

19. Wahlperiode

Schriftliche Anfrage

des Abgeordneten Jan Lehmann (SPD)

vom 26. Januar 2026 (Eingang beim Abgeordnetenhaus am 2. Februar 2026)

zum Thema:

IT-Infrastruktur der Berliner Justiz

und **Antwort** vom 17. Februar 2026 (Eingang beim Abgeordnetenhaus am 19. Februar 2026)

Senatsverwaltung für Justiz
und Verbraucherschutz

Herrn Abgeordneten Jan Lehmann (SPD)
über
die Präsidentin des Abgeordnetenhauses von Berlin

über Senatskanzlei - G Sen -

A n t w o r t
auf die Schriftliche Anfrage Nr. 19/25065
vom 26. Januar 2026
über IT-Infrastruktur der Berliner Justiz

Im Namen des Senats von Berlin beantworte ich Ihre Schriftliche Anfrage wie folgt:

1. Welche Stellen sind in Berlin jeweils für die ordentliche Gerichtsbarkeit und die Staatsanwaltschaften zuständig für
- a) Betrieb/Hosting (Rechenzentrum, Netzwerk etc.),
 - b) Fachverfahren (insbesondere E-Akte, Verfahrens- und Dokumentenmanagement),
 - c) Endgeräte/Client-Management,
 - d) E-Mail/Groupware,
 - e) IT-Sicherheit,
 - f) Notfallmanagement?

Zu 1.: In der ordentlichen Gerichtsbarkeit und bei den Staatsanwaltschaften bestehen ausdifferenzierte Zuständigkeiten für die komplexe IT-Landschaft in Abhängigkeit von der jeweiligen Rolle und vom spezifischen IT-Dienst.

Zu 1a): Die Zuständigkeiten für die IT-Infrastruktur und deren Bereitstellung inklusive der technischen Administration und des technischen Managements richten sich danach, ob der konkret genutzte IT-Dienst in justizeigenen oder in Rechenzentren des IT-Dienstleistungszentrums Berlin (ITDZ) bzw. weiterer Anbieter bereitgestellt wird.

Entsprechend bestehen geteilte Zuständigkeiten der jeweiligen IT-Organisationseinheiten des ITDZ, des Kammergerichts, der Generalstaatsanwaltschaft, des Obergerichts Berlin-Brandenburg, des Verwaltungsgerichts und des Sozialgerichts wie in der Antwort zu Frage 2 dienstabhängig dargestellt.

Zu 1b): Die Zuständigkeiten für die IT-Fachverfahren und deren Bereitstellung inklusive der technischen Administration und des technischen Managements richten sich danach, ob der konkret genutzte IT-Dienst in justizeigenen oder in Rechenzentren des ITDZ bereitgestellt wird. Entsprechend bestehen geteilte Zuständigkeiten der jeweiligen IT-Organisationseinheiten wie in der Antwort zu Frage 1a) dargestellt.

Für IT-Systeme zur elektronischen Gerichts- und Verfahrensaktenführung heißt das konkret: In der ordentlichen Gerichtsbarkeit werden die IT-Systeme vollständig – sowohl server- als auch clientseitig – vom ITDZ bereitgestellt. Für die Staatsanwaltschaften werden die zentralen IT-Systemkomponenten (insbesondere Server) ebenfalls vom ITDZ, die dezentralen IT-Systemkomponenten von der IT-Abteilung 10 der Generalstaatsanwaltschaft bereitgestellt.

Zu 1c): Auf die Antwort zu Frage 1b) wird hinsichtlich der Zuständigkeiten für die Clients Bezug genommen. Für das Management der Endgeräte (Hardware) in den jeweiligen Gerichts- und Behördenstandorten sind die Dezernate X im Kammergericht und die IT-Abteilung 10 in der Generalstaatsanwaltschaft zuständig, wobei der Bezug der Endgeräte nach Möglichkeit aus Rahmenverträgen des ITDZ erfolgt.

Zu 1d): Die Bereitstellung einschließlich der technischen Administration der Bürosoftware zur Kommunikation und Zusammenarbeit (insb. E-Mailing) erfolgt in der ordentlichen Gerichtsbarkeit durch das ITDZ und in den Staatsanwaltschaften durch die IT-Abteilung 10 in der Generalstaatsanwaltschaft.

