Telefon 089 – 233 76 77 77 **it@M**

Digitale Souveränität als strategisches Leitprinzip – Sichere Software für München

Digitale Souveränität: Sichere Software für München
Antrag Nr. 20-26 / A 05673 von der SPD-Fraktion, Fraktion Die Grünen - Rosa Liste
vom 02.06.2025, eingegangen am 02.06.2025

Digitale Souveränität als strategisches Leitprinzip I – Beschaffungen
Antrag Nr. 20-26 / A 05710 von der Fraktion Die Grünen - Rosa Liste
vom 26.06.2025, eingegangen am 26.06.2025

Digitale Souveränität als strategisches Leitprinzip II – Risikoanalyse, Alternativen und Umstiegsszenarien
Antrag Nr. 20-26 / A 05711 von der Fraktion Die Grünen - Rosa Liste
vom 26.06.2025, eingegangen am 26.06.2025

Sitzungsvorlage Nr. 20-26 / V 18562

Beschluss des IT-Ausschusses als Werkausschuss für it@M vom 28.01.2026 (SB)

Öffentliche Sitzung

Kurzübersicht

zum beiliegenden Beschluss

Anlass	Antwort des IT-Referats auf die Stadtratsanträge: Digitale Souveränität: Sichere Software für München, SPD-Fraktion, Fraktion Die Grünen - Rosa Liste vom 02.06.2025 Digitale Souveränität als strategisches Leitprinzip I – Beschaffungen, Fraktion Die Grünen - Rosa Liste vom 26.06.2025 Digitale Souveränität als strategisches Leitprinzip II – Risikoanalyse, Alternativen und Umstiegsszenarien, Fraktion Die Grünen - Rosa Liste vom 26.06.2025
Inhalt	Das in den Stadtratsanträgen adressierte Thema der digitalen Souveränität ist hoch aktuell und besitzt für die Arbeit des IT-Referats größte Relevanz. Aufgrund der Stadtratsanträge zur digitalen Souveränität wurden die Aktivitäten zu diesem Thema im IT-Referat sowie auch die Zusammenarbeit mit anderen Organisationen, z. B. ZenDiS, Open Source Business Alliance und Dataport weiter

	intensiviert. Ferner wurden das referatsweite Verständnis der digitalen Souveränität definiert und eine Methodik zur Bewertung von digitaler Souveränität entwickelt und als Souveränitätscheck auf das Serviceportfolio des IT-Referats angewandt. Die Definition von digitaler Souveränität, die Methodik und die Ergebnisse des Souveränitätschecks werden in der Beschlussvorlage vorgestellt.
Gesamtkosten / Gesamterlöse	/
Klimaprüfung	Ist Klimaschutzrelevanz gegeben: Nein
Entscheidungs-vorschlag	Der Stadtrat nimmt den Vortrag der Referentin zur Kenntnis, dass das IT-Referat Lock-in Effekte vermeidet, weitergehende Sicherheitsgarantien realisiert, kontinuierlich den Markt beobachtet und zu einem geeigneten Zeitpunkt Umstiegsszenarien plant. Darüberhinaus wird das IT-Referat im Vergabeprozess offene Standards wesentlich strenger einfordern. Das IT-Referat wird beauftragt, die Methodik zur Prüfung auf digitale Souveränität weiterzuentwickeln und eine entsprechende Integration in die relevanten IT-Prozesse vorzunehmen. Das IT-Referat wird beauftragt, den Stadtrat im Rahmen der bereits bestehenden jährlichen Bekanntgabe zu E- und Open-Government zum Stand der digitalen Souveränität zu informieren. Das IT-Referat wird beauftragt, die Aktivitäten in der Operationalisierung zur Wahrung und Förderung der digitalen Souveränität selbständig fortzuführen.
Gesucht werden kann im RIS auch unter	Digitale Souveränität; Score; Open Source; Souveränitätscheck
Ortsangabe	/

Telefon 089 – 233 76 77 77 **it@M**

Digitale Souveränität als strategisches Leitprinzip – Sichere Software für München

Digitale Souveränität: Sichere Software für München
Antrag Nr. 20-26 / A 05673 von der SPD-Fraktion, Fraktion Die Grünen - Rosa Liste
vom 02.06.2025, eingegangen am 02.06.2025

Digitale Souveränität als strategisches Leitprinzip I – Beschaffungen
Antrag Nr. 20-26 / A 05710 von der Fraktion Die Grünen - Rosa Liste
vom 26.06.2025, eingegangen am 26.06.2025

Digitale Souveränität als strategisches Leitprinzip II – Risikoanalyse, Alternativen und Umstiegsszenarien
Antrag Nr. 20-26 / A 05711 von der Fraktion Die Grünen - Rosa Liste
vom 26.06.2025, eingegangen am 26.06.2025

Sitzungsvorlage Nr. 20-26 / V 18562

3 Anlagen

- Stadtratsanträge
- Ergebnisse Souveränitätscheck
- Stellungnahmen

Beschluss des IT-Ausschusses als Werkausschuss für it@M vom 28.01.2026 (SB)

Öffentliche Sitzung

Inhaltsverzeichnis **Seite**

I. Vortrag der Referentin

Zusammenfassung

Das in den Stadtratsanträgen adressierte Thema der digitalen Souveränität ist hoch aktuell und besitzt für die Arbeit des IT-Referats größte Relevanz.

Die Aktualität des Themas im öffentlichen Diskurs beruht zum einen auf der um sich greifenden Erkenntnis, dass eine stabil funktionierende Behörden-IT ein vitaler Bestandteil des öffentlichen Lebens geworden ist und damit zu den kritischen Infrastrukturen gehört, die nicht ausfallen dürfen. Zum anderen beruht sie auf der weltpolitischen Lage, in der allzu umfangreiche Abhängigkeiten von unter fremder Jurisdiktion agierenden Big-Tech-Unternehmen zum Risiko werden, weil diese Geschäftspartner durch ausländische Mächte dazu veranlasst werden können, sensible Daten aus den Softwareprodukten abzuschöpfen, erpresserischen Druck auf öffentliche Einrichtungen auszuüben oder gar – etwa durch Abschaltung von Software oder durch ferngesteuerte Zerstörung von Daten oder Hardware – Abläufe bei öffentlichen Einrichtungen zu stören und damit potentiell großen Schaden zu verursachen.

Wie groß die Relevanz des Themas für das IT-Referat ist, lässt sich schon daran ablesen, dass der Digitaltag des IT-Referats am 27. Juni 2025 unter der Überschrift „Open Source und Digitale Souveränität“[1] stattfand.

Aufgrund der Stadtratsanträge zur digitalen Souveränität wurden die Aktivitäten zu diesem Thema im IT-Referat sowie auch die Zusammenarbeit mit anderen Organisationen, z. B. ZenDiS, Open Source Business Alliance und Dataport, weiter intensiviert. Ferner wurden das referatsweite Verständnis der digitalen Souveränität definiert und eine Methodik zur Bewertung von digitaler Souveränität entwickelt und als Souveränitätscheck auf das Serviceportfolio des IT-Referats angewandt. Die Definition von digitaler Souveränität, die Methodik und die Ergebnisse des Souveränitätschecks werden in diesem Beschluss vorgestellt.

