

Inhaltsprotokoll

Öffentliche Sitzung

Ausschuss für Digitalisierung und Datenschutz

68. Sitzung
9. März 2026

Beginn: 14.02 Uhr
Schluss: 15.47 Uhr
Vorsitz: Johannes Kraft (CDU)

Vor Eintritt in die Tagesordnung

Vorsitzender Johannes Kraft weist auf die vorgeschlagene Tagesordnung vom 27. Februar 2026 hin. Gebe es hierzu Anmerkungen oder Änderungswünsche?

Christopher Förster (CDU) bemerkt, dass die zahlreichen Zuschauerinnen und Zuschauer im Saal sicher hauptsächlich wegen der geplanten Diskussion zum Gesetz zur Änderung des Berliner Datenschutzgesetzes und weiterer Rechtsvorschriften gekommen seien. In den vergangenen Tagen hätten die Koalitionsfraktionen hierzu viele Fragen, Meldungen, Meinungen und Pressemitteilungen erreicht, so etwa von Frag Den Staat oder von der Berliner Datenschutzbeauftragten. Diese Meldungen würden sehr ernst genommen und man sei nun dabei, einige Punkte zu prüfen und gegebenenfalls zu ändern. Aus diesem Grund werde der Antrag gestellt, den Tagesordnungspunkt 3 heute zu vertagen.

Jan Lehmann (SPD) ergänzt, den Koalitionsfraktionen sei die Situation in Berlin – gerade mit Blick auf terroristische Anschläge – bewusst: Die Infrastruktur müsse geschützt werden. Es sei aber auch von herausragender Bedeutung, dass neue Schutzmaßnahmen gut durchdacht seien. Wenn aus der Zivilgesellschaft oder von der Datenschutzbeauftragten Mitteilungen zu den geplanten Änderungen an einem Gesetz kämen, müssten diese natürlich ernst genommen werden. Um die Mitteilungen seriös bewerten und gegebenenfalls Korrekturen vornehmen zu können, werde ein wenig Zeit benötigt. Deshalb solle der Punkt vertagt werden.

Marc Vallendar (AfD) hält fest, seine Fraktion sei zwar damit einverstanden, heute noch nicht über das Gesetz abzustimmen, es könne jedoch zumindest über den Entwurf diskutiert werden. Aus Sicht der Opposition seien einige Punkte zu besprechen; es sei nicht akzeptabel, dass ein Gesetzesentwurf nur bilateral zwischen CDU und SPD umgearbeitet werde. In der

Plenarsitzung sei der Entwurf noch als besonders dringlich präsentiert worden; die Koalition habe hier eine schnellstmögliche parlamentarische Behandlung angestrebt. Nun erbitte sie zusätzliche Zeit und beantrage eine Vertagung – dieses Vorgehen sei nicht nachvollziehbar. Die Abstimmung könne vertagt werden; aufgrund der handwerklichen Mängel am Entwurf, die diskutiert werden müssten, werde die AfD-Fraktion dem Vertagungsantrag im Ganzen jedoch nicht zustimmen.

Gollaleh Ahmadi (GRÜNE) bekräftigt, dass die Koalition den Gesetzesentwurf mit hoher Dringlichkeit habe beschließen wollen. Die Opposition habe stets den Eindruck geäußert, dass man sich für die Behandlung des Themas mehr Zeit hätte nehmen sollen. Die Zivilgesellschaft habe sich nun – wie erwartet – zu dem Vorhaben geäußert. Wenn die Vertagung dazu führen solle, dass die Koalition den Gesetzesentwurf noch einmal neu bewerten und nachbessern wolle, werde sich die Fraktion Bündnis 90/Die Grünen dem nicht in den Weg stellen. In der Abstimmung zur Vertagung werde man sich enthalten.

Elke Breitenbach (LINKE) unterstreicht, dass die Koalition der Behandlung des Themas mit großer Vehemenz eine hohe Dringlichkeit zugesprochen habe. Die Opposition habe schon früh um Zeit zum Nachdenken und Bewerten gebeten, da klare Kritikpunkte bestanden hätten. Die Vertagung sei also prinzipiell zu begrüßen; die Linksfraktion erwarte jedoch, dass sich die Koalition nun wirklich mit dem Gesetz und den diversen offenen Briefen und Stellungnahmen beschäftige. Auch die Berliner Datenschutzbeauftragte habe sich bereits ausführlich geäußert. Es bleibe zu hoffen, dass sich die Fehler am Entwurf noch heilen ließen und die Verzögerung nun zu mehr Transparenz und Information für die Zivilgesellschaft werde führen können.

Vorsitzender Johannes Kraft hält fest, alle Fraktionen hätten sich nun zu Wort gemeldet. Es lägen keine weiteren Fragen oder Wortmeldungen der Ausschussmitglieder vor.

Der **Ausschuss** beschließt mehrheitlich, der Antrag der Koalitionsfraktionen auf Vertagung des Tagesordnungspunktes 3 solle angenommen werden. Die Tagesordnung werde entsprechend geändert. – Weiteres: Siehe Beschlussprotokoll.

Punkt 1 der Tagesordnung

Aktuelle Viertelstunde

Carsten Schatz (LINKE) stellt die von seiner Fraktion zuvor schriftlich eingereichte Frage:

„Welche KI-Systeme setzen welche Senatsverwaltungen für welche Zwecke ein und wieso verschickt die Finanzverwaltung KI-Slop als Stellungnahme?“

Vorsitzender Johannes Kraft weist darauf hin, dass auch eine schriftliche Beantwortung der Frage möglich sei, sollte die Beantwortung im Rahmen einer Aktuelle Viertelstunde nicht möglich sein.

Staatssekretärin Martina Klement (Skzl) führt aus, dass es bis zum Inkrafttreten des neuen § 16a des E-Government-Gesetzes so gewesen sei, dass die Senatsverwaltungen KI-Systeme hätten ausprobieren dürfen, um eigene Erfahrungen sammeln zu können. Recht früh sei über ein Rundschreiben festgesetzt worden, dass die letzte Entscheidung immer beim Menschen liege – Rahmenbedingungen für die Nutzung von KI-Systemen habe es also gegeben, die Ressorts hätten diese jedoch nicht anzeigen müssen. Mit dem Inkrafttreten des § 16a sei eine Anzeigepflicht eingeführt worden: Die Senatskanzlei wolle einen Überblick darüber erhalten, welche KI-Tools in den Verwaltungen zur Anwendung kämen. Die Anzeigepflicht sei auch Teil der Rahmendienstvereinbarung, die mit dem Hauptpersonalrat ausgearbeitet werde.

Die Frage der Linken habe man zum Anlass genommen, die Senatsverwaltungen zu fragen, welche Chatbots und LLM derzeit in den Häusern verwendet würden. SenASGIVA nutze aktuell keinen eigenen KI-Chatbot, plane aber den Einsatz von BärGPT. SenFin habe DOK_KI und TREK_KI im Einsatz und prüfe ebenfalls die Nutzung von BärGPT. SenJust nutze zur juristischen Recherche Juris AI und den beck-chat. SenKult nutze keinen eigenen KI-Chatbot, führe aber BärGPT ein. SenMVKU habe gemeldet, derzeit keine KI-Tools zu verwenden. In der SenStadt stehe ein Pilotbetrieb für die Vorprüfung von Wohngeldanträgen an. SenWEB habe gemeldet, man wolle den DIWI-Chatbot launchen. SenWGP habe ebenfalls einen Piloteinsatz von DOK_KI und TREK_KI geplant und werde BärGPT einführen. Aus den anderen Senatsverwaltungen habe man keine aktuellen Rückmeldungen bekommen. – Sollte die Frage der Linken darauf abzielen, eine Liste wirklich aller KI-Systeme in der Berliner Verwaltung zu erhalten, müsse darüber an anderer Stelle weiter gesprochen werden.

Thorsten Steinmann (SenFin) präzisiert, die Senatsverwaltung für Finanzen habe DOK_KI, TREK_KI und BAK_KI im Einsatz. DOK_KI, ein Tool zur Zusammenfassung von Dateien, und TREK_KI, ein allgemeiner Chatbot, würden seit dem 18. November 2024 genutzt. Seit dem 1. Juli 2025 sei auch BAK_KI eingeführt; das Tool solle mit einer KI das Erstellen von Beschreibungen von Aufgabenkreisen – BAKs – unterstützen. Es solle bald landesweit zur Verfügung gestellt werden. Bislang werde BAK_KI in der Senatsverwaltung für Finanzen von den Führungskräften und Büroleitungen genutzt. Mit SenWGP sei eine Kooperationsvereinbarung abgeschlossen worden: Diese Senatsverwaltung nutze alle drei Applikationen.

