**BÜRGERSCHAFT
DER FREIEN UND HANSESTADT HAMBURG**

Drucksache 22/15704

22. Wahlperiode

02. 07. 24

Mitteilung des Senats an die Bürgerschaft

Stellungnahme des Senats zum 32. Tätigkeitsbericht Datenschutz des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit über die Berichtsperiode 2023 (Drucksache 22/15032)

I.

1. Soweit der Sachverhalt im Tätigkeitsbericht umfassend und erschöpfend dargestellt wird, sieht der Senat von eigenen Ausführungen ab, wenn keine weitergehende Stellungnahme erforderlich ist. Dies betrifft die Tzn. II.1.1-1.3, II.7, II.17, III.14, IV.5, VI.1, VI.5, VI.7

2. Des Weiteren sieht der Senat von Ausführungen zu Sachverhalten ab,

   – welche die Dienststelle des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI) betreffen (Kap. VII.) oder

   – die nicht in der Zuständigkeit der Öffentlichen Verwaltung der Freien und Hansestadt Hamburg liegen (Tzn. I., II.4, II.6, II.9-16, II.18, III.5-9, III.11-13, III. 15-21, IV.1-4, V.).

II.

Prüfungen

Im Einzelnen nimmt der Senat zum 32. Tätigkeitsbericht wie folgt Stellung (entspricht der Zählung des Tätigkeitsberichts):

1.4 Prüfung POLAS

Im Rahmen einer erfolgten Stichprobe des HmbBfDI im Zusammenhang mit der Prüfung der Speicherungen von Personen wurden als Ansatzpunkt die Personengebundenen Hinweise (PHW) gewählt. Durch die Polizei Hamburg wurde für den HmbBfDI zunächst eine Liste derjenigen Personen erstellt, die im Polizeilichen Auskunftssystem POLAS mit den PHW „Psychische Verhaltensstörung“, „Gewalttätig“ und „Betäubungsmittelkonsument“ hinterlegt sind.

Das Ergebnis der Stichprobe von 89 Personen führte dazu, dass der HmbBfDI bei der Polizei Hamburg weitergehende Informationen anforderte, deren Übersendung im Frühjahr 2024 erfolgte. Der HmbBfDI führte daraufhin am 23. April 2024 eine Vor-Ort-Überprüfung beim Landeskriminalamt Hamburg durch. Es wurden ca. 40 Datensätze mit entsprechenden PHW-Einträgen eingesehen. Die Bewertung seitens des HmbBfDI liegt der Polizei Hamburg bisher nicht vor.

2. **Data Breach bei der Hochschule für Angewandte Wissenschaften (HAW)**

Wie im Tätigkeitsbericht ausgeführt, stand die Hochschule für Angewandte Wissenschaften

Hamburg während des gesamten Vorgangs im engen Austausch mit dem HmbBfDI. Insbesondere erfolgte hinsichtlich der korrekten Umsetzung der Benachrichtigungspflicht nach Artikel 34 DSGVO eine enge Abstimmung mit der Aufsichtsbehörde. Diese erteilte der HAW Hamburg eine entsprechend bindende Handlungsempfehlung, die von der HAW Hamburg – wie im Bericht dargestellt – umgesetzt wurde.

Maßnahmen, die im Zusammenhang mit dem Datenschutzvorfall durchgeführt werden mussten, wurden zum 1. November 2023 abgeschlossen. Die Hochschule hat fortwährend über den Stand der Maßnahmen auf der eigens dafür eingerichteten Internet-Seite öffentlich berichtet. Diese transparente Kommunikation war ein wichtiger Bestandteil, um das Vertrauen der Betroffenen zu wahren und die Datenschutzbestimmungen einzuhalten.

3. **Sichere Kommunikation mit den Jugendhilfe-Trägern**

Die aktuelle Projektplanung sieht im ersten Schritt die Pilotierung des Mailgateways ab Mitte 2024 vor. Hierbei sollen ausgewählte Abteilungen des Allgemeinen Sozialen Dienstes (ASD) zunächst pilothaft mit einem Träger, welcher über die geeignete technische Ausstattung verfügt, über die Gateway-Infrastruktur kommunizieren. Die Trägerumfrage hatte hierzu erste Auskünfte gegeben. Nach erfolgreicher Pilotierung würde in nachfolgenden Ausbaustufen die Anbindung weiterer Träger vorbereitet werden.

