

Vorlage – zur Beschlussfassung –

Gesetz zur Änderung des Berliner Datenschutzgesetzes und weiterer Rechtsvorschriften

Der Senat von Berlin
InnSport - I E 1 - 02211
9(0)223-1170

An das
Abgeordnetenhaus von Berlin

über Senatskanzlei - G Sen -

Vorblatt

Vorlage - zur Beschlussfassung -
über
Gesetz zur Änderung des Berliner Datenschutzgesetzes und weiterer Rechtsvorschriften

A. Problem

Seit der Neufassung des Berliner Datenschutzgesetzes im Jahr 2018 hat sich Änderungsbedarf ergeben, der sowohl aus der praktischen Anwendung des Gesetzes resultiert als auch aus Folgeänderungen aufgrund bundesrechtlicher Regelungen.

Die veränderte Sicherheitslage, insbesondere mehrere Anschläge auf die Elektrizitätsversorgung in Berlin erfordern eine Stärkung der Resilienz Kritischer Infrastruktur (KRITIS). Für KRITIS besteht weiterhin eine erhöhte, wenn auch abstrakte, Gefährdung. Insbesondere die zuletzt mehrfach betroffene Energieversorgung ist auch weiter als potenzielles Anschlagziel zu sehen. Dieser Gefährdungssituation muss wirksam und nachhaltig entgegengetreten werden.

Auch weitere Rechtsvorschriften, die teilweise seit längerer Zeit nicht mehr geändert wurden, bedürfen - auch im Hinblick auf den Schutz der KRITIS - einer Überarbeitung.

B. Lösung

Das Berliner Datenschutzgesetz und weitere Rechtsvorschriften sind in Teilen zu ändern.

C. Alternative/Rechtsfolgenabschätzung

Keine.

D. Auswirkungen auf den Klimaschutz und die Umwelt
Keine.

E. Auswirkungen auf die Gleichstellung der Geschlechter
Die Regelungen wirken sich gleichermaßen auf alle Geschlechter aus.

F. Auswirkungen auf das elektronische Verwaltungshandeln
Keine.

G. Kostenauswirkungen auf Privathaushalte und/oder Wirtschaftsunternehmen
Keine.

H. Gesamtkosten
Keine.

I. Auswirkungen auf die Zusammenarbeit mit dem Land Brandenburg
Keine.

J. Flächenmäßige Auswirkungen
Keine.

K. Zuständigkeit
Senatsverwaltung für Inneres und Sport

Der Senat von Berlin
InnSport - I E 1 - 02211
9(0)223-1170

An das
Abgeordnetenhaus von Berlin

über Senatskanzlei - G Sen -

Vorlage

- zur Beschlussfassung -

über Gesetz zur Änderung des Berliner Datenschutzgesetzes und weiterer Rechtsvorschriften

Das Abgeordnetenhaus wolle beschließen:

Gesetz zur Änderung des Berliner Datenschutzgesetzes und weiterer Rechtsvorschriften

Vom

Artikel 1

Änderung des Berliner Datenschutzgesetzes

Das Berliner Datenschutzgesetz vom 13. Juni 2018 (GVBl. S. 418), das zuletzt durch Artikel 4 des Gesetzes vom 11. Dezember 2025 (GVBl. S. 590) geändert worden ist, wird wie folgt geändert:

1. In § 1 Absatz 2 werden die Wörter „(ABl. L 199 vom 4.5.2016, S. 89; L 127 vom 23.5.2018, S. 9)“ durch die Wörter „(ABl. L 119 vom 4.5.2016, S. 89; L 127 vom 23.5.2018, S. 9)“ ersetzt.
2. In § 11 Absatz 1 Satz 1 Nummer 1 werden nach den Wörtern „erlassenen Rechtsvorschriften“ die Wörter „sowie der §§ 19, 20 und 25 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982; 2022 I S. 1045), das zuletzt

durch Artikel 10 des Gesetzes vom 9. Januar 2026 (BGBl. 2026 I Nr. 7) geändert worden ist, in der jeweils geltenden Fassung“ eingefügt.