Zur Frage nach der Stellungnahme sei zu sagen, dass im Justizariat des Hauses Noxtua verwendet werde, eine Erweiterung von beck-online. Das Tool komme nur im Justizariat und im Referat ZSA zum Einsatz. Eine Kollegin habe der Abteilung I, welche für das Rahmengesetz zuständig sei, eine Datei zusammengefasst, und auf der Basis der zusammengefassten Datei habe die Abteilung I weiter gearbeitet. Dabei seien die Textpassagen, die das Justizariat zur Verfügung gestellt hatte, gelöscht worden; trotzdem sei in den Dokumenteneigenschaften nur Noxtua abgebildet. SenInnSport und SenJust hätten das Word-Dokument dann noch weiter verändert; schließlich sei es dann dem Abgeordnetenhaus zur Verfügung gestellt worden. Die Stellungnahme sei also mitnichten von einer KI erstellt worden. Es habe nur eine Unterstützungsleistung des Justiziariats an die Abteilung I gegeben. In den Dateieigenschaften sei Noxtua jedoch noch ersichtlich gewesen.

Carsten Schatz (LINKE) bemerkt, Noxtua sei in der Aufzählung der verwendeten KI-Tools nicht vorgekommen. – Die Stellungnahme habe seine Fraktion als pdf-Dokument erreicht. Wäre das vorangehende Word-Dokument vor dem Konvertieren in eine pdf-Datei tatsächlich noch einmal bearbeitet worden, hätten sich die Dokumenteneigenschaften eigentlich anpassen

müssen. Könne noch etwas dazu gesagt werden, warum hier die KI als Verfasserin stehen geblieben sei?

Thorsten Steinmann (SenFin) antwortet, er könne technisch nicht beurteilen, wie die Vorgänge bei der Umwandlung von einer Word-Datei in eine pdf-Datei genau seien. Jemand habe aus der Word-Datei eine pdf-Datei generiert; die Dokumenteneigenschaft sei dabei erhalten geblieben.

Stefan Ziller (GRÜNE) stellt die von seiner Fraktion zuvor schriftlich eingereichte Frage:

„Wie steht es um den medienbruchfreien Anwohnerparkausweis bzw. wann ist mit dem Abschluss des Vorhabens zu rechnen?“

Staatssekretärin Martina Klement (Skzl) fragt, ob – wie angefordert – eine Vertretung der zuständigen SenMVKU anwesend sei. Sollte dies nicht der Fall sein, müsse die Antwort schriftlich nachgereicht werden. – Nach Kenntnisstand der CDO arbeite die SenMVKU mit dem Landesamt für Bürger- und Ordnungsangelegenheiten – LABO – daran, in einem ersten Schritt sicherzustellen, dass die Anwohnerparkberechtigung hinter dem Kennzeichen hinterlegt werden könne.

Christopher Förster (CDU) weist darauf hin, dass eine große Berliner Zeitung heute erneut über den IT-Dienstleister des Landes Berlin, das ITDZ, berichtet habe. Dieser befinde sich im Krisenmodus. Könne eine aktuelle Auskunft darüber gegeben werden, ob diese Informationen zutreffend seien?

Staatssekretärin Martina Klement (Skzl) bestätigt, dass über das ITDZ in den vergangenen Wochen und Monaten immer wieder berichtet worden sei. Zuletzt habe es eine Sitzung des Hauptausschusses gegeben, in der die Situation gemeinsam mit der Vorständin des ITDZ, Dr. Maria Borelli, dargelegt worden sei. Im Vergleich zu dieser Hauptausschusssitzung habe sich nicht viel verändert: Die Lage im ITDZ sei zweifelsohne angespannt. Es sei aber klarzustellen, dass in den Medien nun wiederholt falsch dargestellt worden sei, dass das ITDZ im vergangenen Jahr viele Millionen Euro und in diesem Jahr noch einmal 18 Millionen Euro Unterstützung erhalten habe. Diese Darstellung verschweige die Tatsache, dass das ITDZ den gesamten Kassenkredit, den es im vergangenen Jahr erhalten habe, vollständig zurückgezahlt habe. Es blieben aktuell lediglich die 18 Millionen Euro.

Zweitens sei das Land Berlin ein sehr säumiger Kunde. Auch hierüber sei im Hauptausschuss diskutiert worden. Es gelte zu bedenken, dass das Land Berlin an die Landeshaushaltsordnung gebunden sei, wenn es selbst Rechnungen bezahle: Rechnungen dürften erst zum Ende der Rechnungsfrist, also zur Fälligkeit, beglichen werden. Die Rechnungen des ITDZ seien bis vor Kurzem mit einer Zahlungsfrist von 30 Tagen gestellt worden. Dies habe dazu geführt, dass das Land Berlin erst zum Ende dieser Zahlungsfrist gezahlt habe. Aufgrund der Liquiditätsschwierigkeiten sei das Zahlungsziel nun auf 14 Tage verkürzt worden, sodass ein Zahlungsfluss schneller entstehen könne.

In den Presseberichten würden auch zahlreiche vakante Abteilungsleitungen erwähnt. Nach Kenntnisstand der CDO sei nur eine Stelle vakant. Es würden zudem anonyme Schreiben erwähnt, die in der Tat auch in der Senatskanzlei eingegangen seien. Alle Vorwürfe würden

ernst genommen und es werde ihnen nachgegangen. Es sei von außen nicht zuverlässig einzuschätzen, ob es sich um Einzelmeinungen handle oder ob eine überwiegende Meinung im ITDZ dargestellt werde. Deswegen solle eine anonyme Mitgliederbefragung durchgeführt werden, um zu klären, ob es sich um ein Massenphänomen oder Einzelmeinungen handle. Objektive Kriterien könnten die dargestellten Punkte, die als Massenphänomen beschrieben würden, bisher nicht bestätigen: Im Jahr 2022 habe es im ITDZ eine Fluktuationsquote von 9,32 Prozent gegeben; zuletzt habe diese nur noch bei 6,4 Prozent gelegen. Zumindest in der Fluktuationsquote schlugen sich die beschriebenen Probleme also nicht nieder.

Der Verwaltungsrat nehme die Darstellungen trotzdem ernst und begleite den Prozess weiter: Es gebe einen engen Austausch mit dem Personalrat des ITDZ, es werde eine Mitarbeiterbefragung geplant, und man sei im Austausch mit Wirtschaftsprüfern, um die Frage zu klären, ob eine Sonderprüfung beauftragt werden könne. Auch die interne Revision des ITDZ sei eingebunden. Man habe auch Kontakt mit dem Rechnungshof aufgenommen, um zu klären, ob und wie der Rechnungshof unterstützen könne. Die nächste Sitzung des Verwaltungsrats finde in der nächsten Woche statt. – Es sei insgesamt wichtig, die Lage beim ITDZ zu beruhigen, da der landeseigene Betrieb für die Zukunft der Hauptstadt einer der wichtigsten Player sei.

Vorsitzender Johannes Kraft stellt fest, dass keine weiteren Fragen oder Wortmeldungen vorlägen. Die Aktuelle Viertelstunde könne für die heutige Sitzung abgeschlossen werden.

Punkt 2 der Tagesordnung

Bericht aus der Senatskanzlei

Staatssekretärin Martina Klement (Skzl) berichtet wie üblich von den Terminen und Veranstaltungen seit der letzten Ausschusssitzung am 23. Februar 2026. Am folgenden Dienstag, den 24. Februar, habe eine Senatssitzung stattgefunden, in der insgesamt drei Themen aus dem Bereich der CDO besprochen worden seien: die Multi-Cloud-Strategie, der Bericht zum Sachstand der Implementierung der Verwaltungsreform und der letzte vierteljährliche Bericht zu den Ausnahmen von der Abnahmepflicht durch das ITDZ nach dem E-Government-Gesetz. Am Donnerstag, den 26. Februar, habe eine Plenarsitzung im Abgeordnetenhaus stattgefunden. Außerdem sei am gleichen Donnerstag das Digitalkabinett zu einer kurzen Sondersitzung zusammengekommen, in der zum Beispiel der Data Hub für das Land Berlin thematisiert worden sei. Als Nächstes sei zu diesem Thema eine Senatsbefassung geplant. Am Freitag, den 27. Februar, habe es gemeinsam mit der Bildungsverwaltung einen Pressetermin an der Ernst-Haeckel-Schule in Marzahn-Hellersdorf gegeben, bei dem gefeiert worden sei, dass nun alle Berliner Schulen mit leistungsfähigem Internet versorgt seien. Das Vorhaben, dessen Umsetzung bis zum Ende des Jahres geplant gewesen sei, sei nun schneller realisiert worden als gedacht. Am Freitag habe auch eine politische Spitzenrunde zur Verwaltungsreform stattgefunden: Hier sei es insbesondere um den Aufgabenkatalog für die Berliner Verwaltung gegangen, dessen erster Entwurf sich derzeit im senatsinternen Mitzeichnungsverfahren befinde, und um das Konnexitätsausführungsgesetz, bei dem man sich mit Blick auf die inhaltliche Ausgestaltung eines Entwurfs auf der Zielgeraden befinde. Die erste Senatsbefassung könne voraussichtlich zügig beginnen.

