



PROTOKOLL STADTRAT KLOTEN

04. März 2025 · Beschluss 72-2025

9.5.1.1 Projekte

IDG-Status: öffentlich

IT, Microsoft M365; Nutzung

Ausgangslage

Microsoft 365 (folgend M365) ist ein zentrales Lösungs- bzw. Softwarepaket der Firma Microsoft Corp. Redmond (USA). Das Paket wurde 2011 unter dem Namen Office365 auf den Markt gebracht und stetig funktional ausgebaut. Es beinhaltet die seit Jahrzehnten bekannten Officeapplikationen Word, Excel und PowerPoint, aber auch umfangreiche Cloudanwendungen, wie z.B. eMail- und Kalenderlösungen. Die Stadt Kloten setzt die genannten Applikationen auf breiter Basis ein. Sie sind unverzichtbare Hilfsmittel für die Leistungserbringung von Verwaltung und Schule und des damit verbundenen Informationsaustausches mit externen Anspruchsgruppen.

M365 umfasst darüber hinaus marktdominante Kollaborationslösungen (Chat, Voice, Video, Dateiverwaltung) sowie umfangreiche Sicherheitslösungen wie z.B. die auch von der Stadt Kloten eingesetzte 2-Faktor-Authentifizierung. M365 ist der de facto Standard im Bereich kollaborativer Office-Lösungen, der sich auch gegenüber namhaften anderen Anbietern (z.B. Google) erfolgreich am Markt behauptet. Die M365-Plattformen wurden über die Jahre hinweg sukzessiv gegenüber dem Internet geöffnet, wodurch die Applikationen plattformübergreifend und auf allen gängigen mobilen Betriebsplattformen genutzt werden können. Nahezu alle massgeblichen nationalen wie auch internationalen Lösungsanbieter haben ihr Produktportfolio auf die partielle (Web-)Integration von M365-Lösungsbausteinen abgestimmt und nutzen dafür die von Microsoft zur Verfügung gestellten Software- bzw. Architekturbestandteile (Schnittstellen).

Mit Beschluss 59-2023 vom 7.3.2023 hat der Stadtrat die Einführung der neuen, cloudbasierten Schulverwaltungslösung "Pupil" der Pupil AG (St. Gallen) genehmigt. Dieser Beschluss beschreibt u.a. den breiten Einsatz von M365 für die Schulen unter Berücksichtigung der Lösung Pupil und der GeVer-Lösung CMI. In der Folge wurde M365 im Rahmen der Implementation der neuen Schulsoftware erfolgreich eingeführt. Im Betrieb hat sich die Lösung bisher bewährt. Die M365-Umgebung der Schule wird in einer dezidierten Instanz (sog. Tenant, eine Art Mandantenstruktur) betrieben und von der Abteilung Informatik administriert. Damit ist sichergestellt, dass Nutzende der Schulinstanz nicht auf die (künftige) M365-Verwaltungsinstanz zugreifen können. Ein Betrieb von Pupil ohne M365 ist nahezu unmöglich. Vor der Gewährung der Systemnutzung musste jede (Lehr-)Person eine neue, in Abstimmung mit dem Datenschutzbeauftragten der Stadt Kloten (Swiss Infosec AG, Sursee) ausgearbeitete Datenschutzerklärung unterzeichnen, um den sachgerechten Umgang mit sensiblen Informationen organisatorisch zu reglementieren.

Auf der Grundlage des Entscheids zur Einführung der Schulverwaltungslösung Pupil musste sich die Abteilung Informatik intensiv mit dem Themenkomplex M365 auseinandersetzen und entsprechende Kompetenzen in der Administration der Lösung aufbauen. Dies erfolgte parallel zum Submissionsvorhaben "IT-Infrastruktur-outsourcings" (1. HJ 2024), innerhalb dessen Anforderungen hinsichtlich eines M365-Einsatzes formuliert

