegenden Konzepte, d.h. es erfolgt die Analyse, inwieweit bestehende Konzepte angepasst und/oder ergänzt werden müssen.

Aufbau und Ablauf des PoC werden zudem begleitend in einer Projektdokumentation verschriftlicht.

2.2.2 PoC-Umsetzung Phase 1

Die Phase 1 der PoC-Umsetzung gliedert sich in

- Abrundung Pilotumgebung
- Start mit Pilotgruppe 1

Abrundung Pilotumgebung

Vor dem Start der Pilotierung sind u.a. folgende Tätigkeiten durchzuführen:

- Cloud-Aktivierung der Arbeitsplätze für die erste Pilotgruppe
- Sicherheitseinstellungen Office 365
- Abbildung einer initialen Struktur des Gruppenlaufwerks für ITD und BASFI

Start mit Pilotgruppe 1

Die Pilotgruppe 1 besteht aus ausgewählten Mitarbeiterinnen und Mitarbeitern des ITD und der BASFI.

In dieser Phase erfolgen erste Funktionstests wie z.B.:

- Übernahme von Dokumenten in die neue Ablage in SPO
- Anlegen von Dokumenten
- Gemeinsame Bearbeitung von Dokumenten
- Test von Freigaben

Dataport und /oder unterstützender Dienstleister begleiten diese Phase intensiv, um notwendige Anpassungen an der Konfiguration vorzunehmen.

Zum Ende der Pilotierung erfolgt eine erste Bewertung und Abstimmung, wie die Fortführung des PoC gestaltet wird.

2.2.3 PoC-Umsetzung Phase 2

In der Phase 2 erfolgt die Ausweitung des PoC auf weitere ausgewählte Mitarbeiterinnen und Mitarbeiter des ITD und der BASFI (Pilotgruppe 2).

Vorab erfolgen die notwendigen Konfigurationsanpassungen (Übernahme der Benutzer- und Computerkonten in AAD, Cloud Aktivierung der Arbeitsplätze).

Bei Bedarf erfolgt eine initiale Einweisung der Pilotgruppe 2.

Dataport begleitet auch diese Phase – in regelmäßigen Review-Gesprächen erfolgen erste Analysen und ggf. Anpassungen der Konfiguration.

2.2.4 Auswertung & Empfehlung

In die Auswertung des PoC werden alle PoC-Teilnehmer einbezogen:

- über einen zu entwickelnden Fragebogen erfolgt eine Befragung aller am PoC beteiligten Mitarbeiter per Online-Abfrage; die Abfrage erfolgt anonym, Antworten sind nicht einzelnen Personen zuzuordnen
- über Einzelinterviews werden nach Auswertung der Fragebögen häufig genannte Aspekte (Lob, Kritik) vertieft

Aus den Ergebnissen der Auswertung wird eine Empfehlung für die weitere Umsetzung eines Collaborate Workspace generiert.

2.2.5 Migration der Produktivdaten

Vor Abschluss der PoC ist ein Konzept zur Migration der im PoC abgelegten Produktivdaten in SPO zu erstellen. Voraussetzung hierfür ist die Vorgabe, in welches Zielsystem die Migration der Daten zu erfolgen hat. Je nach Datenvolumen und Zielsystem kann eine manuelle Migration der Daten durch den Anwender oder ein automatisiertes Verfahren sinnvoll sein.

Vor dem vereinbarten PoC-Endedatum erfolgt die Überführung der Daten in das Zielsystem, die Verantwortung für die Überführung der Daten liegt beim Auftraggeber.

Die Konfiguration der am PoC beteiligten Endgeräte wird auf den in der Senatskanzlei bzw. in der BASFI gültigen Standard zurückgesetzt; die für den PoC angelegten OUs, administrative Konten und Gruppen im O- Premises-Verzeichnisdienst werden gelöscht.

2.3 Ausweitung des PoC auf weitere Services (optional)

2.3.1 Pilotierung weiterer Office 365 Apps / Services

Je nach Verlauf des PoC kann der Wunsch / die Notwendigkeit entstehen, weitere Services im Kontext von Office 365 zu testen. Hierbei sind folgende Voraussetzungen zu beachten:

- der gewünschte Service steht in der euMC zur Verfügung
- der gewünschte Service ist in den bereitgestellten Subskriptionen enthalten

Hinweis:

Der Aufwand für die Pilotierung weiterer Office Apps / Services kann derzeit nicht abschließend kalkuliert werden. Hierzu wird ein initialer Aufwand geschätzt, für eine vollständige Betrachtung ist ggf. ein ergänzender Auftrag notwendig.