In der vergangenen Woche habe die CDO die CODE University besucht, um sich einen Überblick über die dortigen Angebote der Fachkräfteausbildung zu verschaffen. Es sei außerdem eine Delegation aus dem Südtiroler Landtag zu Gast in Berlin gewesen: Es seien ganz ähnliche Erfahrungen und Herausforderungen mit den Themen Digitalisierung und Verwaltungsmodernisierung ausgetauscht worden. – Am Mittwoch, den 4. März, habe die CDO im Rahmen des Fachkongresses Digitaler Staat mit anderen Länder- und Firmenvertretern an einer Paneldiskussion zum Thema KI teilgenommen. Zeitgleich habe an diesem Mittwoch eine Sitzung des Hauptausschusses stattgefunden, in der eigentlich die Migrationsreife der Verwaltungsgebäude hätte besprochen werden sollen. Das Thema sei in die nächste Sitzung verlagert worden.

In der laufenden Woche werde am morgigen Dienstag, den 10. März, wieder eine Senatsitzung stattfinden. Man habe sich heute bereits darauf verständigt, die Vergabestrukturen voraussichtlich in der nächsten Sitzung des Senats zu beschließen – was zu begrüßen wäre, da es sich bei der Vergabestrukturenreform um einen zentralen Baustein im Prozess der Verwaltungsmodernisierung handle. Es werde in dieser Woche außerdem weitere Aktionen zum mobilen Bürgeramt geben, und am Donnerstag stehe das nächste Plenum auf dem Programm. Am Freitag, den 13. März, werde der Fachausschuss des Rats der Bürgermeister tagen und sich mit den Themen Vergabestrukturenreform und Verwaltungsreform, hier insbesondere mit dem Aufgabenkatalog, beschäftigen. Mit Blick auf die Verwaltungsreform seien außerdem Fortschritte zu den Reformwerkstätten zu verzeichnen, die für einzelne Themen zeitnah eingesetzt werden sollten, um sich – aufbauend auf dem Aufgabenkatalog – auch dem Thema der Aufgabenkritik widmen zu können.

Abschließend könne darauf hingewiesen werden, dass der Chatbot zur Behördennummer 115 aus dem föderalen Kontext derzeit im Serviceportal des Landes Berlin pilotiert werde. Das Angebot erfreue sich großer Beliebtheit: Knapp 140 000 Nutzungen seien seit der Inbetriebnahme verzeichnet worden. Insbesondere die Funktion, mit der das Portal in bestimmten Fremdsprachen durchsucht werden könne, scheine sehr gut anzukommen. Nun solle das Angebot verstetigt und ausgebaut werden.

Vorsitzender Johannes Kraft stellt fest, dass zu diesem Bericht keine Fragen oder Wortmeldungen vorlägen.

Meike Kamp (Berliner Beauftragte für Datenschutz und Informationsfreiheit) berichtet, dass es im Innenausschuss eine Erörterung der KI-Mustererkennung durch Videotechnik – unter anderem zu Zwecken des Objektschutzes – gegeben habe. Bei dieser Gelegenheit sei auch über die Beteiligung der Berliner Datenschutzbeauftragten gesprochen worden. Hierzu habe es Ende Januar einen Termin bei der Polizei gegeben, die das Projekt auf einem noch sehr abstrakten Niveau vorgestellt habe: Es sei zu diesem Zeitpunkt noch im Ausschreibungsverfahren gewesen. Es habe keine näheren inhaltlichen Informationen zu konkreten rechtlichen oder technischen Ausgestaltungen gegeben. Bei dem Termin habe die Datenschutzbeauftragte jedoch auf bestimmte Problemfelder hingewiesen, unter anderem darauf, dass eine Anonymisierung von Skelettdaten bei Videotechnik und KI-Mustererkennung nicht trivial sei. Vor dem Hintergrund der nicht ausreichenden Informationen habe man aber keine abschließende Bewertung des Projekts vornehmen können. Der Einsatz der Videoüberwachung werde nun weiter begleitet und man hoffe, dass die Polizei weiterhin die notwendigen Informationen liefern werde. Zu gegebenem Zeitpunkt könne im Ausschuss darüber berichtet werden.

Weiterhin seien auch mehrere Datenschutzbeauftragte der Länder beim Kongress Digitaler Staat mit einem Stand vertreten gewesen; sie selbst habe hier zum Thema KI und Datenschutz gesprochen. Auch bei der Bildungsmesse Didacta werde es einen gemeinsamen Stand geben: Hier sollten Lehrerinnen und Lehrer im Hinblick auf Datenschutz beraten und das Projekt „Young Data“ vorgestellt werden.

Stefan Ziller (GRÜNE) hält fest, seine Fraktion würde sich freuen, wenn die Datenschutzbeauftragte berichten könne, sobald die Polizei bekannt gebe, welche Daten sie genau erheben wolle. Man habe hierzu bislang keine Informationen erhalten; ein KI-System zum Objektschutz sei mit seiner Überwachung und Mustererkennung im Kontext der Informationsfreiheit jedoch auch für Besucherinnen und Besucher des Abgeordnetenhauses und die Arbeit im Haus relevant. Er schlage vor, dass sich auch der Ausschuss mit dem Thema befassen solle, gegebenenfalls gemeinsam mit der Polizei.

Elke Breitenbach (LINKE) gibt an, ihre Fraktion habe von dem Projekt durch eine Ausschreibung erfahren. Könne die Datenschutzbeauftragte noch einmal darlegen, wie sie die Videoüberwachung gerade im Hinblick auf Berufsgeheimnisträgerinnen und -träger bewerte, zu denen auch Abgeordnete oder die Mitarbeitenden an Gerichten gehörten?

Meike Kamp (Berliner Beauftragte für Datenschutz und Informationsfreiheit) wiederholt, sie könne zum jetzigen Zeitpunkt noch keine finale Bewertung abgeben. Mit der Novellierung des Allgemeinen Gesetzes zum Schutz der öffentlichen Sicherheit und Ordnung – ASOG – seien Rechtsgrundlagen für die Nutzung einer Verhaltensmustererkennung im Objektschutz in das Gesetz integriert worden. Dies sei die Grundlage, auf der die Polizei arbeite. Es müsse jedoch noch geprüft werden, wie die Arbeit konkret ausgestaltet werde, wie die Bewegungen von Personen vergrößert oder unkenntlich gemacht würden oder wie lange die Rohdaten aufbewahrt würden. Grundsätzlich gebe es im ASOG jedoch Rechtsgrundlagen für dieses Projekt beziehungsweise die Durchführung von Verhaltensmustererkennungen. Die Datenschutzbeauftragte habe es ferner begrüßt, dass die Polizei die Behörde so frühzeitig involviert habe.

Vorsitzender Johannes Kraft stellt fest, dass keine weiteren Fragen oder Wortmeldungen vorlägen. Der Bericht aus der Senatskanzlei könne für die heutige Sitzung abgeschlossen werden.

Punkt 3 der Tagesordnung

Dringliche Vorlage – zur Beschlussfassung –
Drucksache 19/2999
**Gesetz zur Änderung des Berliner
Datenschutzgesetzes und weiterer
Rechtsvorschriften**

[0151](#)
DiDat(f)
Sport

Auf Antrag der Fraktionen der CDU und der SPD beschließt der **Ausschuss** mehrheitlich, den Tagesordnungspunkt zu vertagen. – Siehe auch „Vor Eintritt in die Tagesordnung“.