3. Dem § 13 wird folgender Absatz 9 angefügt:

„(9) Im Hinblick auf die Befugnisse der oder des Berliner Beauftragten für Datenschutz und Informationsfreiheit im Rahmen ihrer oder seiner Aufsichtstätigkeit über die Einhaltung der Bestimmungen der §§ 19, 20 und 25 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes findet Artikel 58 der Verordnung (EU) 2016/679 entsprechende Anwendung.“

4. In § 19 Absatz 1 werden das Komma nach den Wörtern „literarischen Zwecken“ und die Wörter „einschließlich der rechtmäßigen Verarbeitung auf Grund der §§ 22 und 23 des Gesetzes betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie in der im Bundesgesetzblatt Teil III, Gliederungsnummer 440-3, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 3 § 31 des Gesetzes vom 16. Februar 2001 (BGBl. I S. 266) geändert worden ist,“ gestrichen.

5. § 20 wird wie folgt geändert:

a) Absatz 1 wird wie folgt gefasst:

„(1) Die Beobachtung öffentlich zugänglicher Räume mit Hilfe optisch-elektronischer Einrichtungen (Videoüberwachung) sowie die Verarbeitung der dadurch erhobenen personenbezogenen Daten ist zulässig, soweit sie zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe, zur Wahrnehmung des Hausrechts oder zur Kontrolle von Zugangsberechtigungen erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der betroffenen Personen überwiegen. Der erforderliche Schutz von Einrichtungen, Anlagen oder Teilen davon im Sinne des § 28 Absatz 1 des Katastrophenschutzgesetzes vom 7. Juni 2021 (GVBl. S. 610), das durch Artikel 7 Nummer 5 des Gesetzes vom 11. Dezember 2025 (GVBl. S. 590) geändert worden ist, in der jeweils geltenden Fassung, von staatlichen Einrichtungen der kritischen Infrastruktur, die Einrichtungen nach § 28 Absatz 1 Katastrophenschutzgesetz entsprechen, von zur Aufrechterhaltung der Staats- und Regierungsfunktionen unabdingbar notwendigen Einrichtungen, die einen mit Einrichtungen nach § 28 Absatz 1 Katastrophenschutzgesetz vergleichbaren Schutzbedarf aufweisen, sowie ziviler Objekte, deren Ausfall die zivile Verteidigungsfähigkeit dauerhaft einschränken würde oder denen neben der zivilen auch eine militärische Bedeutung zukommt, dient dem öffentlichen Interesse und geht schutzwürdigen Interessen der betroffenen Personen in der Regel vor.“

b) Dem Absatz 2 wird folgender Satz angefügt:

„Satz 1 gilt nicht in den Fällen des Absatzes 1 Satz 2, soweit dies den erforderlichen Schutz von Einrichtungen, Anlagen oder Teilen davon oder ziviler Objekte im Sinne des Absatzes 1 Satz 2 beeinträchtigen würde; § 23 Absatz 2 Satz 1 und 2 gilt entsprechend.“

6. § 24 Absatz 1 Satz 3 wird aufgehoben.

7. In § 26 Absatz 2 Satz 1 werden die Wörter „in einem Datenschutzkonzept“ gestrichen.

8. In § 48 Absatz 6 werden die Wörter „im Sinne des Absatzes 5“ durch die Wörter „oder das andere Rechtsinstrument nach Absatz 5“ ersetzt.

9. In § 50 Absatz 4 Satz 1 werden die Wörter „in einem Datenschutzkonzept“ gestrichen.

10. § 56 Absatz 1 Satz 2 wird wie folgt geändert:

- a) In Nummer 9 werden vor den Wörtern „die vorgesehenen Fristen“ die Wörter „wenn möglich“ und ein Komma eingefügt.
- b) In Nummer 10 werden vor den Wörtern „eine allgemeine Beschreibung“ die Wörter „wenn möglich“ und ein Komma eingefügt.

11. In § 58 Satz 2 Nummer 5 werden nach den Wörtern „im Zusammenhang mit einer Straftat“ ein Komma und die Wörter „wie insbesondere Personen, die bei Ermittlungen in Verbindung mit der betreffenden Straftat oder beim anschließenden Strafverfahren als Zeuginnen oder Zeugen in Betracht kommen oder Personen, die Hinweise zur Straftat geben können“ eingefügt.

12. In § 67 Absatz 1 Satz 1 in dem Satzteil vor Nummer 1 wird nach den Wörtern „für die Erfüllung seiner Aufgaben“ das Wort „unbedingt“ eingefügt.