2.3.2 dSmartDesk – Integration von OD4B

Im Rahmen dieses Aufgabenpaketes wird die Integration der im Apple-Store bereitgestellten OD4B App auf dSmartDesk-Endgeräte (auf der Grundlage von Apple iOS) analysiert.

Betrachtet werden die

- automatische Bereitstellung der OD4B App auf definierten Endgeräten
- Abbildung des Anmeldeprozess
- Möglichkeiten, Datenbewegungen/-abfluss durch Policies aus dem Mobile Device Management heraus zu steuern

Die Analyse erfolgt in enger Abstimmung mit der verantwortlichen Projektgruppe für dSmartDesk.

3 Rechtliche Rahmenbedingungen

Die Rahmenbedingungen für die Durchführung des PoC sind in der Anlage „Entscheidungsgrundlage Nutzung von Cloudservices“ beschrieben.

4 Zeitliche Einordnung – Grobplanung des PoC-Ablaufs

Für den PoC ist eine Laufzeit von sechs Monaten (Januar – Juni) mit drei Monaten zusätzlichem Puffer (Juli – September) vorgesehen.

Nach aktueller Planung ist folgender Ablauf für den PoC vorgesehen

- Januar – Juni
  - Konzeptreview und PoC Dokumentation
- Januar 2020
  - Abrundung Pilotumgebung
- Februar – März 2020
  - Pilotgruppe 1 testet neue Funktionalitäten in dem Gruppenlaufwerk (SPO)
- April – Mai
  - Ausweitung der PoC Teilnehmer auf Pilotgruppe 2
- Juni
  - Auswertung & Empfehlung
    Falls keine Verlängerung geplant:
  - Rückmigration der Daten
  - Rückbau der PoC Umgebung
- Juli – September (optional)
  - Verlängerung des PoC, ggf. Test weiterer Office365-Services
  - Rückmigration der Daten
  - Rückbau der PoC Umgebung

Die Erweiterung des PoC-Umfangs auf weitere Apps/ Services kann im PoC-Ablauf bilateral abgestimmt und zeitlich eingeordnet werden. Risikofaktor bei kurzfristigen Planänderungen ist die Bereitstellung geeigneten Personals auf Auftraggeberseite, ggf. muss der Unterstützungsanteil durch externe Dienstleister erhöht werden.

Der nach aktuellem Status geplante Rückbau der PoC-Umgebung macht eine Datenmigration der Dokumente, die in SPO abgelegt wurden, erforderlich. Die Migration erfolgt in das dann gültige Zielsystem.

Unter Berücksichtigung des zeitlichen Ablaufs des PoC ist dann die Migration der Daten in den aktuellen BASIS-Fileservice zu planen und umzusetzen.[1]

[1] Konzeption und Aufbau eines neuen Zielsystems sind nicht Bestandteil dieses Angebots, müssen aber ggf. in die Ablaufplanung als Meilensteine aufgenommen werden.

5 Aufwandsaufstellung

Im Folgenden werden die Aufwände für die einzelnen Arbeitspakete beschrieben, hierbei erfolgt eine Unterteilung in

- geschätzter Aufwand in Stunden
- berechneter Aufwand in Stunden

Die Unterscheidung in geschätzten Aufwand und berechneten Aufwand folgt der Verteilung des eingesetzten Personals, welches in dem Zeitraum für anderweitige Produktbelastungen nicht zur Verfügung steht. Dies betrifft das Produkt BASIS, welches eine Personalfinanzierung bestimmter Personalumfänge eingesetzter Fachbereiche für den BASIS-Betrieb über die Clientpauschale beinhaltet. Da für diesen PoC Wissensträger des für den Betrieb geplanten Personals eingesetzt werden (aufgrund des Stundenumfangs ohne Personalaufstockung) käme eine Verrechnung einer Doppelverrechnung gleich, daher werden diese Teilstunden dieses Personals nicht weiterverrechnet.