1. Digitale Souveränität als strategisches Ziel

Die Herstellung und Wahrung digitaler Souveränität ist eines der wesentlichen Anliegen und Ziele der Arbeit des IT-Referats und wird weiter ausgebaut und befördert.

Dabei ist jedoch die digitale Souveränität nicht das einzige Anliegen und Ziel, weshalb die digitale Souveränität nicht absolut betrachtet werden kann, sondern immer nur im Zusammenhang und Zusammenspiel mit anderen Belangen, die jedes Mal gegeneinander abgewogen werden müssen.

So sind neben dem Kriterium der digitalen Souveränität mindestens noch die folgenden bedeutsam bei der Entscheidung für oder gegen eine IT-Lösung:

- Datenschutz
- Barrierefreiheit
- Sozialverträglichkeit
- Nachhaltigkeit
- Funktionalität
- Geschlechtergleichstellung
- Nutzbarkeit (Usability)
- Steigerung der Digitalisierung
- Vergaberechtliche Vorgaben
- Sicherheit
- Wirtschaftlichkeit

[1] https://muenchen.digital/meldungen/2025/so-war-der-digitaltag-2025.html

In einer multipel vernetzten Welt ist es nicht möglich, alle Abhängigkeiten von externen Beteiligten zu eliminieren. Die Digitalisierung kann nur mit Arbeitsteilung und Partnerschaften vorankommen, und die implizieren zwangsläufig Abhängigkeiten. Daher muss immer – in jedem Einzelfall – bewertet werden, inwieweit die in diesen Abhängigkeiten bestehenden Risiken mitigiert oder akzeptiert werden können.

2. Definition zur „digitalen Souveränität“ für die Landeshauptstadt München

Der Terminus wird derzeit im öffentlichen Diskurs viel und oft in unterschiedlichen Kontexten und mit unterschiedlichen Zielsetzungen gebraucht, deshalb ist es notwendig, die für das IT-Referat und damit auch für die Landeshauptstadt München maßgebliche Bedeutung festzulegen. Da es nicht das Ziel sein kann, unabhängig von Land, Bund und EU zu agieren, sondern vielmehr die digitale Souveränität in genau diesem Rahmen verwirklicht werden muss, ist es sinnvoll, mit diesen Institutionen ein gemeinsames Verständnis von digitaler Souveränität zu haben und dieselbe Definition dafür zu verwenden.

Die Definition des Bundes[2] lautet:

> *„Digitale Souveränität“ beschreibt „die Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können“.*

Angestoßen durch die Stadtratsanträge zur digitalen Souveränität übernimmt das IT-Referat die Definition des Bundes.

Die Adverbien „selbstständig, selbstbestimmt und sicher“ werden dabei wie folgt verstanden:

2.1. Selbstständigkeit

Das Subjekt (Individuum oder Institution) ist vollständig eigenständig handlungsfähig, wobei Abhängigkeiten von anderen Akteuren minimiert sind.

2.2. Selbstbestimmtheit

Das Subjekt kann bewusst Entscheidungen treffen, auch über den Wechsel von Produkten und Anbietern, und hat die Kontrolle und jederzeit die Möglichkeit, die Richtung zu beeinflussen.

2.3. Sicherheit

Es herrscht Transparenz, da das Subjekt Kenntnis über Software und Hersteller hat und darüber, ob und wie gesetzliche Vorgaben und Sicherheitsnormen eingehalten und umgesetzt werden.

3. Strategische Komponenten der digitalen Souveränität

Der IT-Planungsrat hat in seinem Beschluss zur digitalen Souveränität[3] folgende drei strategischen Ziele festgelegt:

---

[2] Quelle: https://www.cio.bund.de/Webs/CIO/DE/digitale-loesungen/digitale-souveraenitaet/digitale-souveraenitaet-node.html

[3] Beschluss 2021/09: https://www.it-planungsrat.de/beschluss/beschluss-2021-09 – Kap. 3.1 Strategische Ziele – S. 6 (d. i. Quelle der folgenden drei Zitate)

3.1. Wechselmöglichkeit

Die Öffentliche Verwaltung hat die Möglichkeit einer freien Wahl bzw. eines flexiblen Wechsels zwischen IT-Lösungen, IT-Komponenten und Anbietern. Dies bedeutet, dass leistungsfähige und erprobte Alternativen zur Verfügung stehen, um kurzfristige Produktwechsel zu ermöglichen. IT-Architekturen, Beschaffungswege und Personalschulungen müssen darauf ausgelegt sein, einen Wechsel mit verhältnismäßigen Kosten und angemessenem Aufwand zu ermöglichen.

Die Landeshauptstadt München ist in dieser Hinsicht mit eigenem Rechenzentrum, eigener Vergabestelle und eigenen Softwareentwicklungskapazitäten sehr gut aufgestellt. Gleichwohl bedeutet der Wechsel von einer IT-Lösung zu einer anderen immer Aufwand, der in jedem Einzelfall im Verhältnis zu den erwarteten Vorteilen eines Wechsels betrachtet werden muss, vgl. Ziff. 4.3.4.

3.2. Gestaltungsfähigkeit

Die Öffentliche Verwaltung hat die Fähigkeit ihre IT (mit-)gestalten zu können. Dafür verfügt sie über die notwendigen Kompetenzen sowie (Zusammen-)Arbeitsstrukturen, um IT-Lösungen zu verstehen und bewerten zu können sowie bei Bedarf deren (Weiter-)Entwicklungen bzw. deren Betrieb sicherzustellen.

Auch hierfür ist die Landeshauptstadt München mit den unter Ziff. 3.1. genannten Voraussetzungen und mit der durch das sehr kompetente Personal im IT-Referat, bei it@M und in den GPAMS der Fachreferate vertretenen Expertise bestmöglich gerüstet, wobei die Leistungsfähigkeit immer auch eine Frage der Kapazität und letztlich der Finanzierung ist.

3.3. Einfluss auf Anbieter

Die Öffentliche Verwaltung kann ihre Anforderungen und Bedarfe (z. B. hinsichtlich Produkteigenschaften, Verhandlung und Vertragsgestaltung) gegenüber Technologieanbietern artikulieren und durchsetzen. Neben rechtlichen Vorgaben und Rahmenbedingungen umfasst dies u. a. die Option eines IT-Betriebs in Rechenzentren der Öffentlichen Verwaltung, die Berücksichtigung von Richtlinien zur Informationssicherheit und zum Datenschutz sowie den Einfluss auf Lizenzmodelle und die Produkt-Roadmap.

In diesem Punkt ist die Landeshauptstadt München, wenngleich die größte Kommunalverwaltung Deutschlands, häufig viel zu klein, um sich gegenüber global agierenden Technologieanbietern durchsetzen zu können oder auch nur gehört zu werden. Hier sind übergeordnete Entitäten und Verbünde gefragt, die mindestens auf nationaler, besser noch auf europäischer Ebene die Belange der digitalen Souveränität vertreten und verteidigen.