Zu 1e) und f): Zentrale IT-Komponenten zum Schutz des von der ordentlichen Gerichtsbarkeit und den Staatsanwaltschaften genutzten autonomen Netzes (sog. Berliner Landesnetz, BeLa) werden vom ITDZ bereitgestellt, administriert und gemanagt. Die Zuständigkeiten für dienstespezifische Sicherheitskomponenten folgen den Zuständigkeiten für den jeweiligen IT-Dienst. Im Übrigen haben alle Gerichte und Behörden in der ordentlichen Gerichtsbarkeit und bei den Staatsanwaltschaften behördliche Informationssicherheitsbeauftragte und Business-Continuity-Beauftragte mit Zuständigkeiten gemäß den Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) etabliert.

2. Welche Leistungen werden derzeit durch das ITDZ Berlin erbracht (bitte nach Leistungsbereichen und Systemen auflisten), welche durch sonstige Dienstleister und welche durch justizinterne Einheiten?

Zu 2.: Folgende IT-Leistungen werden justizeigen durch das ITDZ oder durch weitere Anbieter erbracht:

- Bereitstellung der landeszentralen IT-Infrastruktur, z. B. des BeLa inklusive Standardnetzzugang und virtueller Poststelle (VPS): ITDZ
- Bereitstellung der lokalen IT-Infrastruktur, z. B. aktiver Netzwerkkomponenten in den Gerichts- und Behördengebäuden: Justiz

- Bereitstellung landeszentraler IT-Applikationen wie IPV und ProFiskal: ITDZ
- Bereitstellung justizspezifischer IT-Applikationen gemäß IT-Bestands- und Planungsübersicht (IT-BePla):
 - GStA-PersonalDB: Justiz (Generalstaatsanwaltschaft)
 - GStA-Stellenkartei: Justiz (Generalstaatsanwaltschaft)
 - Personaldatenbank StA: Justiz (Staatsanwaltschaft)
 - GStA-Drittschuldner: Justiz (Generalstaatsanwaltschaft)
 - MESTA: ITDZ (dedizierte zentrale IT-Systemkomponenten) und im Übrigen Justiz (Generalstaatsanwaltschaft)
 - eVerwaltungsakte: Justiz (Generalstaatsanwaltschaft)
 - eIP: serverseitig ITDZ und clientseitig Justiz (Generalstaatsanwaltschaft)
- AuLAK: ITDZ
- AUMAV: ITDZ (über das EDV-Landeszentrum für Datenverarbeitung (LZfD))
- Digitales Aktenarchiv: Justiz (Kammergericht)
- AUREG: ITDZ
- AJUKA: ITDZ
- EUMAV: Bundesrechenzentrum
- eIP: ITDZ
- forumSTAR: ITDZ
- eKP: ITDZ
- SolumSTAR: ITDZ
- GOŠA: Justiz (Oberverwaltungsgericht)
- EDEV: Justiz (Oberverwaltungsgericht)
- EUREKA-Fach: Justiz (Sozialgericht)
- EVA: Justiz (Sozialgericht)
- IT-Dienstleistungen aus landesweiten Rahmenverträgen: ITDZ
- IT-Dienstleistungen im Übrigen: Justiz
- Hardware aus landesweiten Rahmenverträgen: ITDZ
- Hardware im Übrigen: Justiz
- Software aus landesweiten Rahmenverträgen: ITDZ
- Software im Übrigen: Justiz

3. Welche wesentlichen vertraglichen Grundlagen bestehen zwischen der Berliner Justiz und dem ITDZ (insbesondere Leistungsbeschreibung und Auditrechte)?

Zu 3.: Die Berliner Justiz schließt mit dem ITDZ in der Regel Vereinbarungen auf Grundlage des Gesetzes über die Anstalt des öffentlichen Rechts IT-Dienstleistungszentrum Berlin (ITDZAöRG BE).

Als zentraler IT-Dienstleister des Landes Berlin schließt das ITDZ regelmäßig von dort standardisierte Verträge unter Anwendung der Gemeinsamen Geschäftsbedingungen (GGB) mit dienstespezifischen Leistungsbeschreibungen, Preisblättern und Regelungen der Servicelevel insbesondere bei sog. EVB-IT-Dienstverträgen ab. Soweit das ITDZ für die Justiz personenbezogene Daten verarbeitet, wird der Vertrag um eine Auftragsverarbeitungsvereinbarung (AVV) ergänzt.