Der geschätzte Aufwand pro Arbeitspaket wurde um diese Stundenzahl bereinigt; der Vollständigkeit halber werden beide Angaben ausgewiesen.

Für die Bearbeitung der Aufgabenpakete kommen Mitarbeiter des Auftragnehmers bzw. beauftragte Dritte zum Einsatz.

5.1 Projektsteuerung & Arbeitspakete

Projektsteuerung

Übergreifende Tätigkeiten über Zeitraum von sechs Monaten	Geschätzter Aufwand (STD)	Berechneter Aufwand (STD)
Projektassistenz	96	96
Steuerung & Planung	180	180
Jour-Fixe-Sitzungen (14-tägig	36	36
Summe	312	312

Verlängerung des PoC pro Monat		
Projektassistenz	16	16
Steuerung & Planung	30	30
Jour-Fixe-Sitzungen (14-tägig)	6	6
Summe	52	52

Konzeptreview und PoC-Dokumentation

Konzeptreview und PoC-Dokumentation	Geschätzter Aufwand (STD)	Berechneter Aufwand (STD)
Konzeption Senior	120	120

PoC Umsetzung Phase 1

PoC Umsetzung Phase 1	Geschätzter Aufwand (STD)	Berechneter Aufwand (STD)
Konzeption Senior	200	48
Fremdleistung	80	80
Summe	280	128

PoC Umsetzung Phase 2

PoC Umsetzung Phase 2	Geschätzter Aufwand (STD)	Berechneter Aufwand (STD)
Konzeption Senior	128	48
Fremdleistung	40	40
Summe	168	88

Auswertung & Empfehlung

Auswertung und Empfehlung	Geschätzter Aufwand (STD)	Berechneter Aufwand (STD)
Konzeption Senior	76	56
Fremdleistung	16	16
Summe	92	72

Migration der Produktivdaten

Migration der Produktivdaten	Geschätzter Aufwand (STD)	Berechneter Aufwand (STD)
Konzeption Senior	120	120

Ausweitung des PoC auf weitere Services (z.B. Teams)

Optional: **Ausweitung des PoC auf weitere Services**	Geschätzter Aufwand (STD)	Berechneter Aufwand (STD)
Konzeption Senior	240	240
Fremdleistung	40	40
Summe	280	280

5.2 Abbildung Azure AD Connect

Die Abbildung der Pilotumgebung bedingt den Aufbau und Betrieb zweier Serversysteme im RZ². Um die Betriebssicherheit sicherzustellen, wird ein produktiver AAD-Connect Server und einer für Test und Stage benötigt.

Für die Bereitstellung und den Betrieb dieser Systeme werden monatlich folgende Kosten veranschlagt:

Bei PoC-Verlängerung pro Monat	Geschätzter Aufwand (STD)	Berechneter Aufwand (STD
TVM AAD Connect	20	20

	RZ-Leistungen	
	Artikelcode	Anzahl
	DP-MSS-APPS/DM/S/WIN	2
	DP-MSS-STO/SANN	140
	DP-MSS-BACK/30	140

Für den Zeitraum von sechs Monaten entstehen somit folgende Aufwände

Für die Laufzeit der Sync Infrastruktur uber einen Zeitraum von 6 Monaten	Geschätzter Aufwand (STD)	Berechneter Aufwand (STD)
TVM AAD Connect	120	120

	RZ-Leistungen	
	Artikelcode	Anzahl
	DP-MSS-APPS/DM/S/WIN	2
	DP-MSS-STO/SANN	140
	DP-MSS-BACK/30	140

Hinweis:

Eine redundante Auslegung wird für den PoC von Seiten des Auftraggebers nicht gefordert.

5.3 Lizenzkosten

Die Subskriptionen, die für den PoC benutzt werden, werden durch den Auftraggeber über eine Zusatzvereinbarung als AddOn zum EA-Vertrag beschafft und für den PoC bereitgestellt.

5.4 Zusammenfassung

Für eine PoC-Laufzeit von sechs Monaten und die Umsetzung der oben genannten obligatorischen Leistungen ergibt sich ein Aufwand von …

	Geschätzter Aufwand Dataport in Stunden	Berechneter Aufwand Dataport in Stunden
Dataport	1008	756
Fremdleistungen	136	136
Summe	1144	892

... zuzüglich der Kosten für Bereitstellung und TVM für die Abbildung des Azure AD Connects gemäß 5.2.