4. Zu den Anträgen im Einzelnen

4.1. Digitale Souveränität: Sichere Software für München

Antragstext

Das RIT wird beauftragt, die Softwarelösungen der Landeshauptstadt München einem Souveränitätscheck zu unterziehen. Dabei soll aufgeschlüsselt werden, welche möglichen Risiken und Schwachstellen bestehen und welche alternativen Angebote, insb. aus Europa, möglich wären.

Begründung

Im Hinblick auf die zunehmende Digitalisierung in allen Bereichen unseres Lebens ist es von immer größerer Bedeutung, dass hoheitliche Aufgaben zuverlässig erfüllt werden können, die digitalen Prozesse sicher sind und sensible Daten geschützt werden. Entscheidungsfragen im digitalen Raum müssen dabei selbstbestimmt und ohne äußere Einflussnahme getroffen werden können.

Die Stadt muss sicher sein, dass sie auf zuverlässige Software ohne Risiken zurückgreifen kann. Dies gilt auch in politisch unsicheren Zeiten.

Gerade deshalb braucht es eine Analyse, ob die Abhängigkeit von ausländischer Software zu Risiken und Schwachstellen führen kann, die frühzeitig zu erkennen und zu verhindern sind. Dies gilt auch insbesondere für neue Software, z.B. aus dem Bereich Künstliche Intelligenz.

Auf Bundesebene wird auf das „Zentrum für Digitale Souveränität der Öffentlichen Verwaltung“ hingewiesen und gebeten, auf dessen Erkenntnisse zurückzugreifen.

4.1.1. Souveränitätscheck

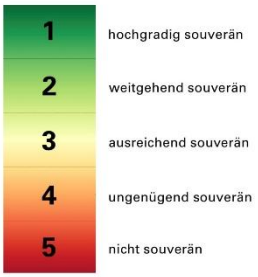
In diesem Antrag wird ein Souveränitätscheck gefordert.

Angestoßen durch diesen Stadtratsantrag hat das IT-Referat mit wissenschaftlicher Begleitung durch die TU München[4] die dazu notwendige Methodik entwickelt. Eine entsprechende Analyse wurde im September/Oktober 2025 über eine Auswahl von 194 Anwendungsservices der Landeshauptstadt München durchgeführt.

Die Auswahl aus den 2.780 Anwendungsservices der Landeshauptstadt München (Stand Oktober 2025), die die Geschäftsprozesse digital unterstützen, erfolgte für diese erste Analyse nach dem Kriterium der Business-Kritikalität.

Jeder einzelne der als besonders kritisch eingestuften Anwendungsservices wurde anhand eines Fragesets auf digitale Souveränität geprüft und das Ergebnis auf fünf Kategorien anhand des „Scores für Digitale Souveränität“ (SDS) gemappt.

Die Ergebnisse der Prüfung lauten wie folgt (Absolute Zahlen in Klammern):



- SDS 1: 33 % (64)
- SDS 2: 33 % (64)
- SDS 3: 8 % (16)
- SDS 4: 5 % (9)
- SDS 5: 21 % (41)

74 % des analysierten IT-Serviceportfolios des IT-Referats (Kategorien 1, 2 und 3) sind digital souverän, da kein Vendor-Lock-in vorliegt und weitere Kriterien der digitalen Souveränität erfüllt sind.

Die Services in der nicht souveränen Kategorie 5 mit 21 % setzen sich zusammen aus gesetzlich vorgeschriebenen Leistungen zur eVergabe, Anwendungsservices großer Anstalten des öffentlichen Rechts in Bayern und Hamburg, Software für die eAkte, deutsche auf die öffentliche Verwaltung spezialisierte Softwarehersteller u. a. im Kontext von Wahlen,

[4] Die wissenschaftliche Begleitung erfolgte durch Prof. Jürgen Pfeffer, TUM School of Social Sciences and Technology. Prof. Pfeffer ist Mitglied des Digitalrats der LHM.

eine Reihe von Services für das Personalmanagementsystem eines deutschen Softwareherstellers und zwei Services eines Softwareherstellers in den USA.

Zusammengefasst bewertet weist das IT-Serviceportfolio des IT-Referats auf der Basis des zugrundeliegenden Fragenkatalogs und der Auswahl der analysierten kritischen Anwendungsservices einen hohen Grad an digitaler Souveränität auf.

Wie sich die Methodik herleitet und wie die einzelnen Kategorien zu interpretieren sind, ist im Anhang zu diesem Beschluss erläutert.

Der jetzt vorliegende Softwarecheck auf digitale Souveränität in der Version 1.0 wird vom IT-Referat gemeinsam mit der TU München in Zukunft fortgeschrieben und weiterentwickelt. Er dient als Grundlage, das Thema digitale Souveränität sachlich strukturiert im Rahmen der gesamten Risiko-Betrachtung zu adressieren und zu bewerten und so letztlich die für die Landeshauptstadt München erforderliche digitale Souveränität herzustellen.

4.1.2. Software ohne Risiken

Des Weiteren wird gefordert:

> *Die Stadt muss sicher sein, dass sie auf zuverlässige Software ohne Risiken zurückgreifen kann.*

Hierzu muss gesagt werden, dass beim Einsatz von Software – wie auch in vielen anderen Lebensbereichen – eine gänzliche Risikofreiheit prinzipiell nicht erzielbar ist. Das heißt: Es geht generell nicht „ohne“ Risiken. Es gilt daher, diese Risiken nach Eintrittswahrscheinlichkeit und Schadenshöhe zu bewerten, sie nach Möglichkeit durch geeignete Maßnahmen präventiv oder korrektiv zu mitigieren und schließlich auf der Basis einer sachlichen Bewertung eine bewusste und informierte Entscheidung zum Umgang mit den verbleibenden Risiken zu treffen.

Dies ist bereits heute die gängige Praxis bei der Einführung neuer Software und anderer IT-Komponenten im IT-Referat: In den produktiven Betrieb kann in der IT-Landschaft der Landeshauptstadt München nur gelangen, was im Rahmen des Informationssicherheitsmanagements systematisch geprüft und nach Annahme der Restrisikodeklaration durch den beauftragenden Fachbereich freigegeben wurde. Des Weiteren ist auch die datenschutzrechtliche Prüfung (und ggf. Restrisikoübernahme durch den Verantwortlichen) Voraussetzung für die Produktivnahme von IT-Lösungen. Eine entsprechende Integration der Methodik zur Prüfung auf digitale Souveränität in die Prozesse im Risikomanagement Informationssicherheit wird aktuell konzipiert.

Als Reaktion auf den Stadtratsantrag wird das IT-Referat in diesem Rahmen künftig neben den Aspekten der Informationssicherheit zusätzliche, unmittelbar die digitale Souveränität betreffende Aspekte systematisch erfassen, bewerten und als weitere Dimension in das Risikomanagement bei der Einführung neuer IT-Services aufnehmen.