Auditrechte der Justiz ergeben sich regelmäßig aus § 2 Abs. 3 Satz 2 des ITDZAöRG BE, aus der jeweiligen Leistungsbeschreibung, der entsprechenden AVV sowie mittelbar aus der BSI-Zertifizierung des ITDZ gemäß ISO 27001.

4. In welchen Fällen kann das ITDZ eigenständig und ohne vorherige Zustimmung der Justiz Änderungen vornehmen, die Verfügbarkeit oder Zugriffsmöglichkeiten auf justizbezogene Daten beeinflussen?

Zu 4.: Zugriffsberechtigte Administratoren des ITDZ *dürfen* technische Änderungen an IT-Systemen ohne vorherige Zustimmung der Justiz grundsätzlich nicht, *können* diese aber durchführen, auch wenn sie die Systemverfügbarkeit betreffen.

5. Trifft es zu, dass ein gesondert geschütztes Rechenzentrums-/Betriebsmodell speziell für Gerichtsakten vereinbart wurde bzw. im Aufbau ist? Es wird gebeten um eine Darstellung des Zeitplanes, Projektstatus und Umfang (Gerichte/Behörden, Datenkategorien, Systeme).

Zu 5.: Das ITDZ errichtet in einem gemeinsamen Projekt mit der Präsidentin des Kammergerichts das Rechenzentrum Justiz, in dem justizspezifische IT-Dienste u. a. für die elektronische Gerichtsakte dediziert für die Justiz bereitgestellt werden.

Vordergründig handelt es sich um IT-Dienste der ordentlichen Gerichtsbarkeit. Hinzu kommen indes IT-Dienste, welche die Präsidentin des Kammergerichts vereinbarungsgemäß auch für die Fachgerichte und für die Staatsanwaltschaften betreiben lässt. Gemäß IT-BePla handelt es sich um die folgenden IT-Dienste:

- AUREG
- AJUKA
- eIP
- forumSTAR
- eKP
- SolumSTAR

Auch der zentrale Justiz-Desktop (BerlinPC Justiz) wird im Rechenzentrum Justiz bereitgestellt.

Der aktuelle Projektstatus ist der folgende: Die Basisinfrastruktur des Rechenzentrums Justiz ist errichtet. Zwei Fachverfahren, ca. 140 BerlinPC-Justiz-Arbeitsplätze und eine erste nicht produktive forumSTAR-Ökosystem-Umgebung sind bereits migriert und in Betrieb.

Der weitere Zeitplan sieht vor:

- bis 02/2026: forumSTAR-Ökosystem-Projektumgebung migriert und in Betrieb
- bis 03/2026: forumSTAR-Ökosystem-Betreuungs- und Schulungsumgebung migriert und in Betrieb
- bis 06/2026: Inbetriebnahme und Endausbau Infrastruktur und Migration aller verbleibenden BerlinPC-Justiz-Arbeitsplätze
- bis 06/2026: Migration und Inbetriebnahme der beiden produktiven forumSTAR-Ökosystem-Umgebungen
- bis 12/2026: Abschlussarbeiten und Migration verbleibender Justizfachverfahren, Projektabschluss

6. Was bedeutet die „isolierte Betriebsumgebung für Gerichtsakten“ konkret und inwieweit werden die digitalen Gerichtsakten isoliert? Betrifft dies ausnahmslos alle Gerichtsakten?

Zu 6.: Im Rechenzentrum Justiz werden justizspezifische IT-Dienste wie die elektronische Gerichtsakte dediziert betrieben. Das bedeutet, dass diese Dienste technisch (justizspezifische IT-Systeme auf justizspezifischer IT-Infrastruktur), betrieblich (justizspezifische IT-Prozesse z. B. beim Releasemanagement) und organisatorisch (z. B. dedizierte named admins) von anderen Kunden des ITDZ separiert den Anforderungen der Justiz gemäß betrieben werden.

Dieser separierte Betrieb betrifft im Rahmen des aktuellen Projekts alle elektronischen Gerichtsakten der ordentlichen Gerichtsbarkeit (vgl. Antwort zu Frage 5).

7. Welche klaren Zugriffs- und Protokollregelungen sind bei dem Zugriff auf Gerichtsakten vorgesehen?

Zu 7.: Die technischen Administratoren des ITDZ erhalten *keinen* Systemzugriff über die jeweilige produktive Justiz-Applikation, sondern ausschließlich auf die von diesen Systemen genutzten IT-Infrastrukturen. Das bedeutet, ein technischer Administrator kann nicht wie ein Anwender beispielsweise das elektronische Gerichtsaktensystem nutzen.