Bei Ausweitung des PoC (Verlängerung der Laufzeit, Umsetzung der optionalen Leistungen) erhöhen sich die Aufwände gemäß der Angaben in 5.1 und 5.2.

PoC Collaborative Workspace in der MS Cloud

dataport

Stand: 29.08.2019

1 Auftrag

Das Amt für IT und Digitalisierung (ITD) möchte in dem PoC „Collaborative Workspace in der MS Cloud“ testen, wie das aktuell im Fileservice abgebildete Gruppenlaufwerk in der Azure-Cloud abgebildet werden kann.
Klassifizieren und automatisches Schützen von Dokumenten ist nicht vorgesehen. Zudem möchte das IDT in diesem PoC den Online-Service Teams von Microsoft testen. Dem ITD geht es darum, den Funktionsumfang und die Nutzbarkeit von Teams im Behördenalltag zu erproben.

Mit dem PoC sollen die erforderlichen Erkenntnisse gewonnen werden, welche Datenabflüsse nach Außen und nach Innen stattfinden und welche Datenschutzrisiken in tatsächlicher Hinsicht bestehen. Der PoC soll aufzeigen, ob und mit welchen Schutzmechanismen wirksam bestehende Datenschutzrisiken ausgeschlossen bzw. auf welches Maß minimiert werden können.

Aufgrund der rechtlichen Rahmenbedingungen ist der PoC so angelegt, dass nur ein eng begrenzter und definierter Kreis der teilnimmt. Ferner ist Maßgabe, dass sich der PoC auf anonymisierte Daten fokussiert und nur dort personenbeziehbare Daten verwendet werden, wo es für den Zweck des PoC erforderlich ist.

Am PoC wird das Amt ITD in vollem Umfang und die IT-Abteilung der BasFI zum Thema Onedrive for Business teilnehmen. Beim Amt ITD werden die Daten ausgeschlossen, die für Personal, Rahmenverträge der FHH und sensible Sicherheitsvorgänge betreffen.

2 Eingangsgrößen

2.1 Zu untersuchende Funktionen/Azure-Dienste

Um den PoC abzubilden, werden mehrere Cloud-Services in Form von Software as a Service (SaaS) von Microsoft benötigt, welche im Folgenden kurz beschrieben werden.

2.1.1 Azure AD

Der Service Azure AD (AAD) stellt die Identitätsverwaltung für die weiteren Cloud-Dienste dar. Er dient zur Authentifizierung und Autorisierung für weitere Cloud-Services und stellt diesen zudem Informationen über Benutzer, Gruppen und Computer bereit.

Die Informationen werden aus dem on premises Active Directory (AD) in das AAD synchronisiert. Die Synchronisation kann z.B. auf AD-Objekte einer bestimmten Organisationseinheit eingeschränkt werden. Das zu synchronisierende Attribut-Set und damit der Umfang der zu synchronisierenden Informationen werden auf die von den Services benötigten Attribute eingeschränkt.

2.1.2 SharePoint Online

Der Service SharePoint Online dient der Speicherung von sowohl Inhaltsdaten (Ordner und Dateien) wie auch von Metadaten (Zeit und Nutzer der letzten Änderung, Kategorie der Daten). Der Zugriff auf dort gespeicherte Daten kann sowohl über den OnDrive for Business (OD4B)-Client als auch über die Weboberfläche des Services erfolgen.

Der Zugriff wird über Berechtigungen gesteuert, die Authentifizierung der Nutzer erfolgt über das AAD (s. 2.1.1).

2.1.3 Teams

Teams ist ein Service, über den Teams wie (Projekt-)Gruppen Termine vereinbaren, gemeinsam an Dateien arbeiten und chatten können. Darüber hinaus ist auch eine Video-Konferenz-Funktion enthalten, diese wird im PoC nicht betrachtet bzw. genutzt.

Teams ist der offizielle Nachfolger von Skype for Business Online, angereichert um Funktionen, die auch Outlook bereitstellt.

Teams kann als ein einheitliches Frontend für dahinterliegende (Backend-)Services wie SharePoint und Exchange gesehen werden.