4.2. Digitale Souveränität als strategisches Leitprinzip I – Beschaffungen

Antragstext

> *Bei den anstehenden strukturell und finanziell relevanten Beschaffungen oder Vertragsverlängerungen im Bereich IT (beispielsweise bei Cloud-Computing, Telefonie, Videokonferenzen, Teamkollaboration, IT-Service-Management) richtet sich das IT-Referat maßgeblich am Ziel der Sicherung der digitalen Souveränität Münchens aus:*
>
> *- Wie vom Stadtrat im November 2020 beschlossen kommen sowohl im Anwendungs- als auch im Infrastruktur-Bereich priorisiert Open Source-Lösungen zum Einsatz, um Herstellerabhängigkeiten zu vermeiden. Die Bedingung „wenn wirtschaftlich und technologisch oder strategisch sinnvoll“ wird allerdings neu gefasst in „wenn keine*

gravierenden wirtschaftlichen, technischen oder fachlich funktionalen Gründe dagegen sprechen“.

- Kompatibilitätsanforderungen und Schnittstellennormen sind in Ausschreibungen jeweils so zu formulieren, dass offene ISO-Standards maßgeblich sind. Der Bezug auf proprietäre Produkte ist konsequent zu vermeiden.

- Bei jeder längerfristigen Festlegung in relevanten Einsatzbereichen werden eingehend die Auswirkungen auf die städtische Entscheidungshoheit über zukünftige Anbieterauswahl, kommunale Daten und kommunale Ausgaben beleuchtet und dem Stadtrat hierzu an geeigneter Stelle Bericht erstattet.

Begründung

*In der Vergangenheit gab es des Öfteren erhebliche Lizenzkostensteigerungen bei proprietärer Software zulasten der Nutzer*innen und auch der Landeshauptstadt München. Auch warnende Stimmen, sich gerade bei Software und Cloud-Computing nicht einseitig abhängig von unter US-amerikanischer Jurisdiktion stehender Konzerne zu machen, gibt es schon länger. Der aktuelle Zustand der transatlantischen Beziehungen erfordert aber eine grundsätzliche Neubewertung bezüglich Daten- und Kostensicherheit beim Bezug von IT-Produkten:*

*Der seit längerem bestehende Konflikt zwischen US-amerikanischem CLOUD Act und europäischer Datenschutz-Grundverordnung birgt angesichts der stark unter Druck geratenen US-amerikanischen Justiz zunehmend reale Risiken für die Datensicherheit. Im aktuellen Handelsstreit und der Debatte um Strafzölle werden europäische Regelungen wie der Digital Services Act von der US-Regierung und US-Tech-Unternehmen direkt attackiert. Es ist nicht mehr undenkbar, dass beispielsweise das Bereitstellen notwendiger Sicherheits-Updates irgendwann als politisches Druckmittel missbraucht wird oder digitale Produkte und Dienstleistungen mit hohen Strafzöllen belegt werden. Vor diesem Hintergrund erhöht sich die Notwendigkeit, deutsche und europäische Abhängigkeiten zu verringern und die Daten von Bürger*innen und Unternehmen bestmöglich vor externen Zugriffen zu schützen.*

Akteure aus Politik und Wirtschaft in Deutschland und Europa erhöhen aufgrund ihrer Sicherheitsbedenken aktuell die Anstrengungen für mehr digitale Souveränität. Notwendig ist das vor allem in den so strategisch relevanten Bereichen Software, Cloud Computing, Sicherheit und Plattformen. Für kommunale IT wird sich in absehbarer Zeit daher gegebenenfalls deutlich der Handlungsrahmen ändern und kommunale IT wird selbst zur strategischen Komponente. Mit der Abschaltung eines von einem russischen IT-Hersteller bezogenen Virenscanners in Folge des russischen Angriffskrieges auf die Ukraine hat das IT-Referat gezeigt, wie schnell es auf aktuelle geopolitische Herausforderungen reagiert. Natürlich sind nicht immer kurzfristige Lösungen direkt umsetzbar, digitale Souveränität erfordert einen langen Atem.

Die Landeshauptstadt München hat früh das Prinzip der digitalen Souveränität in ihrer Digitalisierungsstrategie verankert, setzt eine Vielzahl an FOSS-Anwendungen ein, hat eigene Anwendungen entwickelt und veröffentlicht und mit Projekten wie dem Open Source Dashboard oder dem Open Source Sabbatical sichtbare Akzente gesetzt. Nun sollen die strategische Beschaffung von europäischen IT- sowie Open Source-Produkten und – wo diese noch nicht ausreichend zur Verfügung stehen – die strukturelle Suche nach geeigneten Alternativen intensiviert werden. Angesichts der nachdrücklichen Forderungen aus Politik, Wirtschaft und Zivilgesellschaft zur Verringerung von Abhängigkeiten und der notwendigen Planbarkeit von städtischen Finanzen soll digitale Souveränität hierbei als strategisches Leitprinzip richtungsweisend sein.

Dieser Antrag fordert, dass sich das IT-Referat bei Beschaffungen oder Vertragsverlängerungen maßgeblich am Ziel der Sicherung der digitalen Souveränität Münchens ausrichte.

4.2.1. Priorisierter Einsatz von Open Source-Lösungen

Als ein Werkzeug zur Sicherstellung der digitalen Souveränität nennt der Antrag den priorisierten Einsatz von Open Source-Lösungen. Diese Vorgabe besteht bereits heute als integraler Bestandteil der IT-Strategie des IT-Referats[5] und ist gängige Praxis, doch soll sie, so die Forderung des Antrags, weiter geschärft werden:

> *Die Bedingung „wenn wirtschaftlich und technologisch oder strategisch sinnvoll“ wird allerdings neu gefasst in „wenn keine gravierenden wirtschaftlichen, technischen oder fachlich funktionalen Gründe dagegen sprechen“.*

Open Source ist aus Sicht des IT-Referats ein wesentlicher Baustein dafür, dass die angestrebte Souveränität erhalten bzw. erreicht wird. Dies findet seinen Ausdruck u. a. darin, dass bei allen IT-Projekten im Rahmen der Prüfung auf Konformität explizit die Verwendung von IT-Lösungen auf der Basis von Open Source abgefragt wird. Eine Abweichung davon muss durch IT-Architekt*innen bei it@M überprüft und genehmigt werden.

Die Entscheidungsfindung für den priorisierten Einsatz von Open Source wird bereits aufgrund der aktuellen Formulierung „…wirtschaftlich und technologisch oder strategisch sinnvoll“ erfolgreich umgesetzt, dies zeigen folgende Beispiele:

- Im Bereich IT-Infrastruktur (Serverbetriebssysteme, Datenbanken, Middleware, Webserver etc.) basieren mehr als 60 % der Lösungen auf Open Source-Software.
- Rund zwei Drittel der Server (mehr als 3.700) in den städtischen Rechenzentren verwenden Linux-basierte Betriebssysteme.
- Die stadtweiten IT-Identitäten, also die zentrale Entität für die Zugriffssteuerung und die Verwaltung von Rollen und Rechten in sämtlichen servergestützten IT-Systemen, werden mit der Open Source-Software Keycloak verwaltet.
- Für die Eigenentwicklungen von Fachanwendungen kommt eine Container-basierte Referenzarchitektur zum Einsatz, die komplett auf Open Source-Komponenten basiert.
- Open Source-Software wird in der IT-Sicherheit u. a. im Bereich der Bedrohungsanalyse genutzt: Ein spezieller MISP[6]-Server unterstützt die Verteilung von Informationen über Malware.