Die technischen Administratoren dürfen auf die IT-Infrastruktur *ausschließlich* in zwingenden Fällen zugreifen. Berechtigungen für die IT-Infrastruktur dürfen *nicht* weitergegeben werden.

Im Rechenzentrum Justiz werden *alle* administrativen Zugriffe auf die IT-Infrastruktur durch die eindeutig identifizierbaren Administratoren geloggt und entsprechende Aktivitäten mittels Bildschirmaufnahme für eine mögliche spätere Prüfung aufgezeichnet.

8. Welche Personengruppen haben technisch die Möglichkeit, auf Inhalte von E-Akten bzw. auf richterliche Arbeitsdokumente oder Entwürfe zuzugreifen? (Es wird gebeten um eine Differenzierung zwischen den verschiedenen Systemen/Fachverfahren.)

Zu 8.: Die *technischen Administratoren des ITDZ* erhalten keinen Systemzugriff über die jeweilige produktive Justiz-Applikation wie Fachverfahren, Textsysteme und Systeme zur elektronischen Aktenführung. Sie können ausschließlich auf die von diesen Systemen genutzten IT-Infrastrukturen zugreifen. Das bedeutet, ein technischer Administrator kann nicht wie ein Anwender die genannten IT-Systeme nutzen. Auf Infrastrukturebene ist ein Zugriff beispielsweise auf Datenbankeinträge und Dateien im Filesystem theoretisch möglich. Bezüglich Zulässigkeit und Nachvollziehbarkeit wird insofern auf die Antwort zu Frage 7 Bezug genommen.

Anwendende erhalten gemäß Rechte- und Rollenkonzept Zugriff im Rahmen der applikationsbezogenen Berechtigungen, die fachadministrativ vergeben werden. Auch insoweit wird bezüglich Zulässigkeit und Nachvollziehbarkeit auf die Antwort zu Frage 7 Bezug genommen.

9. Welche Zugriffsrechte bestehen für Gerichtspräsident:innen oder Verwaltungsleitungen auf laufende Verfahren bzw. richterliche Arbeitsdokumente und Entwürfe?

Zu 9.: Zugriffsrechte – auch für Gerichtspräsidentinnen und -präsidenten sowie Verwaltungsleitungen – werden applikationsbezogen (vgl. Antwort zu Frage 8) und generell ausschließlich zur Wahrnehmung übertragener dienstlicher Aufgaben vergeben.

Konkret bedeutet dies am Beispiel des eingesetzten eLP, dass Gerichtspräsidentinnen und -präsidenten wie alle anderen Nutzenden im Rahmen ihrer richterlichen Tätigkeit nur aufgrund genereller Vertretungsregelungen und Berechtigungen aus dem Fachverfahren (z. B. Teil desselben Spruchkörpers) Zugriff auf elektronische Gerichtsakten haben oder von originär Berechtigten mittels Einzelzuweisung (z. B. für dienstliche Beurteilungen) ausdrücklich berechtigt werden. Die Stellvertretungsrechte werden dann transparent angezeigt und vergebene Einzelberechtigungen können jederzeit wieder entzogen werden.

Zugriffe auf persönliche Entwürfe und sonstige Dokumente, die noch nicht förmlicher Aktenbestandteil sind, sind solange überhaupt nicht von Dritten – auch nicht von Vertreterinnen und Vertretern – einsehbar, wie sie die Autorinnen und Autoren nicht freigegeben haben.

10. Unter welchen Voraussetzungen ist ein Zugriff anderer Richter:innen (z. B. Vertretungsfälle) möglich?

Zu 10.: Auf die Antwort zu Frage 9 wird Bezug genommen.

11. Welche Maßnahmen bestehen, um missbräuchliche oder einschüchternde Zugriffe (auch innerhalb der Gerichte) zu verhindern bzw. nachverfolgbar zu machen?

Zu 11.: Bei der (Weiter-) Entwicklung der eingesetzten justizspezifischen IT-Systeme wurde ein hohes Maß an *Systemobservability* umgesetzt. Diese ermöglicht sowohl eine effektive technische Überwachung der Systeme als auch die Verhinderung und Aufdeckung missbräuchlicher Zugriffe zum Schutz richterlicher Entscheidungsprozesse mittels *Logging* und *Monitoring*. Die Datenübertragung innerhalb und zwischen den justizspezifischen IT-Systemen erfolgt zur Wahrung der Revisionssicherheit auch konsequent *transaktionssicher* (z. B. mittels Verschlüsselung, Erzeugung und Überprüfung von Hashwerten).