2.1.4 Exchange Online

Exchange Online ist ein Groupware-Service, der Postfächer (inkl. Kalender und Adressbuch) bereitstellt. Dies können sowohl persönliche Postfächer für die Nutzer, wie auch Teams-Postfächer sein.

2.1.5 Azure Vault

Azure Vault bietet eine Verwaltung für kryptografische Schlüssel in der Cloud. Es gibt verschiedene Optionen zur Schlüsselgenerierung und –verwaltung. Aus sicherheitstechnischer Sicht ist grundlegend zu unterscheiden zwischen der Option „Host your own Key“ (HyoK), bei der Schlüssel ausschließlich on premises verwaltet und genutzt werden und allen anderen Optionen, bei denen die Schlüssel in der Cloud verwaltet werden.

Im ersten Fall (HyoK) haben die Cloud-Services und der Cloud-Anbieter keinen Zugriff auf die Schlüssel und somit auch nicht auf die Daten im Klartext. Das bedeutet, dass sie die Daten auch nicht verarbeiten können und somit im Funktionsumfang stark begrenzt werden, so können z.B. Office-Dokumente nicht über Office-Online bearbeitet werden.

In allen anderen Fällen liegen die Schlüssel in der Hoheit von Microsoft und können zur Entschlüsselung der Daten heran gezogen werden. Dies schützt vor externen Angreifern.

2.1.6 Azure Information Protection

Azure Information Protection (AIP) ist eine Lösung, um sensible Daten zu schützen. Dazu müssen die Daten zunächst bezüglich ihres Schutzbedarfs bewertet und mit einem entsprechenden Label versehen werden. Hierzu können Regeln definiert werden, die in bestimmten Fällen die Label automatisch erzeugen.

Basierend auf dem Schutzbedarf der Daten werden Richtlinien erstellt, was mit den Daten entsprechend der Label passieren darf und was nicht (Zugriff von extern, Speicherung in der Cloud, …). MS stellt die Cloud wie folgt auf:

Abbildung 1: Microsoft Regionen[1]

Dienste	Verfügbarkeit
Azure AD	EU
Azure Information Protection	Nicht regional
Azure Vault	offen
Exchange Online	aktuell EU, ab 2020 Deutschland
SharePoint Online	aktuell EU, ab 2020 Deutschland
Onedrive for Business	aktuell EU, ab 2020 Deutschland
Teams	EU
Office 365	aktuell EU, ab 2020 Deutschland

Abbildung 2:Verfügbarkeit von Microsoft Diensten[2]

2.2 Daten

Daten, die in der Cloud gespeichert und verarbeite werden, lassen sich in folgende Kategorien unterteilen:

1. Technische/Verwaltungsdaten
    a. Benutzerdaten/Attribute, z.B. Name, Telefonnummer, Standort, Büronummer, Mail-Adresse, SID, …
    b. Computerdaten, z.B. Maschinenname, SID, …
    c. Gruppeninformationen, z.B. Mitglieder, Mailadressen, SID, ..
2. Metadaten von Dokumenten/Datensätzen, z.B. Dateiname, letzter Bearbeiter/Zugriff, …

[1] Ausschnitt aus: https://azure.microsoft.com/de-de/global-infrastructure/regions/, Stand 29.08.2019
[2] https://azure.microsoft.com/de-de/global-infrastructure/, ergänzt durch Infos von Microsoft per Mail

3. Inhaltsdaten, z.B. Dateien, (Text-, Video- und Voice-)Chats, Kalendereinträge,…

Bei den Daten zu den Benutzer-Objekten im AAD handelt es sich um personenbezogene Daten. Für die Inhaltsdaten und Metadaten wurde noch keine Schutzbedarfsfeststellung getroffen.

2.3 Schutzfunktionen Azure

Daten in der Azure Cloud werden einerseits durch Berechtigungen vor dem Zugriff nicht autorisierter Nutzer geschützt, andererseits werden sie mittels Kryptografie vor unberechtigtem Zugriff geschützt.

Die Berechtigungen werden durch den Kunden festgelegt.

Die Kryptografie beinhaltet einerseits Verschlüsselungsalgorithmen und andererseits das Schlüsselmanagement (siehe auch 2.1.5). Die Verschlüsselungsalgorithmen entsprechen dem Stand der Technik.