wurden. Mittlerweile verfügen zwei Personen der Abteilung Informatik über vertiefte Administratoren- und zwei weitere Personen über Basiskenntnisse in der Administration von M365. Der Knowhow-Aufbau erfolgte in Zusammenarbeit mit dafür spezialisierten externen Dienstleistern und Weiterbildungen, darunter auch spezifische Schulungen zum Themenkomplex Sicherheit. Die Abteilung Informatik administriert und betreibt seit Frühsommer 2024 einen umfangreichen M365-Pilotbetrieb innerhalb einer dezidierten Verwaltungsumgebung; darin enthalten z.B. auch die künftige Lösung bzgl. Festnetztelefonie auf Basis des M365-Moduls "TeamsVoice". In Summe verfügt die Abteilung Informatik heute über das Knowhow, um M365 im Regelbetrieb stabil administrieren zu können.

Mit Beschluss 238-2024 vom 3.9.2024 hat der Stadtrat der Abteilung Informatik den Auftrag zur Realisierung eines IT-Infrastrukturoutsourcings erteilt, darin enthalten ist auch die Implementation von M365-Leistungsbestandteilen. Die im Rahmen eines Submissionsverfahrens evaluierte Lösung umfasst zahlreiche M365-Funktions- und Sicherheitsbestandteile (z.B. die gesamte Telefonielösung, Authentifizierungsverfahren, Nutzerverwaltung) sowie das Management der künftigen M365-Umgebung. Das IT-Infrastrukturoutsourcing wurde, angesichts dessen zeitlichen Nutzungsrahmens von mind. 5 Jahren (optional bis 7 Jahre), auch auf der Grundlage der von Microsoft publizierten strategischen Weiterentwicklungen von M365 submissioniert. Den Strategien ist zu entnehmen, dass zentrale Lösungsbausteine im Portfolio von Microsoft mittelfristig nur noch unter funktionaler Berücksichtigung der Cloudinfrastruktur von Microsoft betrieben und genutzt werden können. Ohne den Einsatz von M365 müsste das Vorhaben IT-Infrastrukturoutsourcings gestoppt, restrukturiert und in zentralen Bestandteilen neu aufgesetzt werden.

Die Nutzung von M365 im Bereich der öffentlichen Verwaltung unterliegt zahlreichen, teilweise sich widersprechenden Regelwerken. Das Kernproblem der M365-Nutzung begründet sich in Aspekten des Daten- und Informationsschutzes im Kontext der cloudbasierten Datenspeicherung (und des diesbezüglichen Datenkontrollverlustes des Kunden) des US-Unternehmens Microsoft, welche primär unter die US-Gesetzgebung (US Cloud Act) fällt und damit teilweise in Konflikt zur schweizerischen Gesetzgebung steht (stark vereinfachte Darstellung, vgl. Ausführung im beiliegenden ISDS-Konzept). Die Vorgaben der kant. Datenschutzbeauftragten (Zürich) hinsichtlich des Einsatzes von M365 sind technisch und rechtlich – über die Kantons Grenzen hinweg - stark umstritten, die geforderte Datenverschlüsselung (sog. Double Key Encryption) ist – auch aus Sicht Datenarchivierung – nicht operabel. Die Problematik wird in juristischen Fachkreisen intensiv und durchaus kontrovers diskutiert¹.

Es gibt Gemeinden im Kanton Zürich, welche M365 inkl. umfangreicher Clouddienste ohne ergänzende Datenverschlüsselungsmechanismen betreiben, wie aber auch solche, die vorerst noch an der Nutzung der veralteten (2016) und lokal installierten Produktversionen von Word, Excel etc. festhalten und die weitere "Einsatzregulierung" abwarten. Die kantonale Verwaltung Zürich nutzt M365 unter der Regie des AFI (Amt für Informatik) und die Bundesverwaltung migriert nach einem Pilotbetrieb aktuell auf M365². Aus einer Nutzungsanalyse der Gemeinde Bülach, welche von der Abteilung Informatik verifiziert wurde, resultierte, dass mindestens 40 Gemeinden im Kanton Zürich für ihre eMail-Kommunikation Zugangspunkte der Cloudlösungen von Microsoft nutzen (Stand Q4.2024).