Das Grundprinzip Open Source wird durch das IT-Referat verantwortungsvoll gelebt, was u. a. durch die genannten Beispiele sehr deutlich wird. Der Aufbau eines Open Source Hubs und der Open Source Expertise im IT-Referat wie auch des Open Source Program Office (OSPO) bei it@M unterstreichen dies darüber hinaus.

Eigenentwicklungen der Landeshauptstadt München werden inzwischen regelmäßig als freie Software lizenziert und als Open Source über GitHub[7] und die Plattform OpenCode[8] veröffentlicht, was einen weiteren Beitrag zur Stärkung der digitalen Souveränität bildet, und zwar der eigenen wie auch der digitalen Souveränität der anderen öffentlichen Institutionen, die (jetzt und in Zukunft) von diesen Produkten Gebrauch machen.

Diese nachhaltige Verstetigung von Open Source in der IT-Landschaft der Landeshauptstadt München zeigt sich bereits auf Basis der aktuellen Formulierung.

Durch die vorgeschlagene Neuformulierung würde das Kriterium der Wirtschaftlichkeit herabgestuft, was aufgrund der Haushaltslage und der Vorgaben der Bayerischen Gemeindeordnung zur Wirtschaftlichkeit nicht in Betracht kommen (vgl. Stellungnahme der Stadtkämmerei und des Personal- und Organisationsreferats Abs. 6). Demzufolge

---

[5] https://opensource.muenchen.de/de/principles.html
[6] MISP: Malware Information Sharing Platform
[7] https://github.com/it-at-m/
[8] https://opencode.de/de und https://gitlab.opencode.de/landeshauptstadt-muenchen

muss das IT-Referat die Änderung der Formulierung ablehnen. Die Priorisierung von Open Source, wie durch die Formulierung verankert, gilt weiterhin.

4.2.2. Offene Standards

Eine weitere Forderung lautet:

> *Kompatibilitätsanforderungen und Schnittstellennormen sind in Ausschreibungen jeweils so zu formulieren, dass offene ISO-Standards maßgeblich sind. Der Bezug auf proprietäre Produkte ist konsequent zu vermeiden.*

Offene Standards sind ein wesentlicher Bestandteil jeder guten IT-Architektur und schon deshalb beim IT-Referat grundsätzlich präferiert und gefordert.[9]

Nichtsdestotrotz wird es auch künftig Fälle geben, in denen Bezüge auf proprietäre Produkte und Standards notwendig sein werden, nämlich immer dann, wenn bei der Landeshauptstadt München proprietäre Software im Einsatz ist, die nicht kurzfristig ersetzt werden kann, und Schnittstellen zu dieser Software benötigt werden. Beispiele hierfür sind SAP und die Microsoft-Produktfamilie. Auch wenn sich der Bezug auf proprietäre Produkte nicht vermeiden lässt, fordert das IT-Referat im Rahmen der Vergabe für die Integration derartiger Fachanwendungen die Einhaltung von offenen technischen Designprinzipien wie REST[10].

Das IT-Referat wird sicherstellen, dass eine wesentlich strengere Einforderung offener Standards zukünftig Bestandteil der städtischen Vergabeunterlagen sein wird.

4.2.3. Prüfung der Auswirkung auf städtische Entscheidungshoheit

Außerdem wird gefordert:

> *Bei jeder längerfristigen Festlegung in relevanten Einsatzbereichen werden eingehend die Auswirkungen auf die städtische Entscheidungshoheit über zukünftige Anbieterauswahl, kommunale Daten und kommunale Ausgaben beleuchtet und dem Stadtrat hierzu an geeigneter Stelle Bericht erstattet.*

Durch die Operationalisierung der Prüfung auf digitale Souveränität werden die Auswirkungen wie gefordert durch das IT-Referat betrachtet. Die Ergebnisse dieser Prüfung wird das IT-Referat dem Stadtrat jährlich vorlegen.

Der Antrag beschreibt in der Folge die in der Abhängigkeit von Softwareprodukten US-amerikanischer Großkonzerne bestehenden Risiken in Bezug auf Kosten und die digitale Souveränität. Diese Analyse stimmt mit dem Verständnis des IT-Referats überein.

4.3. Digitale Souveränität als strategisches Leitprinzip II – Risikoanalyse, Alternativen und Umstiegsszenarien

Antragstext

> *Wo Open Source-Lösungen bei den anstehenden strukturell und finanziell relevanten Beschaffungen oder Vertragsverlängerungen im Bereich IT im Einzelfall (noch) keine gangbare Alternative darstellen, wird das IT-Referat gebeten*
>
> *- Lock-in-Effekte zu vermeiden,*

---

[9] Vgl. auch Beschluss des IT-Ausschusses vom 19.02.2025, Sitzungsvorlage Nr. 20-26 / V 15347 „Die Daten müssen fließen“: https://risi.muenchen.de/risi/dokument/v/8854712

[10] REST: Representational State Transfer. Offenes Designprinzip für die Maschine-zu-Maschine-Kommunikation

- in direktem Austausch mit den Anbietern möglichst noch zusätzliche Sicherheitsgarantien auszuhandeln,

- eine kontinuierliche Marktbeobachtung sicherzustellen und zu geeignetem Zeitpunkt Umstiegsszenarien zu planen.

Zusätzlich wird das IT-Referat gebeten, seinen fachlichen Austausch zu digitaler Souveränität mit Bund, Ländern und anderen Kommunen zu intensivieren und den IT-Ausschussmitgliedern im Herbst über sich abzeichnende Projekte auf Bundes- und Europaebene zu berichten und welche kurz-, mittel- und langfristigen Möglichkeiten sich hierfür für Münchens digitale Souveränität ergeben. Dabei ist insbesondere zu prüfen, welche europäischen Cloud-Anbieter für die öffentliche Verwaltung eine mögliche Alternative darstellen und wie sich die Landeshauptstadt München auch politisch dafür einsetzen kann, dass es ggf. auf europäischer Ebene zum Aufbau eines solchen Anbieters kommt.

Begründung

Siehe Begründung unter 4.2.

Hier wird das IT-Referat gebeten, in Fällen, in denen andere als Open Source-Lösungen beschafft werden, folgende Aspekte besonders zu beachten:

4.3.1. Vermeidung von Lock-in-Effekten

Diesem Ziel dient zum einen die schon unter Ziff. 0angeführte Ausrichtung an offenen Standards. Diese Vorgabe ermöglicht im Zusammenspiel mit der EAI[11]-Bebauungsrichtlinie der Landeshauptstadt München z. B. den Austausch von IT-Lösungen, die mit anderen Softwareprodukten per Schnittstelle interagieren, ohne dass bei diesen anderen Softwareprodukten große Veränderungen erforderlich werden.

Die EVB-IT-Vertragsunterlagen für Cloud der Landeshauptstadt München fordern den Export von Daten, die für die Landeshauptstadt am Ende eines Cloud-Services relevant sind, als zwingendes (A-) Kriterium. Diese Regelung ist eine Voraussetzung, dass künftig auf eine funktional ähnliche Fachanwendung bei einem anderen Cloud-Anbieter oder im eigenen Rechenzentrum umgestiegen werden kann, was auf die Anforderung nach „Selbstbestimmtheit“ (s. Ziff. 2.2.) einzahlt.