Hinsichtlich der Anregung im Tätigkeitsbericht, das Projekt solle die bereits verworfenen Lösungen (E2E Verschlüsselung mittels Verschlüsselungszertifikaten bei allen Kommunikationspartnern) erneut prüfen, möchte der Senat gerne auf die ursprüngliche Problematik eingehen. Bei der Nutzung einer Zertifikatslösung (z.B. S/MIME) liegt die wesentliche Herausforderung in der initialen Herstellung der Betriebsbereitschaft und dem laufenden Betrieb (Schlüssel austauschen, verwalten, Zertifikate erneuern), gerade im Hinblick auf die hohe Fluktuation beim ASD. Das im Tätigkeitsbericht angesprochene niedrige E-Mailvolumen spielt dabei nur eine untergeordnete Rolle.

Alles in allem sieht auch der Senat die Notwendigkeit einer FHH-weiten Lösung. Die Herausforderungen einer Insellösung (nur ASD und Träger) hatte das Projekt am 12. Oktober 2023 in einem Schreiben an die Senatskanzlei deutlich gemacht. Eine zentrale Lösung wird durch die Unterarbeitsgruppe Verschlüsselte Kommunikation angestrebt (s. hierzu die Ausführungen zu Tzn. III.4).

5. **Umsetzung des Onlinezugangsgesetzes**

Die Senatskanzlei steht in dieser Angelegenheit im Austausch mit dem HmbBfDI. Eine erste Rückmeldung zu allgemeinen Punkten der jeweiligen Prüfberichte ist bereits im April 2024 erfolgt. Alle weiteren Nacharbeiten zu den datenschutzrechtlichen Dokumentationen der Onlinedienste werden dem HmbBfDI nach Prüfung durch die zuständige Datenschutzbeauftragte vorgelegt.

8. **Hinweisgeberschutz bei der Sozialbehörde**

Die Darstellung des HmbBfDI im Tätigkeitsberichtes trifft weitgehend zu. Unzutreffend ist die Aussage, die Offenlegung der Identität habe darauf abgezielt, den Arbeitgeber dazu zu bewegen, das Arbeitsverhältnis zu beenden. Ziel war vielmehr, als zuständige Fachaufsicht die Beliehene über die Pflichtverletzungen des betroffenen Mitarbeiters, aber auch die dadurch bekannt gewordenen organisatorischen Defizite im Maßregelvollzug, zu informieren und diese umgehend abzustellen.

Der Senat wird die Empfehlung des HmbBfDI aufgreifen und bei nächster Gelegenheit darauf hinwirken, die mögliche ungeplante Regelungslücke im Fachrecht auf geeignete Art und Weise zu schließen.

III.
Berichte

1. **Intelligente Videoüberwachung Hansaplatz**

Die Polizei Hamburg übermittelte dem HmbBfDI am 29. April 2024 auf Nachfrage zur Nutzung der Intelligenten Videobeobachtung nachfolgende Informationen.

Der Start des Anschlussprojekts „IVBeo2“ wird für das 2. Quartal 2024 in Aussicht gestellt und soll zwei Jahre dauern. Durch das Vorhaben sollen sowohl sukzessive die Bilder weiterer Kameras des Standortes Hansaplatz mittels der IVBeo bewertet als auch weitere Kamerastandorte skaliert werden. Ferner wird angestrebt, die Modelle zu spezialisieren, um sie auf diesem Weg auf bestimmte (Hamburger) Umgebungsmerkmale anzupassen und um die Ergebnisse i.S. richtiger Entscheidungen (polizeilich relevante Situationen zu erkennen und zu melden) durch das System zu verbessern. Neben der Skalierung auf weitere Kamerastandorte (jedoch nur solcher Kameras an bisher bereits überwachten bzw. derzeit ertüchtigten Orten) ist ebenfalls angedacht, die genutzten Modelle mittels eigener Daten auf die

jeweilige Hamburger Umgebung zu spezialisieren.

Die Zusammenarbeit mit dem IOSB (Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung) soll dahingehend ausgebaut werden, dass Auszüge der in Hamburg aufgenommenen und gespeicherten Videodaten dem IOSB zum Training der Deep Learning Modelle zur Verfügung gestellt werden. Darüber hinaus werden diese Daten gegebenenfalls um Daten aus eigenen Messkampagnen (z.B. Situationsnachstellung durch Polizeitrainer) ergänzt. Nicht zuletzt steht die Ermittlung von Erfolgskriterien einer Skalierung im Zielfokus des Projekts.