Die Ausgangslage zeigt, dass die Stadt Kloten auf Grundlage der bestehenden geschäftskritischen Schulapplikation "Pupil" und der basisinfrastrukturellen Entwicklungen (IT-Infrastrukturoutsourcing) nahezu zwingend M365 (bzw. ein Teil der darin enthaltenen Lösungsbausteine) zum Einsatz bringen und dafür unter dem Aspekt Daten- und Informationsschutz einen praktikablen Lösungsansatz verfolgen muss. Ohne den

¹ Replik von David Rosenthal (Februar 2024) auf das "Cloud"-Gutachten von Markus Schäfer (Juli 2023)
https://www.rosenthal.ch/downloads/Rosenthal_Cloud-Gutachten-Replik.pdf

² <https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-102770.html>

Einsatz von M365 werden die Ziele der Digitalstrategie der Stadt Kloten in absehbarer Zeit nicht erreicht, wesentliche Vorhaben würden stark negativ beeinflusst (z.B. das IT-Infrastrukturoutsourcing) und bestehende Lösungen (z.B. Schullösung Pupil) müssten in ihrer Nutzung – ohne Alternative – erheblich eingeschränkt werden.

Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept) für den Einsatz von M365

Die Abteilung Informatik hat vom Stadtrat im Rahmen der Diskussionen rund um das Vorhaben IT-Infrastrukturoutsourcing den Auftrag erhalten, die Grundlagen für den Einsatz von M365 zu erarbeiten. Dabei steht nicht die Beschreibung des Lösungsumfangs von M365 im Zentrum, sondern die Darlegung des die Einführung von M365 bestimmenden Informationssicherheits- und Datenschutzkonzeptes. In der Folge wurde zusammen mit dem Datenschutzbeauftragten der Stadt Kloten (Swiss Infosec AG, Sursee) ein entsprechendes Vorhaben angestossen, dessen Ergebnisse nun, auf der Grundlage struktureller Vorgaben des Kanton Zürichs, vorliegen (ISDS-Konzept M365, v1.1, 17.2.2025).

Das ISDS-Konzept regelt die rechtlichen, architektonischen und betrieblichen Aspekte des M365-Einsatzes in der Stadt Kloten und ist als verbindliche Vorgabe bzw. Voraussetzung für den Einsatz von M365 – auch im Kontext des laufenden Projektes IT-Infrastrukturoutsourcing – zu verstehen. Unter Berücksichtigung der im ISDS-Konzept formulierten Rahmenbedingungen kann die Stadt Kloten M365 zum Einsatz bringen, Lösungsbestandteile schrittweise in die städtische Applikationslandkarte integrieren und den Informations- und Datenschutz gewährleisten. Die damit verbundenen Risiken sind tragbar, die Restrisiken beschränken sich summarisch auf bewusst grob fahrlässiges Verhalten der Nutzenden (vorsätzlicher Missbrauch personenbezogener Daten) und globale Krisensituationen.

Zum geplanten Einsatz von M365 liegt eine dezidierte Stellungnahme des Datenschutzbeauftragten der Stadt Kloten, Reto Zbinden (Swiss Infosec AG, Sursee) vom 18.2.2025 vor, welche den Einsatz von M365 - unter Berücksichtigung der im ISDS-Konzept beschriebenen Rahmenbedingungen - als nicht kritisch bewertet:

Auszug aus der Stellungnahme: Die Bearbeitungen, welche künftig mittels M365 erfolgen sollen, sind nicht neu und werden bereits heute durchgeführt. Entsprechend ändert sich grundsätzlich nichts an den hierzu erforderlichen gesetzlichen Grundlagen. Die Stadt Kloten beabsichtigt nur Sachdaten und (einfache) Personendaten mit M365 zu bearbeiten. Besondere Personendaten und dem Amts-/Berufsgeheimnis unterliegende Daten werden nach wie vor in den bestehenden Fachapplikationen (z.B. Abacus, Innosolv) bearbeitet und gespeichert. Der geplante Einsatz von M365 ist also kein Ersatz für bestehende Fachapplikationen, sondern soll vielmehr für die Kommunikation, Zusammenarbeit und Optimierung behördlicher Abläufe verwendet werden. Aus diesem Grund wird der geplante Einsatz von M365 aus Sicht Datenschutz als nicht kritisch bewertet.