4.3.2. Aushandeln zusätzlicher Sicherheitsgarantien mit den Anbietern

Hiervon macht das IT-Referat bereits nach Kräften Gebrauch. Mit Unternehmen wie Cisco im Kontext der Nutzung von Webex, ServiceNow und SAP konnten jeweils Vereinbarungen getroffen werden, die sicherstellen, dass Daten der Landeshauptstadt München ausschließlich in europäischen Rechenzentren und unter vollständiger Berücksichtigung der DSGVO verarbeitet werden dürfen.

Derartige Verhandlungen und Vertragsabschlüsse sind – auch wegen der in Ziff. 3.3. angesprochenen Kräfteverhältnisse zwischen Anbietern und der Landeshauptstadt München – außerordentlich anspruchsvoll und sie gehen mit signifikanten Aufwänden bei der Technik, dem Management, der Vergabestelle und der Rechtsabteilung einher.

---

[11] EAI: Enterprise Application Integration. Diese Bebauungsrichtlinie legt fest, dass Schnittstellen stets über eine Middlewarearchitektur umgesetzt werden, sodass zwei Softwareprodukte nicht per Schnittstelle direkt miteinander kommunizieren, sondern jeweils über Middleware-Server, die den gesamten Datenverkehr managen und die zu übertragenden Daten aus dem Format der einen Anwendung in das Format der anderen transformieren.

4.3.3. Kontinuierliche Marktbeobachtung

Eine zwar nicht kontinuierliche, aber regelmäßige Marktbeobachtung stellt das IT-Referat dadurch sicher, dass Verträge grundsätzlich auf wenige Jahre befristet sind und danach neu ausgeschrieben bzw. abgerufen werden müssen. Einer Ausschreibung geht bei der Landeshauptstadt München immer eine MBUC[12]-Analyse voraus, die zwingend eine aktuelle Markterkundung vorsieht.

Der Markt wird aus einer Reihe unterschiedlicher Perspektiven verteilt über alle Referate der Stadt beobachtet: Bei it@M von den verantwortlichen Service Ownern und IT-Architekt*innen, in den IT nutzenden Referaten durch die Facharchitekt*innen und die führenden Fachanwender*innen (Key User). Deswegen sieht es das IT-Referat als hinreichend sichergestellt an, dass die Landeshauptstadt München jeweils rechtzeitig davon erfährt, wenn der Markt (der kommerzielle wie der freie) neue Konzepte, Vorgehensweisen und Produkte hervorbringt.

4.3.4. Planung von Umstiegsszenarien

In der Antragsbegründung wird als positives Beispiel für einen schnellen Umstieg der Wechsel des stadtweit eingesetzten Virenscanners (von Kaspersky auf SentinelOne) genannt und einschränkend angemerkt, dass „nicht immer kurzfristige Lösungen direkt umsetzbar“ sind. Tatsächlich sind Umstiegsszenarien namentlich bei großflächig eingesetzten Produkten, die in massenhaftem Einsatz sind und viele Schnittstellen zu anderen Produkten und Prozessen aufweisen, überaus komplex und kostenintensiv. Als Beispiel sei nur auf den derzeit laufenden Umstieg des Rechnungswesens der Stadtkämmerei von der bisherigen SAP-ERP-Lösung auf das neuere SAP S/4HANA, also das Projekt neoFIN (vormals digital/4finance), verwiesen. Der Aufwand ist beträchtlich, obwohl hier der Umstieg geordnet (und nicht unter plötzlich entstandenem Druck) und innerhalb der Produkte eines einzigen Herstellers mit umfänglicher Unterstützung durch diesen erfolgt. Der Aufwand, den der Umstieg zu einem ganz anderen Produkt bedeuten würde, ist noch weitaus höher zu veranschlagen.

Auch bei Softwareprodukten mit geringerer Komplexität als SAP ist es immer wieder der schiere Aufwand, der gegen einen Umstieg von einem Produkt zu einem anderen spricht und der nicht selten dazu führt, dass an bekanntermaßen nicht optimalen Lösungen über längere Zeiträume hinweg festgehalten wird, obwohl präsumtiv bessere verfügbar sind. Dabei ist zu beachten, dass der Aufwand keineswegs ausschließlich oder auch nur überwiegend im IT-Referat bzw. bei it@M anfällt. Auch für die die jeweilige IT-Lösung nutzenden Fachreferate kann der durch den Wechsel der Lösung bedingte Aufwand erheblich sein: Je nach Gegebenheiten müssen Organisationsstrukturen und Prozesse angepasst und Mitarbeiter*innen (um)geschult werden.

Ein Umstieg auf ein anderes Produkt wird vom IT-Referat immer bei einem Vertragsende erwogen oder während der Laufzeit bei signifikanten sicherheitstechnischen, lizenztechnischen und/oder politischen Veränderungen.

4.4. Ausblick

Die Stadtratsanträge zeigen dem IT-Referat, dass die Stadtratsfraktionen die Sorge des IT-Referats um die digitale Souveränität teilen und dass es bei den bisherigen und allen kommenden Maßnahmen zur Stärkung der digitalen Souveränität mit der Zustimmung und Unterstützung des Stadtrates rechnen kann.

---

[12] MBUC: Systematische Prüfung der Optionen Make, Buy, Use und Compose als obligatorische Voraussetzung für den Start eines IT-Projekts

Angeregt durch die Stadtratsanträge zur digitalen Souveränität sind die Arbeiten zur digitalen Souveränität im IT-Referat beschleunigt und auch die Zusammenarbeit mit anderen Organisationen wie z. B. ZenDiS, Open Source Business Alliance und Dataport intensiviert worden. Sie sollen in Zukunft noch weiter intensiviert werden.

Der jetzt neu entwickelte Softwarecheck auf digitale Souveränität in der Version 1.0 wird vom IT-Referat in Zukunft fortgeschrieben und weiterentwickelt. Er dient als Grundlage, das Thema digitale Souveränität sachlich strukturiert im Rahmen der gesamten Risiko-Betrachtung zu adressieren und zu bewerten und so letztlich die für die Landeshauptstadt München erforderliche digitale Souveränität weitestgehend zu fördern.

5. Klimaprüfung

Ist Klimaschutzrelevanz gegeben: Nein

Die Beschlussvorlage thematisiert die digitale Souveränität als strategisches Leitprinzip für den Einsatz sicherer Software bei der LHM. Damit sind keine relevanten Änderungen im Zusammenhang mit dem der LHM zuzurechnenden Ausstoß von Treibhausgasen verbunden.

Das Ergebnis der Klimaschutzprüfung wurde mit dem RKU vorab abgestimmt.