Fachliche Änderungen z. B. an Dokumenten werden zudem *versioniert* gesichert und so transparent nachvollziehbar gespeichert.

Zudem werden *Zugriffsrechte* auf das erforderliche Maß beschränkt vergeben (vgl. Antworten zu den Fragen 7 bis 10).

Nicht zuletzt dient die technisch, betrieblich und organisatorisch dedizierte Bereitstellung der IT-Systeme innerhalb des *Rechenzentrums Justiz* dem Schutz vor Beeinflussung und missbräuchlichen Zugriffen.

12. Welche Zugriffe werden insgesamt protokolliert (z. B. Lesen, Ändern, Export, Druck etc.)? Gilt dies umfassend für E-Akten/Gerichtsakten und welche Aufbewahrungsfristen gelten für Protokolle?

Zu 12.: Sowohl technische Administratoren als auch Anwendende erhalten von vornherein nur eingeschränkte Zugriffsmöglichkeiten auf IT-Systeme (vgl. Antwort zu Ziffer 8). Konkret bedeutet dies am Beispiel des eingesetzten eIP für die entsprechenden Protokollierungen, dass sämtliche administrativen Zugriffe und Aufrufe von Akten protokolliert und Veränderungen an Dokumenten nachvollziehbar versioniert werden.

Protokolldaten und Versionierung werden dann mit dem jeweiligen Verfahren bei Löschreife entfernt.

13. Werden betroffene Richter:innen/Dezernate automatisch benachrichtigt, wenn Dritte (insb. Außerhalb des Dezernats) auf Akten/Arbeitsdokumente zugreifen? Wenn ja, wie? Wenn nein, warum nicht?

Zu 13.: Im Missbrauchsfall werden die betroffenen Anwendenden in geeigneter und rechtlich zulässiger Weise individuell unterrichtet. Eine Automatisierung dieses Prozesses wird nicht unterstützt.

14. Welche nicht-europäischen Softwareprodukte/Services (z. B. Betriebssysteme, Office/Groupware, Cloud-Dienste, Sicherheitsprodukte) werden in der Berliner Justiz eingesetzt? Es wird gebeten um eine Auflistung nach Systemkategorien.

Zu 14.: Bei den justizspezifischen Kernapplikationen (insb. Fachverfahren, Textsysteme, Systeme für den elektronischen Rechtsverkehr und die elektronische Aktenführung) werden keine außereuropäischen Softwareprodukte, sondern ausschließlich im Justizeigentum stehende IT-Systeme eingesetzt. Bei den standardisierten Büroanwendungen werden aktuell nicht europäische Officeprodukte von Microsoft, Cisco und OpenText genutzt.

Im Bereich der IT-Infrastruktur werden bereits und zunehmend zahlreiche open-source Produkte (z. B. Linux-Distributionen, Wildfly, OpenJDK, MySQL) genutzt.

Teilweise müssen noch nicht-europäische Softwareprodukte eingesetzt werden, da nur diese für die Nutzung der jeweiligen Applikation kompatibel und freigegeben sind. Hierbei handelt es sich um Produkte aus den Bereichen Betriebssysteme (Microsoft, RedHat), Virtualisierung (Citrix, VMware), Datenbanken (Microsoft, Oracle), Server (Apache) und Middleware (Oracle).

15. Welche justizkritischen Kernprozesse (E-Akte, beBPO, elektronischer Rechtsverkehr, Authentifizierung) sind funktional abhängig von solchen Produkten/Services?

Zu 15.: Die justizspezifischen Kernapplikationen sind von nicht-europäischen Infrastruktur-Softwareprodukten nicht funktional abhängig, schon weil die Systeme in abgeschotteten private clouds in den jeweiligen Rechenzentren des ITDZ oder der Justiz ohne technische Zugriffsmöglichkeit der außereuropäischen Hersteller betrieben werden.

16. Wie stellt der Senat sicher, dass die Berliner Justiz bei einem extern veranlassten oder anbieterbedingten Ausfall zentraler nicht-europäischer IT-Dienste („Kill-Switch“) weiterhin arbeitsfähig bleibt und welche konkreten Notbetriebs- und Exit-Maßnahmen sind dafür vorgesehen?