Das ISDS-Konzept wurde von Everyware AG (Zürich), als künftiger Betreiber der gesamten IT-Infrastrukturen (im Kontext des IT-Infrastrukturoutsourcings), geprüft. Everyware AG sieht keine Hindernisse, die Vorgaben des ISDS-Konzeptes im Rahmen der M365-Umsetzung zu berücksichtigen.

Implementation M365 für die Verwaltung

Unter strikter Berücksichtigung des vorliegenden ISDS-Konzeptes soll M365 für die Verwaltung entlang des sich bereits in der Umsetzung befindlichen Vorhabens IT-Infrastrukturoutsourcing operationalisiert werden. In einer ersten Projektphase können damit, sofern der diesbezügliche Bedarf in den Fachinstanzen ausgewiesen werden kann, folgende Dienste auf Basis von M365 implementiert werden:

- Office-Standardanwendungen (Word, Excel, Powerpoint, Outlook etc.)
- Exchange Online (Mailedienste)
- Teams (Collaboration)
- Teams Voice (Telefonie)
- OneDrive (Dateiablage)
- SharePoint (Dateiablage)
- Planner (Projektplanung)
- Bookings (Terminverwaltung, auch für ext. Anspruchsgruppen)
- Whiteboard (Collaborative Online-Wandtafel)
- Form (Formulare)
- Lists (Informationsmanagement)
- PowerBI (Business Intelligence)
- Copilot (KI-Anwendung)
- Power Automate (Workflowsteuerung)

Die Einführung umfasst zusätzlich die stufenweise Implementation folgender Sicherheitsmechanismen:

- Customer Lockbox (Sicherheitslösung für Datenzugriff durch Microsoft)
- Multi-Faktor-Authentifizierung
- Conditional Access Rules (spezifisches Regelwerk für M365-Zugriff auth. Benutzer)
- PIM (Privileged Identity Management für Administratoren)
- Ergänzende Sicherheitslösungen im Kontext IT-Infrastrukturoutsourcing, hier insbesondere externe SOC-Dienste (Security Operation Center).

Die Einführung von M365 erfolgt im Projektmodus. Das Vorhaben wird durch das übergeordnete PL-Gremium des IT-Infrastrukturoutsourcings geführt (Stadt Kloten, Everyware AG, Metagon AG) und gegenüber dem Steering Committee, welchem Vertreter von Geschäftsleitung und Stadtrat angehören, rapportiert und überwacht. Durch diese Projekteingliederung wird die Einführung von M365 automatisch durch die Projektstreams (=Teilprojekte) "Informations-/Datenschutz" und "Security/BCM" begleitet. Dem Stream "Informations-/Datenschutz" gehört u.a. auch der Datenschutzbeauftragte der Stadt Kloten an (Swiss Infosec AG, Sursee). Mit dieser organisatorischen Regelung ist eine datenschutzkonforme Einführung von M365 auf der Grundlage des ISDS-Konzeptes sichergestellt.

Überarbeitung der Datenschutzerklärungen gegenüber dem Personalkörper

Mit der Einführung von M365 im Bereich der Schule (Pupil, siehe oben) und der den Betrieb voraussetzenden Datenschutzerklärung gegenüber den Nutzenden wurde deutlich, dass die Stadt Kloten die diesbezüglichen Regelwerke und Prozesse zu Gunsten grösserer Flexibilität (Anpassungsmanagement) und effizienteren Prozessen überarbeiten und vereinheitlichen sollte. Diese Erkenntnis deckt sich mit der Einschätzung des Datenschutzbeauftragten der Stadt Kloten (Swiss Infosec AG, Sursee) und der HR-Abteilung. Es ist deshalb vorgesehen, die Prozesse und Unterlagen bzgl. Datenschutzerklärung (gegenüber dem Personalkörper) unter Berücksichtigung der HR-Prozesse (Ein-/Austritt) und dem IT-Infrastrukturoutsourcing (inkl. M365) zu überarbeiten und zu vereinheitlichen.