2. **Einsatz von Microsoft 365 in der Freien und Hansestadt Hambug**

Die Workshops zu Microsoft 365 wurden auch nach Abschluss des Berichts sowie im Jahr 2024 fortgesetzt. Auf Grund der Komplexität erfordert die Klärung aller Sachverhalte Zeit. Es gibt aus heutiger Sicht jedoch auf allen Gebieten weitere Fortschritte. Im Folgenden geht der Senat auf einzelne Punkte des Berichtes ein.

Die Fragen zur Rechtskonformität wurden seitens des Senats beantwortet, der HmbBfDI bleibt zum Jahresende 2023 jedoch bei einer abweichenden Bewertung. Die Differenzen sollen 2024 durch Workshops aufgelöst werden. Bis Anfang Mai 2024 haben bereits drei weitere Workshops stattgefunden, in denen u.a. ein gemeinsames Verständnis darüber hergestellt wurde, welche Daten von Microsoft wie und wofür verwendet werden. Zudem hat Microsoft einen Vorschlag für eine Zusatzvereinbarung zur Verfügung gestellt, die mit dem HmbBfDI geteilt wurde.

Der Einsatz weiterer nicht cloudbasierter Versionen des Office Pakets (z.B. Office 2021) bleibt weiterhin eine Option. Deswegen ist der flächendeckende Einsatz vom M365 nicht auszuschließen, er ist aber auch noch nicht beschlossen. Ebenfalls bleibt die Nutzung der neuen Funktionalitäten von M365, wie z.B. Teams, auch für die mit M365 ausgestatten Nutzenden zunächst optional. Ende 2023 wurden Alternativen zu Office 2019 bereits diskutiert und Office 2021 als Alternative nicht ausgeschlossen. Parallel dazu werden Möglichkeiten zur Abdeckung des hohen Schutzbedarfs unter Einsatz von Office365 ermittelt. Dazu gehört eine Aufnahme der Anforderungen, die ein Arbeitspaket im laufenden Projektjahr 2024 ist.

Eine Entscheidung zum Einsatz von Viva Engage steht im Jahr 2024 noch aus, es ist nicht Bestandteil der im Jahr 2023 in Produktion befindlichen Version. Eine Pilotierung mit einer eingeschränkten Teilnehmergruppe ist in Vorbereitung.

Die im Bericht angesprochene Evaluierung und ein möglicher Abgleich der Funktionalitäten sind bisher nicht geplant und wurden seitens des Senats bisher auch nicht in Aussicht gestellt.

3. **Microsoft Rights Management System (RMS) in der Freien und Hansestadt Hambug**

Zunächst führt der HmbBfDI aus, dass die Folge der Umstellung auf die neue Infrastruktur eine „Diskontinuität der Verfügbarkeit bisheriger geschützter Inhalte“ sei und „alle bis zum Zeitpunkt des Neuaufbaus mit RMS-geschützten Inhalte dann nicht mehr entschlüsselt werden können und daher unlesbar werden“, sofern „diese nicht bereits oder spätestens bis zum Umschalttermin in anderer Form gespeichert wurden“. Das Angebot seitens der Senatskanzlei bzw. Dataport zur Auswertung der Laufwerke nach verschlüsselten Dateien und eine Anleitung zur Identifikation und Möglichkeiten der Entschlüsselung betroffener Dateien bzw. Mails sollen eine Diskontinuität der Verfügbarkeit weitestgehend verhindern. Eine Diskontinuität kann nur entstehen, wenn die Daten nicht vorher anderweitig gesichert (z.B. in Akten) wurden. Diese Sicherung liegt in der Verantwortung der jeweiligen Behörde.

Im nächsten Schritt führt der HmbBfDI aus, dass es in bestimmten Fällen Pflichten gibt, Maßnahmen zu ergreifen, die über eine Transportverschlüsselung hinausgehen. Diese Darstellung mag weitestgehend richtig sein. Vor dem Hintergrund, dass die gesamte Infrastruktur bei Dataport für Schutzbedarf hoch ausgelegt ist, wird aktuell geprüft, ob und welche weiteren Schutzmaßnahmen erforderlich sind.