6. Abstimmung mit den Querschnitts- und Fachreferaten

Querschnitts- bzw. Fachreferat	Anmerkung	Stellungnahme des IT-Referats
KR, RAW, MK, BAU, MOR, RKU, GPR, SOZ, KULT, PLAN		Das RIT dankt herzlich für die Zustimmung und Unterstützung.
Stadtgüter München, Märkte München, KGL	Diese Referate haben „Fehlanzeige“ gemeldet.	
SKA	"Die Stadtkämmerei unterstützt unbedingt die Wichtigkeit dieses Themas. Allerdings dürfen aufgrund der Haushaltslage und der Vorgaben der GO zur Wirtschaftlichkeit die Bedingungen für den Einsatz von Open Source nicht aufgeweicht werden. Das Kriterium Wirtschaftlichkeit ist insofern nicht herabzustufen."	In Ziff. 4.2.1 und im Antrag der Referentin in Punkt 4 wurde der letzte Satz umformuliert, um diesem Hinweis Rechnung zu tragen.
KVR	"... sollte unter Punkt 4.3.4 näher dargelegt werden, welche Rolle, die in der Beschlussvorlage erwähnten, zusätzlichen Kosten für die Referate in der Wirtschaftlichkeitsbetrachtung und der Entscheidung für eine Open Source Lösung spielt. Außerdem	Dieser Hinweis sollte durch die Änderung der Formulierung in Ziff. 4.2.1 und im Antrag der Referentin in Punkt 4 (s.o.) erledigt sein.

	bitten wir um Darstellung, wie diese Kosten in den Referaten finanziert werden sollen."	
KVR	"Des Weiteren werden bereits regelmäßig Eigenentwicklungen der LHM als freie Software lizenziert und auf den bekannten Plattformen veröffentlicht. Neben der Stärkung der digitalen Souveränität, die hiermit geleistet wird, gibt diese Praxis jedoch auch Einblicke in den Aufbau der städtischen IT. Daher sollten aus Sicht des Kreisverwaltungsreferates diese Veröffentlichung nochmals kritisch unter den Aspekten der IT- und Cybersicherheit betrachtet werden."	Bei der Veröffentlichung von Code achtet das RIT akribisch darauf, sensible Informationen auszuschließen. So werden beispielsweise Konfigurationsdateien, die Serveradressen o.ä. beinhalten, grundsätzlich nicht veröffentlicht, sondern in einem nur intern zugänglichen Code-Repository verwaltet. Die Geheimhaltung von Funktionsweisen als Sicherheitsmaßnahme (security by obscurity) gilt ansonsten als sehr unzuverlässiger Ansatz, der in modernen IT-Sicherheitskonzepten keine Rolle spielt.
KVR	"In der Beschlussvorlage sollte ... transparent abgebildet werden, wie mit amerikanischen Cloudanbietenden umgegangen wird, deren europäische Rechenzentren ebenfalls dem Cloud Act unterliegen."	Das entscheidende Kriterium bei der Bewertung von Cloudanwendungen ist der Sitz des Mutterkonzerns (vgl. Anlage Souveränitätscheck). Die zentrale Maßnahme ist die Vereinbarung von zusätzlichen sicherheitstechnischen Maßnahmen bei der Nutzung von Cloudservices von nicht-EU-Anbietern.
POR	"Es wird leider nicht dargestellt, welche Open-Source-Lösungen sich in der Vergangenheit als nicht geeignet erwiesen haben und daher nicht mehr im Serviceangebot von it@M verfügbar sind. An dieser Stelle wird auf LIMUX und Digi-WF beispielhaft verwiesen, von deren Einsatz aus nachvollziehbaren Gründen wieder abgesehen wurde."	Bei der Entscheidung für oder gegen eine Softwarelösung steht immer ihre Eignung für den vorgesehenen Einsatzzweck als Kriterium an erster Stelle. Aus Sicht des RIT war für die Entscheidung gegen Limux und DigiWF nicht die Tatsache ausschlaggebend oder auch nur relevant, dass es sich um OpenSource-Lösungen handelt.
POR	"Die Ziffer 4 des Antrags der Referentin wird kritisch gesehen, da sie dem Grunde nach als Beweislastumkehr zu verstehen ist. Gerade in wirtschaftlich herausfordernden Zeiten sollten	In Ziff. 4.2.1 und im Antrag der Referentin in Punkt 4 wurde der letzte Satz umformuliert, um diesem Hinweis Rechnung zu tragen.

	stets alle gefundenen Software-Lösungen nach dem gleichen Schema bewertet werden. Eine marktgängige Lösung auszuschließen, weil beim Open-Source-Konkurrenzprodukt keine „gravierenden […] fachlich funktionalen Gründe dagegen sprechen“, sollte nicht der Maßstab sein."	
MSE	"... muss vor Entscheidungen über eine IT-Lösung zwingend auch die bestmögliche Erfüllung der vorhandenen fachlichen Anforderungen aus wirtschaftlicher und technischer Sicht sowie die notwendige Usability berücksichtigt werden."	Bei der Entscheidung für oder gegen eine Softwarelösung steht immer ihre Eignung für den vorgesehenen Einsatzzweck als Kriterium an erster Stelle.
MSE	"... keine Diskussion zur Ablösung etablierter proprietärer Standardanwendungen wie SAP oder MS-Office durch eine Open-Source-Lösung ..., um u. a. Planungssicherheit zu behalten und erhebliche Migrationskosten (falls es überhaupt technisch mögliche Alternativen gibt) sowie Einbußen in der Funktion und Usability zu vermeiden."	Die BV legt in Ziff. 4.3.4 dar, dass der Umstieg von einer Software auf eine andere gut erwogen sein muss. Die genannten Produkte SAP und MS-Office stehen derzeit nicht zur Debatte.
AWM	"... Einsatz proprietärer Software dort sinnvoll, wo sie eine bessere Usability, eine verlässlichere Integration in bestehende Verfahren oder einen einfacheren Austausch mit Bürger*innen und anderen Institutionen ermöglicht."	Bei der Entscheidung für oder gegen eine Softwarelösung steht immer ihre Eignung für den vorgesehenen Einsatzzweck als Kriterium an erster Stelle.
AWM	"Wichtig ist in diesem Zusammenhang, dass die Besonderheiten eines Betriebes der kritischen Infrastruktur Beachtung finden."	Gerade bei kritischen Infrastrukturen ist der Aspekt der digitalen Souveränität besonders gewichtig – und kritisch. Deshalb können Open Source-Lösungen in diesem Kontext besonders sinnvoll sein. Es gilt aber vor allem das zuvor Gesagte (erstes Kriterium ist die Eignung für den vorgesehenen Einsatzzweck), sodass die Auswahl einer Lösung in jedem einzelnen Fall separat zu bewerten und zu entscheiden ist.