Controlling der Nutzung M365 durch DSB-/ISB-Board

Das Datenschutz-/Informationssicherheits-Board der Stadt Kloten, welches sich personell aus dem Verwaltungsdirektor, dem Bereichsleiter Finanzen+Logistik, dem Leiter Informatik und zwei Vertretern des Datenschutzbeauftragten der Stadt Kloten (Swiss Infosec AG, Sursee) zusammensetzt, wird das Controlling der

Nutzung von M365 überantwortet. Das Board nimmt diese Funktion (u.a. Monitoring Sicherheitsvorfälle) bereits heute wahr und tagt ca. alle 6-8 Wochen. Damit ist sichergestellt, dass der Einsatzumfang und der Betrieb von M365 (und weiterer Applikationen) unter dem Aspekt Daten- und Informationssicherheit unabhängig von der Abteilung Informatik stetig überwacht wird.

Risikobetrachtung

Der Einsatz von M365 in Verwaltung und Schulen ist nicht frei von betrieblichen und datenschutzrechtlichen Risiken. Der Einsatz von M365 impliziert die Nutzung von Onlinediensten, deren Verfügbarkeit massgeblich von den Microsoft-Betriebsmodellen abhängig sind und der US-Gesetzgebung unterstehen. Die US-Gesetzgebung, hier insbesondere der sog. Cloud Act, gewährleistet, dass Justizbehörden der USA auf richterlichen Beschluss hin Daten von US-Cloudanbieter abgreifen und einsehen dürfen (stark vereinfachte Darstellung). Dies unabhängig vom Ort der Datenspeicherung, d.h. auch Rechenzentren von US-Anbietern, die ihren Standort in der EU – oder im Fall Microsoft in der Schweiz – haben, unterstehen dem Cloud Act. Auch wenn die rechtlichen Hürden für einen US-behördlichen Datenzugriff hoch sind, besteht mit dem Einsatz von M365 das Risiko, dass von der Stadt Kloten nicht autorisierte Personen und Behörden Daten und Informationen der Stadt Kloten einsehen und den Datenverkehr überwachen. Dies ist nur durch den Einsatz von hochkomplexen und sehr teuren Verschlüsselungslösungen zu verhindern, deren Einsatz jedoch den Funktionsumfang und die Nutzenaspekte von M365 massiv einschränken und aus denen grosse Einschränkungen bzgl. Usability resultieren. Darüber hinaus könnten Anforderungen des Staatsarchivs mit einer solchen Schutzmassnahme nicht erfüllt werden. Die Nutzung von IT-Lösungen aus der Cloud (wie es z.B. auch bei der Schulverwaltungslösung Pupil der Fall ist) impliziert immer einen partiellen Datenkontrollverlust und eine starke betriebliche Abhängigkeit vom Anbieter. Daraus resultiert eine u.U. deutliche Einschränkung der sog. "digitalen Souveränität". Wenn ein Anbieter ausschliesslich Schweizer Recht untersteht (z.B. die Cloud-Dienste von Abacus), sind die mit der Nutzung verbundenen Risiken bzgl. Daten- und Informationsschutz sowie Gewährleistung gut tragbar. Die Nutzung von M365 unterliegt jedoch nicht vollumfänglich der Schweizer Gesetzgebung. Das vorgesehene M365-Einsatzkonzept der Stadt Kloten tritt diesem Umstand mit applikatorischen (Labeling bzw. Datenklassifizierung), technischen (z.B. von Microsoft unabhängige eMail-Verschlüsselung, bereits heute im Einsatz) sowie organisatorischen Massnahmen entgegen. Damit werden schützenswerte und besonders schützenswerte Informationen in den Rechenzentren unseres Partner Everyware AG (Zürich) und mittelfristig innerhalb der GeVer-Lösung von CMI Axioma nachvollziehbar verwaltet und gelangen somit nicht auf Plattformen von Microsoft.