Punkt 4 der Tagesordnung

Besprechung gemäß § 21 Abs. 3 GO Abghs [0150](#)
IT-Sicherheit auch in Marzahn-Hellersdorf? Was ist DiDat
nach Veröffentlichung der Mängelliste des
Rechnungshofberichts passiert? Wie geht's weiter?
(auf Antrag der Fraktion Bündnis 90/Die Grünen)

Vorsitzender Johannes Kraft weist darauf hin, dass es die Möglichkeit gebe, die Öffentlichkeit zur Besprechung dieses Tagesordnungspunkts auszuschließen, sollte dies notwendig sein. – Da der Ausschuss keine Notwendigkeit sehe, könne wie gewohnt fortgefahren werden.

Stefan Ziller (GRÜNE) erinnert in der Begründung des Besprechungsbedarfs daran, dass der Rechnungshofbericht aus dem vergangenen Jahr am Beispiel des Bezirks Marzahn-Hellersdorf aufgelistet habe, welche Aspekte mit Blick auf die IT-Sicherheit zu verbessern seien. Viele Punkte seien bereits durch die IT-Sicherheitsberichte der letzten Jahre bekannt gewesen. Nun solle besprochen werden, was im Bezirk seit der Veröffentlichung des Berichts passiert sei und wie die Probleme behoben werden könnten. An den Senat richte sich zudem die Frage, wie es weitergehen solle – Teile der Probleme gebe es vermutlich auch in anderen Bezirken. IT-Stellen seien finanziell nicht ausreichend ausgestattet, es fehle vor allem eine Standardisierung. Der Rechnungshofbericht werde nicht ohne Grund erstellt und müsse ernst genommen werden.

Staatssekretärin Martina Klement (Skzl) bestätigt, dass Marzahn-Hellersdorf kein Einzelfall sei. In anderen Bezirken und Verwaltungen würde bei einer Prüfung vermutlich eine ähnliche Situation vorgefunden werden. Das Land Berlin müsse aus dem Bericht nun also die richtigen Schlussfolgerungen ableiten: Der Bericht werde sehr ernst genommen und man sei in einem engen Austausch, auch mit dem Bezirk, um die Erkenntnisse aufzuarbeiten. Mit der Rechnungshofpräsidentin müsse abgestimmt werden, welche Teile des Berichts öffentlich seien und welche nicht. Der Senat wolle seine Stellungnahme zum Bericht des Rechnungshofes in der morgigen Sitzung beschließen.

Bezirksstadtrat Stefan Bley (BA Marzahn-Hellersdorf; Abtl. Schule, Sport, Weiterbildung, Kultur und Facility-Management) hält fest, dass der Bezirk bereits im Jahr 2024 Gespräche mit dem Rechnungshof geführt habe. Aus dem Jahresbericht habe das Bezirksamt viele Schlussfolgerungen gezogen und im Jahr 2025 bereits die ersten Aspekte bearbeitet. Eine der wichtigsten Ableitungen aus dem Bericht sei der dringende Abstimmungsbedarf zwischen der IT-Sicherheitsbeauftragten und der Serviceeinheit Facility Management und hier speziell dem Fachbereich IT. In den vergangenen Jahren sei hier aufgrund von Personalvakanzan ein Bearbeitungsrückstand entstanden, der gemeinsam aufzuarbeiten und nachhaltig zu schließen sei. Dabei habe die IT-Sicherheit des Bezirksamts oberste Priorität.

Der Rechnungshof habe in seinem Bericht vom 17. März 2025 insgesamt 11 Feststellungen benannt, die unterschiedliche Bereiche der IT-Sicherheit im Bezirksamt betreffen. Aufgrund der teils sehr hohen Komplexität einzelner Mängel habe man noch nicht alle davon angehen können. Der Rechnungshof beanstande unter anderem die organisatorische Eingliederung der Informationssicherheitsbeauftragten, die innerhalb der Linienorganisation in der Serviceeinheit Facility Management verortet gewesen sei. Dieser Mangel sei bereits Anfang 2025

behaben worden, indem die IT-Sicherheitsbeauftragte nun unmittelbar der Behördenleitung und hier dem Bereich der Bezirksbürgermeisterin unterstellt worden sei. Im Rahmen der weiteren Feststellungen seien fehlende IT-Sicherheitsschulungen und Unterweisungen für die Dienstkräfte des Bezirksamts bemängelt worden. Dieser Sachverhalt sei bereits im Sommer 2024 aufgegriffen worden: In Zusammenarbeit mit dem externen Schulungsanbieter SoSafe sei ein umfangreiches Schulungskonzept zur Sensibilisierung der Dienstkräfte hinsichtlich des Schutzes vor unbefugten Zugriffen Dritter implementiert worden. Ein Teil des Schulungskonzepts sei auch eine Kampagne zum sicheren Umgang mit E-Mails sowie zur Erkennung von Phishing-Mails gewesen.

Weiterhin führe der Rechnungshof aus, dass die Sicherheit der Kommunikation per E-Mail sowie über das Internet nicht durchgängig gemäß den Vorgaben des Bundesamts für Sicherheit in der Informationstechnik ausgestattet sei. In diesem Zusammenhang habe der Fachbereich IT im Sommer 2025 gemeinsam mit dem zentralen IT-Dienstleister – ITDZ – eine zusätzliche Sicherheitseinrichtung in Form eines Proxy-Servers zwischen der behördlichen und landesweiten Kommunikation implementiert. In den kommenden Wochen und Monaten werde die Sicherheit der Kommunikationsinfrastruktur weiter ausgebaut und verschärft.

Der Rechnungshof beanstandete ebenfalls unzureichende Maßnahmen zum Zugriffsschutz. Durch den Aufbau einer neuen Nutzerverwaltung auf Basis von Microsoft Active Directory sei sowohl eine verschärfte Passwortrichtlinie eingeführt als auch organisatorisch sichergestellt worden, dass Administrationskonten ausschließlich für administrative Tätigkeiten genutzt würden. In einer weiteren Feststellung erwarte der Rechnungshof die unverzügliche Erstellung, Umsetzung und regelmäßige Fortschreibung eines vorgabenkonformen Datensicherungskonzepts sowie die Überprüfung einer erfolgreichen Wiederherstellung des IT-Gesamtsystems. Diese Anforderungen seien durch die Implementierung einer neu aufgebauten Backup-Lösung erfüllt und erfolgreich getestet worden. Im Rahmen der Wiederherstellungstests identifizierte Mängel seien unverzüglich behoben worden. Darüber hinaus werde die Backup-Lösung derzeit durch den Fachbereich IT weiter ausgebaut, um sowohl einen längeren Sicherheitszeitraum abzudecken als auch durch eine zusätzliche räumliche Trennung die Sicherheit der Sicherungsdaten weiter zu erhöhen.

Die angesprochenen, verschiedenen infrastrukturellen Mängel der IT habe der Fachbereich IT bereits in vielen Fällen beheben können. So sei eine Überarbeitung des Zutrittskonzepts für die Technikräume veranlasst worden und die Pfortnerdienste seien erneut hinsichtlich ihrer Aufgaben zur Gewährleistung der Sicherheit und Zugriffskontrolle sensibilisiert worden. Darüber hinaus habe die Serviceeinheit Facility Management den Fachbereich Bau sowie das Objektmanagement damit beauftragt, die physische Sicherheit der IT-Büroräume sicherzustellen. Ein entsprechendes Umsetzungskonzept liege bereits vor; es könne aus Kapazitätsgründen jedoch voraussichtlich erst im Jahr 2026 umgesetzt werden. Der Sicherheitsmangel, dem zufolge Verbindungen des Haupt-Wiring-Centers zugänglich gewesen seien, sei durch die Migration des Haupt-Wiring-Centers in den Hauptserverraum am Standort Rieser Straße vollständig behoben worden.

Mit der zum November 2025 bestellten IT-Sicherheitsbeauftragten würden die Fachbereiche IT, Bau sowie Objektmanagement in den kommenden Monaten die beanstandeten Dokumentationen, Konzepte, Anweisungen und Belehrungen gemeinsam überarbeiten, aktualisieren und fortschreiben. Zudem werde das Informationssicherheitsmanagementteam wieder die

erforderliche Beschlussfähigkeit erlangen. Die kontinuierliche Sensibilisierung der Dienstkräfte im Bereich der Informationssicherheit werde durch den weiteren Ausbau der SoSafe-Schulungen sichergestellt. Die Schulungsmaßnahmen würden regelmäßig aufgefrischt und durch den Erwerb von Zertifikaten, die zur Aufnahme in die Personalakten vorgesehen seien, mit entsprechenden Anreizmechanismen flankiert. Die Fachbereiche IT und Bau richteten derzeit einen neuen Serverraum ein: Durch den Einsatz moderner Sicherheits- und Überwachungstechnik sowie durch den Aufbau redundanter Systeme werde ein wesentlicher Beitrag zur Erhöhung der Ausfallsicherheit geleistet. Ergänzend hierzu trage die weitere räumliche Verteilung der gesamten Backuplösung auf mehrere Bürodienstgebäude zur Stärkung der Sicherheit und zur verbesserten Wiederherstellbarkeit des IT-Gesamtsystems bei.

