

Noch offene Frage aus der Mail von Hr. Donner vom 22.07.2025

Kalkulation der Betriebs- & Migrationskosten für die gesamte Einführung der in Phase II definierten Produkte & Realisierung des Konzeptes.

Bisher konnten wir nur die Lizenzkosten sowie die Dienstleisterkosten der in Phase I umzusetzenden Aufgaben beziffern. (siehe Beschlussvorlagen 0027/2025 und 1090/2025). Erst auf Basis des zu erstellenden Konzeptes werden wir in der Lage sein, weitere Betriebs & Migrationskosten zur Verfügung zu stellen.

Fragen aus der Mail von Hr. Donner vom 20.08.2025

- Wie gestaltet sich die Arbeit mit verschlüsselten Daten konkret bei der Nutzung von MS 365 im Browser? Ist das überhaupt möglich? Gibt es technische Voraussetzungen dafür? Eine Nutzung der "M365 im Web" ist zum aktuellen Sach- & Projektstand nicht vorgesehen. Wir werden M365 Apps for Enterprise als Client auf den Endgeräten der Stadt Mainz installieren.
Es ist in Projektphase I nicht vorgesehen, Daten außerhalb des Rechenzentrums der KDZ abzuspeichern/ abzulegen, hierzu werden ausschließlich die Server & Speichermedien der KDZ verwendet.
Die Einführung der Produkte Sharepoint, Onedrive, Teams, Exchange, etc. werden in Projektphasen II erfolgen. Bis dahin wird keine Möglichkeit bestehen, Daten extern abzuspeichern.
- Ist eine unterschiedliche Stärke bei der Verschlüsselung der Daten überhaupt sinnvoll dahingehend, dass den Usern eine Klassifizierung von Dokumenten ob ihrer Notwendigkeit der Stärke der Verschlüsselung eher schwerfällt? Ist es daher eher zu empfehlen, dass ausschließlich die am stärksten mögliche Verschlüsselung gewählt wird? Welche Kosten entstehen dadurch?
Es gibt mehrere Möglichkeiten, Daten in M365 zu verschlüsseln. Generell gilt es, folgende Möglichkeiten der Verschlüsselung zu unterscheiden: Zum einen in Telemetrie-, Audit- & Analysedaten, welche durch firmeneigene Zertifikate verschlüsselt werden können, sowie der Zugriff auf diese durch eine sogenannte "Customer Lockbox". Zum anderen besteht die Möglichkeit alle abgelegten Daten (Sharepoint, OneDrive, oder Exchange) durch eine Double key encryption (DKE) zu verschlüsseln. In Phase I besteht aktuell lediglich Bedarf an der Konfiguration der Customer Lockbox, welche bereits Teil der geplanten und präsentierten Lizenzierung ist. In Phase II - bei Einführung der Sharepoint- und OneDrive-Dienste - müssen darüber hinaus auch abgelegte Daten (durch das oben genannte DKE-Verfahren) verschlüsselt werden. Da die Preise hierzu frühestens in Phase 2 erfragt werden können, können wir aktuell lediglich Preise zur Orientierung bereitstellen: Lizenziert wird pro Transaktion: bsp. Kosten 10.000 Transaktionen kosten 0,027 € (<https://azure.microsoft.com/de-de/pricing/details/key-vault/>)
- In der heutigen Sitzung des Werkausschusses wurde angesprochen, dass mit der Zuschaltung weiterer Komponenten zusätzliche Consulting-Leistungen eingekauft werden müssten. Können Sie das bitte für die verschiedenen, angedachten

Komponenten/Funktionen aufführen und die (z.B. aus dem Austausch mit anderen Kommunen in Erfahrung gebrachten) zu erwartenden jeweiligen Kosten beziffern? Diese Kosten können wir aktuell nicht beziffern. Es ist geplant, ggf. weitere Beratungsleistungen in Bezug der Sharepoint-Einführung, Mailmigration (HCL Notes - Exchange) und der MS Teams-Einführung einzukaufen. Eine Kostenschätzung wird zu diesen Projektphasen wie gewohnt durch die Beschlussvorlage dem WA bereitgestellt, damit darüber entschieden werden kann.