Bei der Verschlüsselung der Daten wird wie folgt unterschieden:

- In Transport
  - ➢ Die Daten werden während der Übertragung z.B. per TLS oder IPSec verschlüsselt.
- At Rest
  - ➢ Die Daten werden vor dem Speichern verschlüsselt und beim Lesen entschlüsselt.
- In Process / In Transition
  - ➢ Die Daten werden verschlüsselt verarbeitet. Die Techniken und Algorithmen sind derzeit noch nicht für eine umfassende Verschlüsslung geeignet und finden in den im PoC betrachteten Services keine Anwendung.

Für alle Arten der Verschlüsselung ist entscheidend, wer auf die verwendeten Schlüssel und damit auf die Daten im Klartext zugreifen kann (siehe auch 2.1.5).

2.4 Rahmenbedingungen

Die folgende Tabelle stellt einen Auszug für den PoC relevanter Rechtsgrundlagen, Regelungen und Prüfaufträge zusammen:

Lfd. Nr.	Titel	Typ	Betroffenheit im PoC
1	EU Datenschutzgrund-verordnung	EU-Verordnung	Personenbezogene Daten in den Bereichen der technischen und Verwaltungsdaten, der Metadaten und der Inhaltsdaten (siehe Kap. 2.2)
2	HmbDSG	Landesgesetz	Personenbezogene Daten in den Bereichen der technischen und Verwaltungsdaten, der

			Metadaten und der Inhaltsdaten (siehe Kap. 2.2)
3	HmbSÜG (VO zu §34)	Landesgesetz	Sowohl Dataport als auch die SK (und damit ITD) sind Sicherheitsbereiche nach HmbSÜG; über die Auftragskette gilt diese Vorgabe für allen Daten im PoC.
4	Informationssicher-heitsleitlinie der FHH (IS LL)	Interne Rege-lung der FHH	Alle Informationen im PoC sind nach Maßgabe der Leitlinie und mitgeltenden Regelungen zu verarbeiten. Die Leitlinie sieht eine Orientie-rung an IT-Grundschutz vor.
5	US Cloud-Act (Clarify-ing Lawful Overseas Use of Data Act)	US-Amerikan-isches Recht	Alle Informationen im PoC
6	Vertragliche Verein-barungen zum Lizenzrecht	Verträge	Lizenzen für Nutzer außerhalb der FHH
7	Vorgaben des IT-Pla-nungsgrates	Interne Rege-lungen	Gemäß den Vorgaben des ITPLR-Beschlus-ses 2015/5 müssen Cloud-Anbieter eine Ver-traulichkeitsvereinbarung abschließen, nach der Daten nicht in den Bereich fremdstaatli-cher Offenbarungspflichten und Zugriffsmög-lichkeiten gelangen dürfen, die sich außerhalb der Bundesrepublik Deutschland gegen Cloud-Anbieter richten können. MS hat zwar wiederholt erklärt, dass MS gegen entspre-chende Anordnungen der Rechtsweg be-schreiten wird, hat aber ebenfalls keinerlei Zweifel daran gelassen, dass MS dem US-Recht unterliegt und dessen Geltung für MS nicht vertraglich abbedungen werden kann. Dieser Aspekt ist im Rahmen des PoCs zu be-werten.
	Beschluss ITPLR vom 27.06.2019, 29. Sitzung		1. Der IT-Planungsrat richtet zur gemeinsa-men Befassung mit dem Thema „Daten und Anwendungen der öffentlichen Verwaltungen im Cloud-Betrieb“ eine Arbeitsgruppe unter Federführung Nordrhein-Westfalens mit Ver-tretungen aus Bund und Ländern ein. 2. Die Arbeitsgruppe wird beauftragt, dem IT-Planungsrat Empfehlungen zu Anforderungen an Softwarehersteller für den Betrieb von An-wendungen in der Cloud vorzulegen.

			3. Die Arbeitsgruppe wird beauftragt, dem IT-Planungsrat Empfehlungen für das weitere Vorgehen hinsichtlich des Umgangs mit entsprechenden Softwareanbietern vorzulegen. 4. Der IT-Planungsrat bittet die Arbeitsgruppe um einen Zwischenbericht zu seiner 31. Sitzung.