Zu 16.: Ein Killswitch ist durch den Betrieb in souveränen private clouds des ITDZ und der Justiz ausgeschlossen (vgl. Antwort zu Frage 15).

17. In welchem Umfang gilt die Open-Source-Strategie des Landes Berlin auch für die Berliner Justiz?

Zu 17.: Auf Grundlage des Gesetzes zur Förderung des E-Government (EGovG Bln) gilt die Open Source Strategie für das Land Berlin für die öffentliche Verwaltung und grundsätzlich nicht unmittelbar für die Justiz, vgl. § 1 Abs. 2 EGovG Bln. Dies schließt nicht aus, dass aus der Strategie abgeleitete Vorgaben künftig auch für die Justiz gelten werden, beispielsweise Richtlinien für Vergabeverfahren.

Unabhängig vom Geltungsbereich der Open Source Strategie des Landes Berlin teilt die Justiz die dargestellten Ziele und strebt die deutliche Erhöhung des Anteils an open-source Software, wie in der Antwort zu Frage 14 dargestellt, ausdrücklich an.

18. Die Open-Source-Strategie des Landes Berlin sieht die Identifikation von Konzentrationsrisiken sowie die Bewertung von Souveränitätsrisiken vor. Werden diese standardisierten Verfahren für die Justizsysteme bereits durchgeführt und wenn ja, mit welchem Ergebnis? Wenn nein, warum nicht?

Zu 18.: Die Open Source Strategie des Landes Berlin findet auf die Justiz grundsätzlich keine Anwendung. Insbesondere in den länderübergreifenden Entwicklungsverbünden für die justizspezifischen Kernsysteme ist gleichwohl ein fortlaufender Prozess zur Reduzierung proprietärer IT-Infrastrukturen etabliert und vorangeschritten (vgl. zu alledem Antwort zu Frage 17).

19. Gelten die gemäß der Open-Source-Strategie vorgesehene Priorisierung von Open Source in der Beschaffung sowie die Begründungspflicht bei Nicht-Beschaffung auch für Beschaffungen in der Justiz? Wie wird dies insbesondere im Hinblick auf Vergabekriterien und Dokumentation praktisch umgesetzt?

Zu 19.: Die Open Source Strategie des Landes Berlin findet auf die Justiz zwar grundsätzlich keine Anwendung. Auch besteht eine ausdrückliche Begründungspflicht bei Beschaffung von closed-source-Software nicht.

Die Reduzierung proprietärer Software und die Stärkung digitaler Souveränität bleibt aber strategisches Ziel der Justiz und wird bei Beschaffungen – auch ohne explizite Pflicht – ohnehin berücksichtigt, zumal die Beschaffung von open-source Software regelmäßig wirtschaftlicher als die proprietärer Software ist.

Letztlich erfolgt die Beschaffung von closed-source Software nicht aufgrund bewusster Entscheidungen gegen open-source Produkte, sondern aufgrund von kurzfristig nicht überwindbaren Systemabhängigkeiten. Diese können nur mittel -und langfristig über eine Anpassung der komplexen Systemarchitekturen erfolgen. Diese setzt die Berliner Justiz mit den jeweiligen länderübergreifenden Entwicklungsverbünden sukzessive um.

20. Welche Notbetriebsverfahren bestehen, wenn zentrale Arbeitsplatzsoftware (z. B. MS Office) ausfällt, aber E-Akte/beBPo verfügbar sind (und umgekehrt)?

Zu 20.: Die justiziellen Kernapplikationen (insb. Fachverfahren, Textsysteme, Systeme für den elektronischen Rechtsverkehr und die elektronische Aktenführung) sind von zentraler Arbeitsplatzsoftware in beide Richtungen entkoppelt und unabhängig.

Dessen ungeachtet plant die Berliner Justiz gemeinsam mit dem ITDZ für das erste Halbjahr 2026 eine Teststellung für Arbeitsplatzsoftware auf Basis von OpenDesk für den Fall, dass ein Zugriff auf zentrale Arbeitsplatzsoftware – jenseits eines Killswitch – beispielsweise durch das Vorenthalten sicherheitskritischer Updates erschwert wird.

21. Ist den Antworten vonseiten des Senats etwas hinzuzufügen?

Zu 21.: Den hiesigen Antworten ist nichts hinzuzufügen.

Berlin, den 17. Februar 2026

In Vertretung

Dirk Feuerberg
Senatsverwaltung für Justiz
und Verbraucherschutz