- Bzgl. des Ausstiegsszenario stellen sich u.a. folgende (Leit-)Fragen:
 - Wird das (sich später in der Cloud befindliche) AD gespiegelt und ein lokales Backup eingerichtet?
Microsoft stellt EntraID zur Verfügung, welches kein ActiveDirectory-System ist. Es besteht keine Notwendigkeit hierzu ein lokales Backup einzurichten, da alle Daten von dem Lokalen AD nach EntraID gesynct wird. Das bedeutet, der originale Datenbestand befindet sich stets lokal im Rechenzentrum der KDZ. Es werden keine Daten aus EntraID in das lokale AD synchronisiert.
 - In welchem Rhythmus werden die Cloud gespeicherten Dateien lokal gesichert? Wo? Wie wird die Berechtigungsstruktur in der Cloud zwischengespeichert? Wie kann diese in einem lokalen Fileserver wieder importiert werden? Welche Produkte kommen dafür in Frage?
In der jetzigen Phase werden keine Dateien in der Cloud liegen oder abgespeichert werden können. Dies wird frühestens in Phase II bei Einführung des Sharepoints/ OneDrive thematisiert. Gerne werden wir die angefragten Punkte in der jeweiligen Projektphase bereitstellen. Aktuell wird hierzu mit einem externen Dienstleister ein Konzept erstellt.
 - In welchem Rhythmus werden die in MS 365 Exchange gespeicherten Accounts/ Postfächer lokal gesichert? Wo? In welcher alternativen technischen Struktur (Produkte) können diese importiert und wieder zugänglich gemacht werden?
Die Einführung eines Exchange-Dienstes ist frühestens Bestandteil der Phase II. Hierzu wird aktuell ein Einführungskonzept mit dem externen Dienstleister erstellt. Es ist aktuell z. b. in der konzeptionellen Klärung, welcher Weg gegangen werden kann. Ggf. ist Exchange Online nicht möglich, da das Mailrouting über das Netz des LDI s läuft. Somit muss ggf. ein Exchange onPremise eingerichtet werden, oder alternativ eine Hybridstellung zwischen Exchange onPremise und Exchange online.
 - Können die Teams-Nachrichten exportiert werden? In welchem Rhythmus würden diese lokal gesichert? Wo? Lassen sich Teams-Nachrichten auch in andere Produkte importieren?
Im Rahmen der aktuellen Projektphase wird die Nutzung von Teams generell deaktiviert sein. Das Produkt Microsoft Teams wird in Phase II auf Basis der abgeschlossenen Konzeptionierung als eigenständiges Projekt realisiert. Stand jetzt können wir nur darauf hinweisen, dass Teams nach BSI, CI5, etc., datenschutzkonform eingeführt wird.
- Wäre eine Migration in die Delos-Cloud problemlos möglich? Wäre die KDZ dazu allein in der Lage oder wären dazu weitere Beratungsleistungen nötig? Wann steht die Delos-Cloud Ihren Informationen zu Folge in dem von der LH Mainz zunächst benötigten Umfang zur Verfügung?
Eine Nutzung der Delos Cloud ist jederzeit möglich. Die Delos Cloud ist ein Provider der M365 Dienste und Funktionalitäten auf Basis der DSGVO durch Microsoft Azure.

” Delos Cloud stellt eine souveräne Cloud für die deutsche Verwaltung basierend auf der Hyperscaler-Technologie Microsoft Azure bereit. Die Dienste der souveränen Cloud-Plattform umfassen dabei insbesondere die umfangreichen Kollaborations-Tools und Produktivitätslösungen von Microsoft Office 365. Die Cloud-Plattform wird gemäß den regulatorischen Vorgaben des Bundes technisch, operativ und rechtlich souverän sein. Damit wird Delos Cloud als derzeit einziges Cloud-Angebot die Vorgaben des BSI für IT-Sicherheit und Geheimschutz sowie die gesetzlichen Vorgaben für Datenschutz in Abstimmung mit der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) vollumfänglich erfüllen.
Quelle: <https://news.microsoft.com/de-de/erste-souveraene-cloud-plattform-fuer-die-deutsche-verwaltung-auf-der-zielgeraden/>

Die Stadt Mainz plant in diesem Projekt ebenfalls die Einführung der oben genannten Dienste durch Microsoft Azure in vergleichbarer Art und Weise. Die Kommunale Datenzentrale wird hierzu in Phase I ein Konzept erstellen, Lizenzen erwerben und Microsoft Apps for Enterprise zur Verfügung stellen. Alle weiteren Dienste werden zunächst deaktiviert & in separaten Projekten der Phase II realisiert.

Quelle: https://www.msxfaq.de/cloud/marketing/delos_cloud.htm
https://news.microsoft.com/de-de/erste-souveraene-cloud-plattform-fuer-die-deutsche-verwaltung-auf-der-zielgeraden/?WT.mc_id=M365-MVP-6771