Es sei zu betonen, dass insbesondere der Aufbau der VDI-Umgebungen im Bezirk Marzahn-Hellersdorf eines der zentralen Projekte sei, um die IT-Sicherheit wesentlich zu verbessern. Aus unterschiedlichen Gründen ziehe sich das Projekt leider schon über einige Jahre hin; hier spielten sowohl personelle als auch finanzielle Gründe eine Rolle. Man hoffe aber, noch in diesem Jahr zu einem positiven Abschluss kommen zu können.

Marc Vallendar (AfD) bemerkt, der Bericht zu Marzahn-Hellersdorf sei ein Offenbarungseid für die IT-Sicherheit in der Berliner Bezirksverwaltung: Es gebe kein IT-Sicherheitskonzept, keinen Notfallplan, Serverräume seien ohne Brandschutz, es gebe unzureichende Zugangskontrollen und offene Türen – und das in einer Zeit, in der Cyberangriffe auf Kommunalverwaltungen bundesweit zunähmen. Er frage den Senat, seit wann diese Lage im Bezirk Marzahn-Hellersdorf bekannt sei. Warum habe die IKT-Steuerung nicht früher eingegriffen? Zweitens wolle er wissen, ob es einen verbindlichen Zeitplan mit Meilensteinen gebe, der auch klare Konsequenzen für den Fall vorsehe, dass diese nicht eingehalten würden. Drittens frage er, wie es in den anderen elf Bezirken aussehe: Habe es auch hier Überprüfungen durch den Rechnungshof gegeben? Falls dies nicht der Fall sei, werde der Senat noch Prüfungen in den anderen Bezirken vornehmen? Oder hätten diese bereits stattgefunden und gezeigt, dass es sich bei Marzahn-Hellersdorf tatsächlich um einen Einzelfall handele?

Stefan Ziller (GRÜNE) weist darauf hin, dass der letzte IT-Sicherheitsbericht, der ihm vorliege, aus dem Jahr 2024 stamme. Gebe es schon einen Bericht aus dem Jahr 2025? Wie sei hier der Status? – Zur Zugänglichkeit der IT-Räume stelle sich die Frage, wie schlimm es sei, wenn diese Räume zugänglich seien. Habe der Senat eine Übersicht darüber, ob und wo es in der Berliner Verwaltung noch offene Räume gebe? Gebe es hier einen Maßnahmenplan? – Nach Informationen des Bezirks habe man sich um das Schulungskonzept und die Firma selbst gekümmert. Sei SoSafe ein Angebot für alle Berliner Verwaltungen und Bezirke, oder müsse jede Behörde eigene Ausschreibungen für Dienstleiter durchführen?

Es habe sich nicht erschlossen, welche Unsicherheiten es bezüglich der Mails gebe: Es sei angegeben worden, dass es ungeschützte Bereiche beim Mailversand gegeben habe. Gebe es dieses Problem auch in anderen Bezirken, oder handele es sich um ein spezielles Problem von Marzahn-Hellersdorf? – Habe die Senatskanzlei eine Übersicht über alle Mängel, die in den Bezirken und Senatsverwaltungen in IT-Sicherheitsfragen vorlägen? Werde es als eine Aufgabe der gesamtstädtischen Steuerung verstanden, gleiche Mängel in mehreren Verwaltungen auch gesamtstädtisch anzugehen, oder ziele die gesamtstädtische Steuerung nur darauf, die Verwaltungsteile mit dem nötigen Geld auszustatten, um die Probleme selbst zu beheben? – Zum Schutz des Landesnetzes scheine eine gemeinsame Vorgehensweise sinnvoller.

Carsten Schatz (LINKE) führt aus, der Bericht des Rechnungshofs habe auf drastische Art deutlich gemacht, welche Probleme es mit Blick auf die IT-Sicherheit in den Bezirken gebe: Es sei erschreckend, dass ein Anschlusskabel für das Berliner Landesnetz ungesichert in einem öffentlich zugänglichen Raum gelegen habe. Ein Abschließen der Räume und ein Schlüsselmanagement seien zwar prinzipiell recht unkomplizierte Maßnahmen, das Zusammenspiel zwischen Facility Management und IT werde aber immer wieder als ein großes Problem benannt, gerade auch bei Ausbaufragen. Es sei berichtet worden, dass die Sicherung der IT-Räume in Marzahn-Hellersdorf voraussichtlich im Jahr 2026 erfolgen könne, dies sei jedoch keine Sicherheit. Wie sehe die konkrete Planung aus?

In der Planung des Doppelhaushalts sei ein großer Schwerpunkt auf die Erneuerung der Hardware gelegt worden. Ein Vertreter des Bezirksamts Marzahn-Hellersdorf habe erläutert, dass das hierfür angesetzte Budget selbst ein IT-Sicherheitsproblem darstelle: Es stehe nach Kürzungen nur ein Viertel der Mittel des Vorjahreshaushaltsplans zur Verfügung. Werde die Hardware nicht erneuert, öffneten sich aber weitere Türen für Angriffe. Wie sehe nun der Plan aus? – Es sei zudem berichtet worden, dass Maßnahmen zur Aus- und Fortbildung schon im vergangenen Jahr durchgeführt worden seien. Im aktuellen Haushaltsplan sei für die Aus- und Fortbildung nun relativ wenig Geld angesetzt worden. Aus- und Fortbildungsmaßnahmen müssten jedoch kontinuierlich durchgeführt und dabei an neue Herausforderungen angepasst werden: Der Schulungsbedarf bleibe. Wie solle dieser mit viel weniger Geld gedeckt werden?

Staatssekretärin Martina Klement (Skzl) beantwortet zunächst die Frage des Abgeordneten Vallendar: Dem Senat sei die Situation in Marzahn-Hellersdorf in dieser Ausprägung seit dem Erhalt der Prüfergebnisse des Landesrechnungshofes bekannt. Es sei aber anzunehmen, dass es sich nicht um einen Einzelfall handle; auch in anderen Verwaltungsstellen seien ähnliche Zustände anzunehmen. Mit Blick auf die Frage, ob und wie der Senat nun die Situation in den einzelnen Bezirken erfasse, sei zu bedenken, dass es im IT-Sicherheitsbereich in den vergangenen Monaten einige neue Regularien gegeben habe – zum Beispiel durch die NIS-2-Richtlinie. Der Senat baue nun eine Prüfinfrastruktur auf. – Der Abgeordnete Ziller habe nach dem IT-Sicherheitsbericht für das Jahr 2025 gefragt: Dieser befinde sich im Moment in der Zeichnung und werde demnächst veröffentlicht werden.

Dr. Olaf Kroll-Peters (Skzl) ergänzt, dass in diesem Sicherheitsbericht noch nicht alle Sachverhalte beschrieben seien, die für eine neue, umfassende Informationssicherheitsstrategie benötigt würden: Er sei in einer Zeit entstanden, in der Angriffe noch nicht so regelmäßig erfolgt seien wie jetzt. Es müssten also zusätzliche Fragen gestellt werden. Auch im IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik – BSI – würden nun Antworten auf die Frage entwickelt, wie Informationssicherheit aktuell gemessen werden könne. Der IT-Sicherheitsbericht müsse in Zukunft entsprechend angepasst werden.

Als Methode zum Aufbau eines soliden Informationssicherheitsmanagements stelle das BSI den Standard 200–2 zur Verfügung. Einige der vom Rechnungshof festgestellten Mängel, die auch in diesem Standard thematisiert würden – wie die Benennung einer sicherheitsbeauftragten Person – seien schon angegangen worden. Es müsse jedoch stets das Gesamtbild betrachtet werden: Natürlich könne man nun einzelne Maßnahmen wie das Abschließen von Räumen umsetzen, es müsse jedoch stets die konkrete Bedrohungslage bewertet und dann entschieden werden, welche Maßnahme am besten und gezieltsten helfen könne. Ein Abschließen von Räumen könne bei Weitem nicht alle Angriffe verhindern.