Abschließend führt der HmbBfDI an, dass er „für die Abwendung von massiven Datenverlusten in Folge der Umstellung“ im Austausch mit den betroffenen Behörden sei und „der Stand der Inventarisierung und Sicherung betroffener Inhalte in den Behörden derzeit weitgehend unbekannt ist“. Alle oben angedeuteten Maßnahmen sind über diverse behördenübergreifende Gremien kommuniziert worden. Der Stichtag zur Umstellung auf die neue RMS-Infrastruktur ist mehrfach nach Sicherheitsbetrachtung und mit Ausnahmegenehmigung des Informationssicherheitsmanagements der Freien und Hansestadt Hambug verschoben worden, um den Behörden genügend Zeit für die Sichtung sowie Sicherung der Daten geben zu können. Außerdem wurde, wie bereits dargestellt, den Behörden das Angebot unterbreitet, Dataport mit einer Auswertung der Laufwerke nach verschlüsselten Dateien zu beauftragen, um

damit den Stand der Sicherung betroffener Inhalte feststellen zu können.

4. **Unterarbeitsgruppe Verschlüsselte Kommunikation**

Der Senat hat die Erläuterungen und Kritikpunkte des HmbBfDI aufgegriffen und bereits in Teilen entsprechend umgesetzt. Die Unterarbeitsgruppe (UAG) Verschlüsselte Kommunikation hat auf Bitten des Entscheidungsgremiums der IT-Leitungen ihre Ergebnisse klarer aufbereitet, sodass offene Fragen des Entscheidungsgremiums neu bewertet werden konnten. Derzeit unterliegen das Verschlüsselungsprogramm PGP (Pretty Good Privacy), der Verschlüsselungsstandard S/MIME und der mögliche Einsatz eines Verschlüsselungs-Gateways der näheren Betrachtung. Der vom HmbBfDI geforderte Aufbau einer Public-Key-Infrastruktur mit dem Einsatz von S/MIME für jeden Arbeitsplatz der Freien und Hansestadt Hambug wird aktuell prioritär geprüft. Sollte diese Prüfung positiv ausfallen, wird die UAG einen entsprechenden Entscheidungsvorschlag zum weiteren Vorgehen vorlegen.

10. **Einführung eines neuen Krankenhausinformationssystems im Universitätsklinikum Hamburg-Eppendorf**

Es trifft zu, dass das UKE bis zum Ende des Berichtszeitraums eine vollständige Risikobetrachtung beim HmbBfDI noch nicht vorgelegt hatte und Ergebnisse einer solchen Betrachtung noch nicht in die technische Architektur des neuen Systems eingeflossen waren.

Auf Grund der sehr hohen Komplexität und der stetigen und schneller werdenden Weiterentwicklung hat das UKE das Projektvorgehen in einer frühen Projektphase vom linearen Wasserfallmodell hin zu einem agileren iterativen Modell geändert. Hierbei werden die Anforderungen nicht initial festgelegt und dann durch den Dienstleister abgearbeitet, sondern Anforderungen sukzessive ausgeformt und im System in vielen kleinen Einzelschritten umgesetzt. Zugleich wurde bereits vor Beteiligung des HmbBfDI im Projekt eine Arbeitsgruppe zur datenschutzrechtlichen Beratung etabliert. Die Einbindung und personelle Unterlegung dieser Arbeitsgruppe wurden mit Fortschreiten des Projektes fortlaufend verstärkt.

Im Februar 2024 hat das UKE eine detaillierte Datenschutz-Folgenabschätzung abgeschlossen und beim HmbBfDI vorgelegt. In dieser werden die Risiken für die Rechte und Freiheiten natürlicher Personen, im Wesentlichen also der Patientinnen und Patienten, eingehend analysiert und bewertet sowie risikominimierende Maßnahmen beschrieben. Dabei konnte das UKE von dem hohen Niveau der seit 2011 nach ISO 27001 auf Basis von IT-Grundschutz zertifizierten und zusätzlich seit 2019 nach §8a des Gesetzes über das Bundesamt für Sicherheit und Informationstechnik (BSIG)auditierten Informationssicherheit profitieren.