Erwägung

Der effiziente Betrieb von Verwaltung und Schule im Kontext digitalisierter Prozesse ist auf die Nutzung moderner IT-Officehilfsmittel angewiesen. Dafür werden heute u.a. Produkte von Microsoft eingesetzt und teilweise, im Verbund mit anderen Lösungskomponenten, für deren Betrieb vorausgesetzt. Die Ausführungen in diesem Papier zeigen die Notwendigkeit einer fortgesetzten M365-Implementation unter Auflagen, die dem Schutzbedürfnis sensibler Informationen entsprechen, auf. Die Implementation von M365 erfolgt unter Rahmenbedingungen, denen der Datenschutzbeauftragte der Stadt Kloten zugestimmt hat. Die Einführung erfolgt im Projektmodus unter Berücksichtigung massgeblicher Kontrollgremien und der Betrieb wird stetig vom DSB-/ISB-Board überwacht. Ohne die Einführung von M365 werden die Ziele der Digitalstrategie nicht zu erreichen sein, das Projekt IT-Infrastrukturoutsourcing müsste mit hohen Kostenfolgen gestoppt und in Teilen neu aufgesetzt werden und der erfolgreiche applikatorische Betrieb der Schulverwaltung (Pupil, M365 und CMI) müsste grundsätzlich überarbeitet werden. Der Entscheid für den Einsatz von M365 auf der Grundlage der beschriebenen Rahmenbedingungen ist notwendig, zeitgemäss, verantwortungsvoll, zukunftsgerichtet und mit dem Vorgehen anderer Gemeinden im Kanton Zürich vergleichbar.

Beschluss:

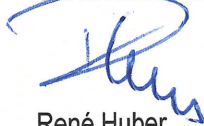
1. Der Stadtrat bewilligt den Einsatz von Microsoft 365 (M365) unter Berücksichtigung des ISDS-Konzeptes.
2. Der Stadtrat akzeptiert die mit dem Einsatz von M365 verbundenen Risiken bzgl. Datenkontrollverlust, Einschränkung der digitalen Souveränität, US-Cloud Act und Datenschutz.
3. Der Stadtrat beauftragt die Leitungsgremien (Projektleitung und Steering Committee) des Vorhabens "IT-Infrastrukturoutsourcing" mit der Einführung und Projektüberwachung von M365.
4. Der Stadtrat beauftragt das Datenschutz-/Informationssicherheit-Board (DSB-/ISB-Board) mit der betrieblichen Überwachung der M365-Nutzung.
5. Der Stadtrat beauftragt den Datenschutzbeauftragten der Stadt Kloten, die HR-Abteilung und die IT-Abteilung mit der Überarbeitung der inhaltlichen und prozeduralen Verarbeitung der Datenschutzerklärungen des Personalkörpers.
6. Die Koordination des Gesamtvorhabens liegt beim Leiter Informatik.

Mitteilungen an:

- Geschäftsleitung der Stadt Kloten
- Harald Lutz, Leiter Informatik
- Susanne Hirzel, Leiterin Personal
- co-Projektleiter und Steering Committee "IT-Infrastrukturoutsourcing" (Verteilung durch Leiter Informatik)
- Datenschutzbeauftragter der Stadt Kloten (Swiss Infosec AG, Sursee, Mitglied DSB-/ISB-Board)

Für Rückfragen ist zuständig: Ruedi Ulli, Bereichsleiter Finanzen+Logistik, Telefon 044 815 12 42

STADTRAT KLOTEN



René Huber
Präsident



Thomas Peter
Verwaltungsdirektor

Versandt: - 5. März 2025