Trotzdem habe der Rechnungshof natürlich zu Recht bestimmte Mängel benannt. Bei der Einstellung oder Benennung von IT-Sicherheitsbeauftragten bestehe auch die Herausforderung, geeignetes Personal zu finden, das sich auch mit den aktuellsten Entwicklungen – wie der genannten NIS-2-Richtlinie – auskenne. Fort- und Weiterbildungsangebote wie beispielsweise über SoSafe seien hier eine wichtige Komponente; das Problem sei jedoch, dass die Anbieter von Schulungsangeboten stets beteuerten, alle Bedarfe abdecken und schulen zu können, auch wenn dies am Ende nicht zwangsläufig der Wahrheit entspreche. Es sei – in Zusammenarbeit mit der VAK – ein Konzept ausgearbeitet worden, mit dem der Schulungsbedarf für das Land Berlin konkret erfasst worden sei. Es seien 15 verschiedene Zielgruppen und über 30 verschiedene Inhalte für Schulungen identifiziert worden. SoSafe könne hier höchstens 50 Prozent des Bedarfs abdecken. Es werde nun eine europaweite Ausschreibung vorbereitet; der Prozess werde noch ein wenig Zeit in Anspruch nehmen.

Zur Frage, ob es in allen Bezirken und Verwaltungsstellen die gleichen Probleme gebe, sei zu sagen, dass es sich in der Tat oft um ähnliche Probleme handele. Mit Blick auf das Thema Informationssicherheit sei eine der größten Herausforderungen, wie bereits beschrieben, das zur Ausübung von Tätigkeiten benötigte Wissen: Zwar sei es richtig, dass Geld und Personal fehlten, das Personal müsse jedoch auch die richtigen Qualifikationen und das notwendige Wissen mitbringen, was häufig nicht der Fall sei. Der Senat begegne dem Problem durch ein Workshopangebot, in dem einige der zentralen Themen adressiert werden sollten, so zum Beispiel die Inhalte der 34 Richtlinien, die laut BSI zur Umsetzung eines Informationsicherheitsmanagements berücksichtigt werden müssten. Das Wissen müsse in der Berliner Verwaltung langfristig aufgebaut werden – auch zu anderen wichtigen Aspekten wie zum Beispiel der sicheren Nutzung von KI-Systemen. Entscheidend sei hier ein strukturiertes und planvolles Vorgehen. Eine Struktur schaffe auch die Grundlage dafür, später verlässlicher einschätzen zu können, ob Informationssicherheitskonzepte zuverlässig umgesetzt worden seien und wo noch Lücken beständen.

Bezirksstadtrat Stefan Bley (BA Marzahn-Hellersdorf; Abtl. Schule, Sport, Weiterbildung, Kultur und Facility-Management) führt aus, dass die Schulungen im Bezirk Marzahn-Hellersdorf noch von der damaligen IT-Sicherheitsbeauftragten organisiert worden seien. – Der Abgeordnete Schatz habe das Thema Budgets angesprochen: In Marzahn-Hellersdorf sei der Komplex der Schulungen aus den Fachbereichen Facility Management und IT ausgelagert und dem Bereich der Bürgermeisterin zugeordnet worden. Die Mittel kämen nun also aus ihrem Budget; er könne derzeit keine genaue Auskunft über dessen aktuellen Stand geben.

Der Abgeordnete Ziller habe nach der IT-Sicherheit im Zusammenhang mit E-Mails gefragt: Der Hauptkritikpunkt sei hier gewesen, dass es im Bezirk Marzahn-Hellersdorf kein Schriftdokument zum Umgang mit E-Mails gegeben habe. In einem Amt müsse stets dokumentiert sein, welche Sicherheitsvorschriften es hierfür gebe. Es werde nun mit der neuen IT-Sicherheitsbeauftragten daran gearbeitet, ein solches Schriftdokument auszuarbeiten. Man habe aber lange gebraucht, um die Stelle zu besetzen: Sie sei länger als ein Dreivierteljahr nicht besetzt gewesen, obwohl es eine Ausschreibung gegeben habe. Es habe sich aber nicht die richtige Person gefunden. Die nun eingestellte Sicherheitsbeauftragte müsse in einigen Punkten noch eingearbeitet werden.

Zur Frage, warum der Anschluss zum Landesnetz öffentlich zugänglich gewesen und der Raum nicht abgeschlossen gewesen sei, sei zu sagen, dass es hier um das ehemalige Rathaus

am Helene-Weigel-Platz gegangen sei. An diesem Rathaus werde momentan eine Sanierung durchgeführt, die damals schon in der Planung gewesen sei. Hierin könnte eine Erklärung für das identifizierte Sicherheitsproblem liegen; der Vorfall sei natürlich trotzdem nicht zu entschuldigen. Mittlerweile sei das gesamte Netzwerk in ein anderes Bürodienstgebäude verlegt worden, das den Sicherheitsstandards entspreche und abgeschlossen werden könne.

Auch die Hardwareerneuerung sei als Sicherheitsrisiko angesprochen worden: Es sei richtig, dass es durch die Beschneidung des IT-Budgets nicht mehr die Umwälzung der IT-Hardware werde geben können, die ursprünglich geplant gewesen sei, womit sicherlich das eine oder andere Sicherheitsrisiko einhergehe. Die Hardware solle nun in einem Rhythmus von fünf Jahre gewechselt werden. Im Zuge der Umstellung auf eine VDI-Umgebung werde es aber noch einmal einen großen Austausch von Rechnern geben müssen.

Staatssekretärin Martina Klement (Skzl) hält abschließend fest, dass die Ausführungen der vergangenen halben Stunde der beste Werbeblock für eine schnellstmögliche Migration zum IT-Dienstleistungszentrum – ITDZ – gewesen seien.

Stefan Ziller (GRÜNE) fragt nach, ob der Senat eine Übersicht darüber habe, ob die Stellen für IT-Sicherheitsbeauftragte nun in allen Bezirken besetzt seien und in welchem Schulungsstadium sich die eingestellten Personen befänden. – Unabhängig davon wolle er fragen, ob es nicht vielleicht eine gute Idee sein könne, relevante Tätigkeitsprofile im Sinne eines Shared Service zentral anzubieten. Sei es vorstellbar, einen Pool an IT-Sicherheitsfachkräften bereitzustellen, die per Abordnung in die jeweiligen Behörden geschickt werden könnten? – Ein solches Vorgehen könne den Vorteil bieten, dass die Fachkräfte zentral und einheitlich geschult würden; zudem könnten sich die Fachkräfte gegenseitig vertreten und gegebenenfalls zwischen den Bezirken rotieren. So könne ein einheitliches Qualitätsniveau sichergestellt werden. – Habe er es zudem richtig verstanden, dass der IT-Sicherheitsbericht letztendlich gar keine zuverlässige Übersicht über die Probleme und die IT-Sicherheitslage im Land biete?

Vorsitzender Johannes Kraft schlägt vor, zumindest den letzten Teil der Frage schriftlich zu beantworten. Die Antwort solle zudem nur die Ausschussmitglieder erreichen.

Staatssekretärin Martina Klement (Skzl) gibt an, sie stimme dem Vorschlag zu. Eine Übersicht über die besetzten Stelle gebe es.

Vorsitzender Johannes Kraft stellt fest, dass keine weiteren Fragen oder Wortmeldungen vorlägen.

Der **Ausschuss** beschließt einvernehmlich, der Tagesordnungspunkt könne abgeschlossen werden.

Punkt 5 der Tagesordnung

Besprechung gemäß § 21 Abs. 3 GO Abghs
Vorstellung der Multi-Cloud-Strategie
(auf Antrag der Fraktion der CDU und der Fraktion der SPD)

[0152](#)
DiDat

Christopher Förster (CDU) hält in der Begründung des Besprechungsbedarfes fest, dass der Regierende Bürgermeister erst vor wenigen Tagen die Multi-Cloud-Strategie für das Land Berlin habe beschließen lassen. Sie sei auch erst vor wenigen Tagen veröffentlicht worden und solle nun im Rahmen der heutigen Ausschusssitzung vorgestellt und diskutiert werden.

Staatssekretärin Martina Klement (Skzl) bestätigt, dass die Multi-Cloud-Strategie erst vor Kurzem beschlossen worden sei – nachdem man im Dezember schon die Open-Source-Strategie beschlossen habe. Beide Strategien sollten das Land Berlin mit Blick auf die digitale Souveränität voranbringen. Der dritte Baustein sei die IKT-Architekturrichtlinie 2.0, die im vergangenen Jahr festgesetzt worden sei.