Ebenfalls im Februar 2024 hat das UKE dem HmbBfDI auch ein Rollen- und Berechtigungskonzept vorgelegt, welches trotz der Komplexität der klinischen Arbeit und Anforderungen in der integrativen Zusammenarbeit nachvollziehbar macht, welche Personen wann welche Zugriffsberechtigungen haben. Dabei war ein Ausgleich zwischen der im klinischen Alltag für die Patientensicherheit unabdingbaren schnellen und unkomplizierten Verfügbarkeit aller medizinischer Informationen und einer möglichst starken Reduktion von Zugriffsberechtigungen zu erreichen. Zugriffsberechtigungen hängen konsequent von der Erforderlichkeit für die Arbeit der jeweiligen Bereiche ab und sind außerhalb eines aktiven Behandlungskontextes auf jene Fälle beschränkt, in denen dies unumgänglich ist, wie etwa für Abrechnungsfragen, die Geltendmachung von Betroffenenrechten und Einsichten in die Patientenakte oder Qualitätskontrollen.

Das UKE sieht sich in der Verantwortung, systemische Nachteile für Patientinnen und Patienten durch Nichtverfügbarkeit medizinischer Daten mit höchster Priorität zu vermeiden und zugleich ein Krankenhausinformationssystem zu implementieren, mit dem Mitarbeitende effektiv und sicher arbeiten können. Insgesamt geht das UKE davon aus, dass das Endprodukt, mit Blick auf die nach dem Ende des Berichtszeitraums ergriffenen Maßnahmen, nach seiner Einführung datenschutzkonform umgesetzt wird, ohne hierbei Abstriche in der Patientensicherheit und Versorgungsqualität hinnehmen zu müssen.

IV.

Bußgelder, Anordnungen, Gerichtsverfahren

6. **Einstellung Gerichtsverfahren in Sachen Videmo 360**

Auf Grund der Unzulässigkeit der Feststellungsklage legte das Gericht die Kosten der Behörde für Inneres und Sport auf. Eine Entscheidung in der Sache ist somit nicht getroffen worden. Auch wenn ursprünglich bzw. phasenweise eine Sachentscheidung beiderseitig erwünscht war, haben beide Parteien Erledigungserklärungen abgegeben. Aus diesem Grund hat das Oberverwaltungs-

gericht eine Sachentscheidung nicht treffen können.

VI.

Beratungen öffentlicher Stellen

2. **Sozialrabatt auf Zeitkarten des hvv**

Der Beratungs- und Abstimmungsprozess konnte im ersten Quartal 2024 abgeschlossen werden. Der hvv hat angekündigt, ein entsprechend neu gefasstes Formular zur Einwilligung zu verwenden.

3. **Sickereffektstudie der Behörde für Stadtentwicklung und Wohnen**

Die geplante Sickereffektstudie stellt eine wichtige Planungsgrundlage für zukünftige Wohnungspolitik dar. Im Austausch mit dem HmbBfDI zu Aspekten der Umsetzung der Studie standen im Grundsatz melderechtliche Bedenken und Umsetzungsfragen im Zentrum, aus welchen sich datenschutztechnische Anforderungen an die Datenerhebung und -nutzung ableiten ließen. Im Zentrum der Diskussion standen dabei Problemstellungen, die sich aus der Novellierung des Bundesmeldegesetzes ergeben haben. Der Umgang mit den novellierten melderechtlichen Anforderungen wurde auf Anraten des HmbBfDI von der für den Wohnungsbau zuständigen Behörde umfangreich mit der für das Meldewesen zuständigen Behörde erörtert. Im Ergebnis konnte eine Lösung für die offenen melderechtlichen Umsetzungsfragen gefunden werden, bei der auch die davon abgeleiteten datenschutztechnischen Aspekte berücksichtigt wurden. Die Schaffung einer neuen Rechtsgrundlage hat sich dabei als nicht erforderlich erwiesen. Zugleich ist hierdurch das Erfordernis einer erneuten Befassung des HmbBfDI entfallen. Ein weiteres thematisches Aufgreifen durch den HmbBfDI ist daher nicht vorgesehen. Aspekte des Datenschutzes werden bei der Umsetzung der Studie beachtet.