3 Analyse

3.1 Schutzbedarf der Daten

Wenn auf eine Schutzbedarfsfeststellung auf Datei- bzw. Datensatzebene verzichtet wird, gilt für den Schutzbedarf aller Daten das Maximumprinzip. Um den Schutzbedarf auch der am höchsten zu bewertenden Daten sicherzustellen, erhalten also alle Daten diesen als höchsten anzunehmenden Schutzbedarf.

Bei den Daten, die in das AAD synchronisiert werden, handelt es sich gemäß EU-DSGVO um personenbezogene Daten, jedoch nicht um personenbezogene Daten besonderer Kategorien.

Betrachte Daten für das ITD:

In der Gruppenablage des ITDs werden derzeit für die Ordner

- IT-Sicherheit\vertraulich
- IT-Personalmanagement
- Amtsorganisation\Amt ITD\Personal

explizit eingeschränkte Rechte vergeben, auf alle anderen Ordner und Dateien haben alle Mitarbeiter des ITDs Zugriff. Da ITD zum Sicherheitsbereich der Senatskanzlei gehört, ist mit der Verarbeitung von als Verschlusssachen (VS) klassifizierten Dokumenten nicht auszuschließen. Diese Daten werden vorläufig im PoC ausgeschlossen und erst einbezogen, wenn für diese Daten Mechanismen der Klassifizierung bereitstehen und erprobt werden können.

Mittels Teams sollen die Nutzer des ITDs dienstlich kommunizieren und gemeinschaftlich an Projekten (und deren Daten) arbeiten.

3.1.1 Sicherheitsüberprüfung

Nach der Verordnung zu §34 des Hamburgischen Sicherheitsüberprüfung- und Geheimschutzgesetz (HmbSÜG) müssen alle Personen, die mit Funktionen der Systemadministration nach Vorgabe des HmbSÜG sicherheitsüberprüft werden. Unabhängig von den wahrgenommenen Funktionen sind „sämtliche Funktionen in Dataport“ als sicherheitsempfindliche öffentliche Bereiche klassifiziert. Hieraus leitet sich die Notwendigkeit einer Sicherheitsüberprüfung für alle Dataport-Beschäftigte und bei beauftragten Unternehmen ab.

Es ist im Rahmen des PoCs zu prüfen, ob durch geeignete Ersatzmaßnamen (zum Beispiel 4-Augen-Prinzip) ein ausreichendes Sicherheitsniveau erreicht werden kann.

Dies ist nicht für alle im Dienstleistungskontext relevanten Mitarbeiter von Microsoft realistisch umsetzbar. Somit ist eine Verarbeitung sowie ein Speicherung von Daten, für die das HmbSÜG Anwendung findet, in der MS-Cloud nicht zulässig. Ersatzmaßnahmen zur Sicherheitsüberprüfung, wie etwa die durch sicherheitsüberprüftes Personal begleitete Administration werden von MS außerhalb der Deutschland-Cloud nicht mehr angeboten. Auch eine verschlüsselte Speicherung in der Form, dass Microsoft und die genutzten Cloud-Services keine Kenntnis über die Daten im Klartext erhalten können, ist zulässig, wenn ein zulässiges kryptografisches Verfahren genutzt wird. Dies würde jedoch aktuell den Funktionsumfang der Cloud-Services auf ein absolutes Minimum (reiner Online-Speicher) reduzieren bzw. die Nutzung einzelner Services ausschließen. Zudem widerspricht dieser Ansatz den formulierten Anforderungen (siehe Kap. 3.2).

3.1.2 EU-DSGVO

Nach den Schutzbedarfskategorien der FHH[3] ergibt sich für die Daten der BASFI (siehe Kap. 3.1) mindestens **hoher Schutzbedarf** hinsichtlich der **Vertraulichkeit**, da auch fehlerhafte Daten gravierende Konsequenzen für die Betroffenen (u.a. Mündel) haben können, ist auch **hoher Schutzbedarf** hinsichtlich der **Integrität** anzunehmen.
Gemäß Art. 35 i.V.m. der von der Datenschutzkonferenz publizierten MUSS-Liste ist für diese Verarbeitungstätigkeit eine Datenschutzfolgeabschätzung vorzunehmen. Diese soll begleitend zum PoC erstellt werden.

3.1.3 Bestehende Verträge

Werden die bestehenden SLA aus dem Basis-Umfeld zugrunde gelegt, gilt auch hinsichtlich der **Verfügbarkeit hoher Schutzbedarf**.