Florian Ebel (Skzl) präsentiert im Anschluss die Grundzüge der Multi-Cloud-Strategie für das Land Berlin: Im Kern bedeute die Arbeit mit einer Cloud, dass Dinge nicht mehr in einem eigenen Rechenzentrum lokal, sondern über Netze bereitgestellt würden. Daran knüpften sich viele Umsetzungsfragen, aber auch Potenziale, die das Land Berlin für sich nutzen wolle.

Es sei voranzustellen, dass die Multi-Cloud-Strategie nicht für das Land Berlin allein, sondern im föderalen Kontext entwickelt worden sei. Seit 2019 arbeite man auch im Bund bereits an Cloudlösungen: Der IT-Planungsrat habe unter anderem eine Strategie zur Stärkung der digitalen Souveränität sowie die Deutsche Verwaltungscld entwickelt, und auch die Ministerpräsidentenkonferenz – MPK – habe sich mit der Frage einer Cloudstellung beschäftigt. Ende 2023 sei dargestellt worden, dass ein Cloud-First-Ansatz verfolgt werden und mit cloud-fähigen und föderal nutzbaren IT-Dienstleistungen die Deutsche Verwaltungscld gestartet werden solle. Auch die Digitalministerkonferenz habe den MPK-Beschluss bekräftigt und die Umsetzung der Deutschen Verwaltungscldstrategie eingefordert. Das ITZBund habe man als einen wesentlichen Player mit govdigital verknüpfen wollen, damit auch von dieser Seite Services in der Deutschen Verwaltungscld bereitgestellt werden könnten. Im Mai 2025 habe die Digitalministerkonferenz die Ankündigung der Europäischen Kommission unterstützt, dass ein europäischer Rechtsrahmen für Cloudlösungen geschaffen werden solle. – Es sei festzuhalten, dass genau in dieser gemeinsamen Arbeit auf allen Ebenen die Chancen einer Cloudstrategie lägen.

Im Kontext der Strategie seien sechs große Herausforderungen identifiziert worden, denen mit einer Cloudlösung begegnet werden könne. Zunächst gebe es in Berlin eine relativ heterogene IKT-Landschaft, die sich auch in unterschiedlichen Rahmenbedingungen und Zuständigkeiten niederschlage. Es gebe Investitionsbedarfe und Altverfahren, die im Betrieb einer gewissen Kostenspirale unterlägen. Bei ihrer Nutzung bestehe zudem die Gefahr, dass eine Abhängigkeit von nur einem Anbieter entstehe, die strukturell zu vermeiden sei. Mit einer dezentralen IKT-Landschaft gehe auch eine begrenzte Transformationsfähigkeit einher: Es könnten hier nicht so leicht Skaleneffekte entstehen wie in einer gemeinsamen, standardisierten Struktur. Dementsprechend gebe es auch mehr Einführungsaufwand bei neuen Services.

Eine weitere Herausforderung sei das Thema des Fachkräftemangels: Ein Drittel der Beschäftigten in der Berliner Verwaltung werde bis zum Jahr 2031 aus dem Dienst scheiden. Auch dies werde Auswirkungen auf den Betrieb von IT-Services haben; mit einem Engagement für mehr Zentralisierung könne ein Stück weit Druck abgebaut werden. Auch die Themen IT-Sicherheit und Datenschutz spielten eine große Rolle: Es gebe ein Spannungsfeld, in dem IT-Unternehmen auf der einen Seite dem CLOUD Act unterlägen und auf der anderen Seite den Anforderungen der Datenschutzgrundverordnung genügen müssten. Zuletzt sei das Thema des Energieverbrauchs zu bedenken: Rechenzentren brauchten viel Energie, die wenigstens möglichst effizient genutzt werden solle.

Aufbauend auf diesen Feststellungen sei dann eine Vision entwickelt worden: Man habe eine Multi-Cloud-Umgebung für das Land Berlin aufbauen wollen, die hochsicher, interoperabel und flexibel gestaltet sein solle. Es werde das Ziel verfolgt, die digitale Souveränität Berlins zu stärken und die Voraussetzung für moderne und zukunftssichere Verwaltungsarbeit zu schaffen. Die Strategie halte acht Leitziele fest: Services sollten optimiert und zentral bereitgestellt werden, es solle ein Cloud-Service-Broker etabliert werden, ein Cloud-First-Ansatz für neue Lösungen solle verfolgt werden, die Ressourceneffizienz solle gesteigert werden, die Flexibilität und Skalierbarkeit der IT-Infrastruktur sollten erhöht werden, es sollten sowohl eine bessere Zusammenarbeit in der Verwaltung als auch eine bessere Verfügbarkeit diverser Services ermöglicht werden, und eine bessere Interoperabilität solle entstehen – etwa durch das erhöhte Nutzen von Open-Source-Lösungen, offener Schnittstellen und Standards. Es gebe im Rahmen der Multi-Cloud-Strategie zudem eine klare Policy zu Sicherheit und Datenschutz. Als Quintessenz ergebe sich mehr Innovationsfähigkeit durch das Reduzieren von Abhängigkeiten und eine leichtere Zugänglichkeit neuer Lösungen. Auch Nachhaltigkeit und Klimaschutz würden unterstützt: Mit einer Zentralisierung der – erhöhten – Rechenleistung könne effizienter gearbeitet werden, als dies in diversen Strukturen möglich sei.

Mit der Multi-Cloud-Strategie sei das Zusammenarbeitsmodell der Deutschen VerwaltungscLOUD umgesetzt worden. Dieses Modell versuchten Bund, Länder und Kommunen gemeinsam zu realisieren. Das ausgewählte Modell entspreche den Grundgedanken des E-Government-Gesetzes; der eigene IT-Dienstleister sei von Beginn an als Partner involviert gewesen und habe am Prozess der Vorbereitung der Umsetzung der Multi-Cloud-Strategie teilgenommen. So habe man den Herausforderungen gemeinsam begegnen können. Das Grundprinzip der Deutschen VerwaltungscLOUD sei es, dass verschiedene Cloud-Service-Anbieter in einem Serviceportal bei sich gehostete Software – die entweder selbst erarbeitet worden oder von Lieferanten bezogen sei – entweder als Infrastructure-as-a-Service, Platform-as-a-Service oder Software-as-a-Service anböten. Es sei also eine Art Portal-Ökosystem entstanden. Darüber hinaus gebe es den Cloud-Service-Beschaffer, den sogenannten Cloud-Service-Broker: Diese Rolle werde vom ITDZ Berlin übernommen. Dies habe den Vorteil, dass das ITDZ bereits Rechenzentren und das Berliner Landesnetz verwalte; diese Strukturen müssten nur noch ertüchtigt werden. Man erhoffe sich Skaleneffekte und wolle gleichzeitig auf unterschiedliche Bedürfnisse eingehen können.

Neben der Community-Cloud-Umgebung der Deutschen VerwaltungscLOUD gebe es noch drei weitere Cloud-Umgebungen: Je sensibler Daten seien, desto mehr eigene Souveränität werde für diese Daten benötigt. Es gebe deshalb eine Private Cloud, die in einem Rechenzentrum des ITDZ Berlin betrieben werde, was ein Höchstmaß an digitaler Souveränität gewährleiste.

Zudem gebe es eine Sovereign Public Cloud, die als Cloud für Open-Source-Lösungen aus dem EU-Rechtsraum diene, und die Public Cloud für proprietäre Cloud-Services von Anbietern im EU-Rechtsraum. Es gebe klare Bedingungen dafür, wann welche Umgebung genutzt werden dürfe: Je sensibler Daten seien, desto näher sollten sie an der Berliner Verwaltung verbleiben. Mit der Multi-Cloud-Umgebung sei ein mehrdimensionales Vorgehen gewählt worden; eine besondere Position komme durch die Möglichkeit der föderalen Anschlussfähigkeit jedoch der Community Cloud zu: Durch sie könnten Services, die in der Deutschen Verwaltungcloud bereitlägen, schnell auch für das Land Berlin nutzbar gemacht werden. Neben der konsumierenden Ebene könnten auch die Services des ITDZ nicht nur der Berliner Verwaltung, sondern auch anderen Verwaltungen angeboten werden. – Das Modell mit den vier Cloud-Ebenen sei als operative Ausformung der Multi-Cloud-Strategie bereits in der IKT-Architektur umgesetzt.