DIR	"Ziff. 4.1.2 Abs. 2 Nach dem Satz „In den produktiven Betrieb kann in der IT-Landschaft der Landeshauptstadt München nur gelangen, was im Rahmen des Informationssicherheitsmanagments systematisch geprüft und nach Annahme der Restrisikodeklaration durch den beauftragenden Fachbereich freigegeben wurde.“ sollte folgender Satz ergänzt werden: „Des Weiteren ist auch die datenschutzrechtliche Prüfung (und ggf. Restrisikoübernahme durch den Verantwortlichen) Voraussetzung für die Produktivnahme von IT-Lösungen.““	Der Satz wurde wunschgemäß in Ziff. 4.1.2 eingefügt.
DIR	"In die Aufzählung in dem Satz „Notwendig ist das vor allem in den so strategisch relevanten Bereichen Software, Cloud Computing, Sicherheit, und Plattformen.“ sollte der Datenschutz als strategisch relevantes Kriterium mit aufgenommen werden ..."	Die zitierte Formulierung ist Teil des Zitats aus dem Antrag Nr. 20-26 / A 05710 "Digitale Souveränität als strat. Leitprinzip I – Beschaffungen" von der Fraktion Die Grünen - Rosa Liste vom 26.06.2025. Änderungen an diesem Text vorzunehmen steht dem RIT nicht zu.
Gleichstellungsstelle für Frauen	"die GSt zeichnet die Sitzungsvorlage mit, wenn unter Punkt 1 ein weiterer Aufzählungspunkt 'Geschlechtergleichstellung' aufgenommen wird."	Der Punkt wurde der Aufzählung unter Ziff. 1 hinzugefügt.
RKU	"In der Beschlussvorlage empfehlen wir folgenden Satz am Ende des Kapitels „Klimaprüfung“: „Das Ergebnis der Klimaschutzprüfung wurde mit dem RKU vorab abgestimmt.““	Der Textvorschlag wurde an Ziff. 5 angehängt.
RBS	"Wir gehen davon aus, dass der Fokus der Beschlussvorlage auf der reinen Verwaltungsseite liegt, die pädagogischen Bereiche inkl. der LHM-S nicht eingeschlossen sind."	Es trifft zu, dass sich diese Beschlussvorlage vorrangig auf die vom RIT (und it@M) verantworteten Entscheidungen für oder gegen einzelne Software-Lösungen bezieht.

RBS	"Ziff. 3.2 'durch das sehr kompetente IT-Personal … und it@M' bitte zufügen 'GPAMS der Fachreferate'"	Die Ergänzung wurde wunschgemäß in Ziff. 3.2 eingefügt.
RBS	Bei digitaler Souveränität eine Aussage zur Effizenz bei der Nutzung von neuen Service EfA Service zufügen.	Für das RIT ist es grundsätzlich sehr interessant bei der Nutzung von neuen Services auf EfA Services zurückzugreifen. Inweit der Einsatz eines einzelnen EfA Service für die LHM effizient ist, hängt von einer ganzen Reihe von Faktoen ab. Diese zu betrachten ginge über die Beantwortung der vorliegenden Stadtratsanträge hinaus.
GSR	„Die oberste Priorität bei der Beschaffung digitaler Lösungen müssen die fachliche Eignung und der zuverlässige Betrieb sowie die verantwortliche Wartung und Pflege entsprechender Lösungen haben, damit die fachliche Aufgabenerfüllung gesichert ist. Wenn im konkreten Fall auch Open-Source-Lösungen diese Anforderung erfüllen, spricht nichts gegen ihren Einsatz.“	Ja, bei der Entscheidung für oder gegen eine Softwarelösung steht immer ihre Eignung für den vorgesehenen Einsatzzweck als Kriterium an erster Stelle.
GSR	„ Das GSR beobachtet jedoch in verschiedenen Vergabeverfahren für die Beschaffung von Standardsoftware, dass jede weitere interne städtische Festlegung und Regulierung höhere Aufwände bei allen internen Beteiligten, aber auch bei den teilnehmenden Bieterunternehmen verursacht.“	Ja, jede weitere interne städtische Festlegung und Regulierung im Vergabeverfahren erhöht die Aufwände intern wie extern. Das IT-Referat ist bestrebt jede zusätzliche neue Festlegung so umzusetzen, dass sie möglichst wenig zusätzlichen Aufwand verursacht.
GSR	…„ Dementsprechend dürfen auch die Vorgaben zur Bevorzugung von Open-Source- Lösungen nicht dazu führen, dass bei entsprechenden Vergaben unverhältnismäßige Aufwände entstehen oder keine Angebote abgegeben werden und im Ergebnis kritische Geschäftsprozesse der Landeshauptstadt München den Wegfall ihrer digitalen Unterstützung riskieren.“	Eine Open Source Lösung wird ausgeschrieben, wenn auf dem Markt Open Source Lösungen verfügbar sind. Wenn keine Open Source Lösungen verfügbar sein sollten, wird ohne Open Source Lösungen ausgeschrieben. Dementsprechend behindert die Ausschreibung von Open Source Lösungen nicht die Möglichkeit, dass der LHM

		Software angeboten wird, die auf einem anderen Lizenzmodell beruhen.

Anhörung des Bezirksausschusses

In dieser Beratungsangelegenheit ist die Anhörung des Bezirksausschusses nicht vorgesehen (vgl. Anlage 1 der BA-Satzung).

Korreferentin (RIT) und Verwaltungsbeirat (RIT-I), Verwaltungsbeirätin (it@M)

Die Korreferentin des IT-Referats, Frau Stadträtin Sabine Bär, der zuständige Verwaltungsbeirat von RIT-I, Herr Stadtrat Lars Mentrup, und die Verwaltungsbeirätin von it@M, Frau Stadträtin Judith Greif, haben einen Abdruck der Sitzungsvorlage erhalten.

II. Antrag der Referentin

1. Der Stadtrat nimmt den Vortrag der Referentin zur Kenntnis, dass das IT-Referat Lock-in Effekte vermeidet, weitergehende Sicherheitsgarantien realisiert, kontinuierlich den Markt beobachtet und zu einem geeigneten Zeitpunkt Umstiegsszenarien plant. Darüberhinaus wird das IT-Referat offene Standards wesentlich strenger im Vergabeprozess einfordern.
2. Das IT-Referat wird beauftragt, die Methodik zur Prüfung auf digitale Souveränität weiterzuentwickeln und eine entsprechende Integration in die relevanten IT-Prozesse vorzunehmen.
3. Das IT-Referat wird beauftragt, den Stadtrat im Rahmen der bereits bestehenden jährlichen Bekanntgabe zu E- und Open-Government zum Stand der digitalen Souveränität zu informieren.
4. Das IT-Referat wird beauftragt, die Aktivitäten in der Operationalisierung zur Wahrung und Förderung der digitalen Souveränität selbständig fortzuführen.
5. Der Stadtratsantrag Nr. 20-26 / A 05673 Digitale Souveränität: Sichere Software für München von der SPD-Fraktion, Fraktion Die Grünen – Rosa Liste ist damit geschäftsordnungsgemäß erledigt.
6. Der Stadtratsantrag Nr. 20-26 / A 05710 Digitale Souveränität als strategisches Leitprinzip I – Beschaffungen von der Fraktion Die Grünen – Rosa Liste ist damit geschäftsordnungsgemäß erledigt.
7. Der Stadtratsantrag Nr. 20-26 / A 05711 Digitale Souveränität als strategisches Leitprinzip II – Risikoanalyse, Alternativen und Umstiegsszenarien von der Fraktion Die Grünen – Rosa Liste ist damit geschäftsordnungsgemäß erledigt.

III. Beschluss

nach Antrag.

Der Stadtrat der Landeshauptstadt München

Der Vorsitzende	Die Referentin
Dominik Krause	Dr. Laura Dornheim
2. Bürgermeister	Berufsm. Stadträtin

IV. Abdruck von I. mit III.

über die Stadtratsprotokolle

an das Direktorium - Dokumentationsstelle
an die Stadtkämmerei
an das Revisionsamt
z. K.

V. Wv. - RIT-Beschlusswesen