3.1.4 Zwischenfazit

Alle Daten mit ev. hohem Schutzbedarf werden aus dem PoC ausgeschlossen.

3.2 Rechts- und Vorgabenkonformität der Anforderungen

3.2.1 Zugriffskontrolle

Eine Muss-Anforderung für den PoC ist, dass Externe bzw. Dritte berechtigt werden sollen, auf für sie freigegebene Daten in SharePoint Online und in Teams zugreifen zu können. Diese Freigaben sollen auch durch die Nutzer möglich sein.
Diese Anforderung steht im Widerspruch zu einer Zugriffskontrolle nach dem Stand der Technik, der gemäß Art. 32 EU-DSGVO zu berücksichtigen ist. Um den Stand der Technik erreichen zu können, sind Normen (gemäß IS LL IT-Grundschutz) und neuere Stände der Technik (z.B. Einsatz von AIP) zu berücksichtigen.[4] Diese Techniken sollen im Rahmen des PoCs betrachtet werden.

[3] Siehe Vorversionen des Schutzbedarfsfeststellungstools der FHH
[4] Beschluss des BVerfG vom 8.8.1978 (so genanntes Kalkar-Urteil)

3.2.2 EU-DSGVO

Die EU-DSGVO sieht vor, dass Dataport sowie der Auftraggeber ein Prüfungsrecht vor Ort haben (Art. 28 Abs. 3 lit h). Im Rahmen des PoCs ist zu prüfen, wie dies konkret umgesetzt werden kann.

3.2.3 IT-Grundschutz

Die Sicherheitskonzeption von Azure beruht auf der ISO 27000-Normenreihe. Für die FHH ist IT-Grundschutz vorgegeben, den Microsoft aktuell nicht unterstützt. Im Sicherheitsmanagement entsteht damit die Aufgabe, die von Microsoft umgesetzten Anforderungen auf IT-Grundschutz abzubilden, was dauerhaft erheblichen Ressourcenbedarf im Sicherheitsmanagement nach sich zieht.

3.3 Konkurrierendes Recht: HmbSÜG, EU-DSGVO und US Cloud-Act

Die Services müssen gemäß Anforderungen von ITD im vollen Umfang von Internen wie Externen verwendet werden können. Dazu gehört unter anderem auch eine Volltextsuche.
Zudem sollen Daten in der Form verschlüsselt gespeichert werden können, dass der Cloud-Dienstleister keinen Zugriff auf die Daten im Klartext erlangen kann.
Im PoC soll geprüft werden wie diese Anforderungen umgesetzt werden können.
Der US-Cloud-Act sieht vor, dass IT-Dienstleister mit Sitz in den USA (wie z.B. Microsoft) Daten auch von ausländischen Kunden und Verarbeitungsorten außerhalb der USA an Sicherheitsbehörden in den USA aushändigen müssen. Eine Beteiligung deutscher Gerichte sowie eine Information der betroffenen Verarbeiter sind nicht vorgesehen. Im PoCs soll im Rahmen einer Risikoabschätzung die Auswirkungen dieser Rechtsvorschriften betrachtet werden.

3.4 Nutzbarkeit der Schutzfunktionen

Im Rahmen des PoCs werden nur Daten mit niedrigem Schutzbedarf verarbeitet. Daher sind zunächst keine zusätzlichen Schutzfunktionen notwendig. Im Rahmen des PoCs soll betrachte werden ob ggf. weiteren Schutzfunktionen ergriffen werden können, um auch Daten mit normalem oder hohem Schutzbedarf ausreichend zu schützen.

3.5 Lizenzrecht

Nutzer, die nicht im AD der FHH verwaltet werden und unter den BMI-Vertrag fallen, wie z.B. Nutzer aus anderen Trägerländern, gelten laut MS-Lizenzbestimmungen nicht als Gäste – die keine Lizenz für einen Zugriff benötigen – sondern als interne Nutzer.

Im Rahmen des PoC ist zu klären, in welchen Szenarien welche Lizenzen erforderlich sind und wer diese Lizenzen bereitstellt.

4 Fazit

In dem oben beschrieben Rahmen ist der PoC umzusetzen.
Die formulierten technischen und rechtlichen Fragestellungen sind im Rahmen des PoCs aufzuarbeiten.