Mit der Veröffentlichung der Multi-Cloud-Strategie sei der erste Meilenstein erreicht worden. Nun solle das Betriebsmodell für den Cloud-Service-Broker folgen, da dieser das Scharnier für die Cloud-Umsetzung in der Berliner Verwaltung darstelle: In diesem Kontext müssten sowohl organisatorische als auch technische Komponenten umgesetzt werden. Es habe hierzu bereits das genannte gemeinsame Projekt mit dem ITDZ gegeben. In der Umsetzungsphase solle dann auch damit begonnen werden, die Wirkung zu messen: Erste Proofs of Concept sollten beim Cloud-Bezug durchgeführt werden, da es sich um neue Prozesse handle, die verprobt werden müssten. Der letzte Meilenstein sei dann die Aufnahme des Betriebs des Cloud-Service-Brokers durch das ITDZ Berlin. – Nach dem Aufbau der Strukturen könnten die Migrationsvorbereitung der Bestandsverfahren und schließlich die Migration dieser Verfahren in die Cloud folgen. Zukünftig sollten Neuentwicklungen nur noch über die Cloud erfolgen, um von allen Vorteilen dieser Lösung profitieren zu können.

Johannes Kraft (CDU) weist darauf hin, dass auf der letzten gezeigten Folien zwei Meilensteine die gleiche Bezeichnung gehabt hätten: Beide trügen den Titel „Konzeption Betriebsmodell“. Sei dies so gewollt? Was sei der Unterschied zwischen den Meilensteinen 2 und 3?

Florian Ebel (Skzl) räumt ein, dass die Benennung im Nachgang eventuell noch spezifiziert werden müsse: Es handle sich im Meilenstein 2 um die Konzeption des Betriebsmodells aus personalplanerischer und organisatorischer Sicht und im Meilenstein 3 um die Konzeption mit Blick auf die erforderliche Technologie und auf Prozesse. Die Aufgliederung sei also bewusst erfolgt.

Jan Lehmann (SPD) fragt, ob anhand eines Beispiels spezifischer dargestellt werden könne, wie in Zukunft mit bestimmten Verwaltungsvorgängen oder Anträgen umgegangen werden solle. Wo fänden sich die Vorgänge konkret in der Cloudstruktur wieder?

Stefan Ziller (GRÜNE) greift die Information auf, dass die Migrationsvorbereitung für die Fachverfahren ab Jahr 5 vorgesehen sei; man könne also voraussichtlich in drei Jahren mit dieser Vorbereitung beginnen. Warum könne hiermit nicht früher begonnen werden? Warum gebe es keine Vorgabe, die besage, dass jede Weiterentwicklung grundsätzlich cloudfähig erfolgen müsse? – Zweitens seien die vier Ebenen der Multi-Cloud-Strategie beschrieben worden. Wozu werde die Public Cloud gebraucht, wenn es drei Stufen gebe, die mit Blick auf die Notwendigkeit digitaler Souveränität angemessener erschienen? Was spreche dagegen, dass das Land nur die anderen drei Ebenen nutze – auch aus Anreizgründen?

Weiterhin interessiere ihn, wer über das Sicherheitslevel von Fachverfahren entscheide: Sei diese Einschätzung eine Aufgabe der jeweiligen Fachverwaltung? Sei die E-Akte grundsätzlich cloudfähig, und in welche Sicherheitskategorie werde sie eingeordnet? Wo arbeiteten Bund und Länder konkret zusammen, und wie werde eine gute Zusammenarbeit sichergestellt, sodass das Entstehen von Einzellösungen in verschiedenen Bundesländern vermieden werde? – Zuletzt interessiere ihn, inwieweit die Cloud-Strategie im Senat mit einer Strategie für Rechenzentren zusammenhänge. Es müsse die notwendige Infrastruktur bereitgestellt werden: Gebe es hierfür eine gezielte Rechenzentrenstrategie, die auch wirtschaftlich eine Rolle für das Land Berlin spielen könne?

Florian Ebel (Skzl) gibt an, er wolle mit dem nachgefragten Beispiel beginnen: Es müsse zunächst festgehalten werden, dass die Multi-Cloud-Strategie weniger auf die Antragsebene als auf die Ebene der Verwaltungsservices ziele. Wenn beispielsweise ein Software-Lieferant mit einer Software für einen Terminfinder an Dataport herantrete und Dataport beschließe, das Produkt zu kaufen, müsse die Software zunächst in den eigenen Dataport-Strukturen für die Deutsche Verwaltungscld vorbereitet werden. Dann könne die Software über das Portal allen Behörden zu einem bestimmten Preis bereitgestellt werden; bislang sei nur ein Bezug über das Internet möglich. Cloud-Service-Beschaffer könnten das Produkt dort finden und einkaufen. Die Cloud-Service-Broker dienten in gewisser Weise auch als ein Navigator durch das System und könnten Behörden dabei unterstützen, geeignete Lösungen zu finden. Eine Cloud-Lösung biete auch die Möglichkeit zu mehr Automatisierung: Von einer Anfrage im Serviceportal bis zur Bereitstellung des gewünschten Services könnten in Zukunft nur 48 Stunden vergehen.

Zum Thema der Migrationsvorbereitung sei zu sagen, dass Neubeschaffungen selbstverständlich schon jetzt auf ihre Cloudreife geprüft werden sollten. Die Realität zeige aber, dass es insbesondere im Bereich der Fachverfahren teilweise sehr spezialisierte Lösungen gebe; man müsse hier handlungsfähig bleiben und sei an der einen oder anderen Stelle noch auf die Public Cloud angewiesen. Die Ausarbeitung der verschiedenen Ebenen sei jedoch als klare Zielsetzung für die Zukunft zu verstehen: Es werde langfristig mehr digitale Souveränität angestrebt. – Im Kontext der Rechenzentren sei auf die Nationale Rechenzentrumsstrategie des Bundes zu verweisen. Die Verantwortung für das Land Berlin liege in der Senatsverwaltung für Wirtschaft, Energie und Betriebe; diese kümmere sich um wirtschafts- und standortpolitische Fragestellungen. In einem wirtschaftspolitischen Ansatz könnten Sovereign Public Clouds gefördert werden. – Über das Sicherheitslevel von Fachverfahren entscheide tatsächlich die jeweils zuständige Behörde. Die Senatskanzlei mache hierfür aber klare Vorgaben.

Johannes Kraft (CDU) fragt nach, welche Ebenen der Cloud-Strategie in einem fiktiven Szenario noch funktionieren würden, wenn sämtliche Verbindungen des Berliner Behördennetzes zum Internet getrennt würden.

Stefan Ziller (GRÜNE) erinnert daran, dass seine Frage nach der E-Akte noch unbeantwortet sei: Müsse hier noch eine Migration organisiert werden?

Florian Ebel (Skzl) führt aus, dass bei einem Internetausfall wahrscheinlich insbesondere die Sovereign Public Cloud und die Public Cloud betroffen wären. Bei der Community Cloud und der Private Cloud müsse geschaut werden, ob auch das jeweilige Netz vom Ausfall betroffen sei: Die Private Cloud laufe direkt über das Landesnetz, die Community Cloud momentan

noch über das Internet – welches dann eventuell ausgefallen sei –, es solle in Zukunft aber mit den Netzen des Bundes gearbeitet werden. Aus diesen Gegebenheiten erschließe sich auch der Ansatz, die Private Cloud und die Community Cloud bevorzugt zu nutzen. – Zur Cloudfähigkeit der E-Akte könne er angeben, dass die Infrastruktur grundsätzlich geeignet sei, die E-Akte cloudfähig zu machen. Sie sei aber momentan in keiner Cloud abgelegt, da sehr sensible Daten in der E-Akte verwaltet würden.

Johannes Kraft (CDU) hakt nach, ob er es richtig verstanden habe, dass nicht abgeschätzt werden könne, ob bei einem Internetausfall die im Wesentlichen über das ITDZ gehostete Private Cloud noch funktionsfähig wäre oder nicht.

Florian Ebel (Skzl) erklärt, dass bei einem Internetausfall der Schutz greife, den das Berliner Landesnetz im Rahmen seiner Sicherheitsmaßnahmen biete: Sollte das Landesnetz weiterlaufen, sei die Public Cloud weiter funktionsfähig.

Vorsitzender Johannes Kraft stellt fest, dass keine weiteren Fragen oder Wortmeldungen vorlägen.

Der **Ausschuss** beschließt einvernehmlich, der Tagesordnungspunkt könne abgeschlossen werden.

Punkt 6 der Tagesordnung

Verschiedenes

Siehe Beschlussprotokoll.