4. **Digitalisierung der behördlichen Posteingangsbearbeitung**

Der Senat begrüßt die aus datenschutzrechtlicher Sicht positive Bewertung der elektronischen Posteingangsbearbeitung. Zur Anmerkung der fehlenden Rechtsgrundlage für die Trainingsphase weist der Senat darauf hin, dass aus den Trainingsdaten für das System der elektronischen Posteingangsbearbeitung sämtliche personenbezogenen Daten anonymisiert bzw. entfernt werden. Das System wird somit ausschließlich mit nicht personenbezogenen Daten trainiert. Die erhöhten Schutzbedarfsanforderungen für Poststücke mit sensiblen Daten werden aus Sicht des Senats ausreichend berücksichtigt und sind in den Unterlagen dokumentiert.

6. **Robotic Process Automation (RPA) in der Freien und Hansestadt Hambug**

Die Umsetzung einer Prozessautomatisierung mithilfe der Technologie Robotic Process Automation (RPA) folgt einer klar definierten Struktur nach den Vorgaben der Freigabe-Richtlinie der Freien und Hansestadt Hambug und wird entsprechend dokumentiert. Der Senat hat die Anregung des HmbBfDI zum Test- und Freigabeprozess zum Anlass genommen, um die bereits bestehende Testdokumentation zu ergänzen. Die Testfallliste für technische Tests (Unit-Tests) wird seitens Dataport inzwischen automatisiert erzeugt. Die Definition der technischen und fachlichen Testfälle orientiert sich an der mit dem Fachbereich abgestimmten Prozessdokumentation, um technische und fachliche Details vollständig im Test abzubilden. Dies wird ergänzt durch eine Handreichung zur Durchführung der Abnahmetests als Informationsmaßnahme für die Fachbereiche.

Die Maßnahmen zur kryptographischen Signatur von Programm-Code zur Sicherung der Authentizität und Integrität von Roboter-Programmen, wird für die RPA-Infrastruktur der Polizei umgesetzt. Für die Ausweitung dieser Empfehlung auf die weitere RPA-Infrastruktur, sowie eine roboterspezifische Verschlüsselung der Zugangsdaten, wird der Senat Kosten und Nutzen der Maßnahmenumsetzung abwägen.

8. **Videoüberwachung in Spielbanken**

Der Senat weist darauf hin, dass die Spielbank bereits gemäß der bis zum 31. Dezember 2023 gültigen Fassung des § 6 Absatz 2b des Gesetzes über die Zulassung einer öffentlichen Spielbank (Spielbankgesetz) zur Überwachung des ordnungsgemäßen Spiels und der Ermittlung des Bruttospielertrages sowie der Tronceinnahmen den Spielablauf in den, dem Publikum zugänglichen Räumen optisch-elektronisch zu erfassen und zu speichern hatte (Videoüberwachung). Die Daten durften in erforderlichem Umfang ausschließlich für konkrete Zwecke der Spielbankaufsicht sowie zur Feststellung und Überprüfung der Besteuerungsgrundlagen und zur Verfolgung von Steuerordnungswidrigkeiten und Steuerstraftaten genutzt und hierfür an die zuständigen Stellen übermittelt werden.

Durch die Änderung des Spielbankgesetzes zum 1. Januar 2024 (siehe Drucksache 22/13248)

wurde das Spielbankunternehmen verpflichtet, der für die Steueraufsicht zuständigen Behörde einen getrennten, dem Stand der Technik entsprechenden, von unternehmensinternen Kontrollen unabhängigen und unbeschränkten Online-Lesezugriff auf die (bestehenden) Überwachungssysteme zu ermöglichen, damit die für die Steueraufsicht zuständige Behörde diese nachträglich und stichprobenhaft überwachen kann. Die unterstützende Nutzung der Videoüberwachung auch durch das behördliche Aufsichtspersonal dient der weiteren Verbesserung der Aufsichtsmöglichkeiten. Sie eröffnet zudem die Möglichkeit, die Anzahl des sichtbaren Aufsichtspersonals in den Spielsälen zu verringern und den gesetzlichen Auftrag an die Steueraufsicht, auch nach Ausweitung des Spielangebots (bedingt durch die zum 1. Januar 2024 neu erteilte Konzession), gewährleisten zu können (siehe Drucksache 22/13771).

Petitum

Der Senat beantragt, die Bürgerschaft wolle von den Ausführungen dieser Drucksache Kenntnis nehmen.

Gestaltung und Layout: Lütcke & Wulff, Rondenbarg 8, 22525 Hamburg, Tel. (040) 23512 9-0