Artikel 2

Änderung des Berliner Informationsfreiheitsgesetzes

Das Berliner Informationsfreiheitsgesetz vom 15. Oktober 1999 (GVBl. S. 561), das zuletzt durch Artikel 10 des Gesetzes vom 10. Juli 2025 (GVBl. S. 270) geändert worden ist, wird wie folgt geändert:

1. Dem § 2 wird folgender Absatz 3 angefügt:

„(3) Dieses Gesetz gilt nicht, soweit Informationen über Einrichtungen, Anlagen oder Teile davon im Sinne des § 28 Absatz 1 des Katastrophenschutzgesetzes vom 7. Juni 2021 (GVBl. S. 610), das durch Artikel 7 Nummer 5 des Gesetzes vom 11. Dezember 2025

(GVBl. S. 590) geändert worden ist, in der jeweils geltenden Fassung, Informationen, die für die Funktionsfähigkeit von staatlichen Einrichtungen der kritischen Infrastruktur, die Einrichtungen nach § 28 Absatz 1 Katastrophenschutzgesetz entsprechen, oder von zur Aufrechterhaltung der Staats- und Regierungsfunktionen unabdingbar notwendigen Einrichtungen, die einen mit Einrichtungen nach § 28 Absatz 1 Katastrophenschutzgesetz vergleichbaren Schutzbedarf aufweisen, von Bedeutung sind, oder Informationen über zivile Objekte, deren Ausfall die zivile Verteidigungsfähigkeit dauerhaft einschränken würde oder denen neben der zivilen auch eine militärische Bedeutung zukommt, betroffen sind.“

2. § 9 wird wie folgt geändert:

a) Absatz 1 Satz 2 wird wie folgt gefasst:

„Das Gleiche gilt, soweit und solange durch das vorzeitige Bekanntwerden des Akteneintrags der Erfolg eines Ermittlungsverfahrens wegen einer Straftat oder einer Ordnungswidrigkeit gefährdet werden kann, nachteilige Auswirkungen für das Land Berlin bei der Durchführung eines laufenden Gerichtsverfahrens zu befürchten sind oder nachteilige Auswirkungen für das Land Berlin bei der Vorbereitung und Durchführung einer gerichtlichen oder außergerichtlichen Geltendmachung oder Abwehr von Ansprüchen unmittelbar zu befürchten sind.“

b) In Absatz 2 Satz 1 werden die Wörter „nur bis zu deren rechtskräftigem Abschluss.“ durch die Wörter „sowie der Vorbereitung und Durchführung einer gerichtlichen oder außergerichtlichen Geltendmachung nur bis zum rechtskräftigen Abschluss der Gerichtsverfahren oder bis zur Beendigung der außergerichtlichen Geltendmachung oder Abwehr von Ansprüchen.“ ersetzt.

c) Folgender Absatz 3 wird angefügt:

„(3) Über Absatz 1 und 2 hinaus besteht das Recht auf Akteneinsicht oder Akteneintragskunft nicht

1. für Vorgänge der Steuerverwaltung,

2. für Informationen,

a) über die die Antragstellerin oder der Antragsteller bereits verfügt oder die in zumutbarer Weise aus allgemein zugänglichen Quellen beschafft werden können,

b) die einer Geheimhaltungs- und Vertraulichkeitspflicht durch Einstufung als Verschlusssache nach § 6 Absatz 1 und 2 des Berliner Sicherheitsüberprüfungsgesetzes vom 25. Juni 2001 (GVBl. S. 243), das zuletzt durch Artikel 3 des Gesetzes vom 13. Juni 2018 (GVBl. S. 418) geändert worden ist, in der jeweils geltenden Fassung oder nach der Geschäftsordnung des Abgeordnetenhauses von Berlin unterfallen,

c) die einem Berufs- oder besonderen Amtsgeheimnis unterliegen oder

- d) deren Bekanntwerden die IT-Sicherheit oder die IT-Infrastruktur der in § 2 Absatz 1 genannten öffentlichen Stellen gefährden könnte, oder
- 3. wenn der Antrag offensichtlich missbräuchlich, insbesondere zum Zweck der Vereitelung oder Verzögerung von Verwaltungshandlungen, erfolgt.“

Artikel 3 **Änderung des Bäder-Anstaltsgesetzes**

Das Bäder-Anstaltsgesetz vom 25. September 1995 (GVBl. S. 617), das zuletzt durch Artikel 11 des Gesetzes vom 10. Juli 2025 (GVBl. S. 270) geändert worden ist, wird wie folgt geändert:

1. Dem § 23 wird folgender Satz angefügt:

„Die Verarbeitung ist insbesondere zulässig zur

1. Kontrolle der Gültigkeit von Eintrittskarten oder Zugangsberechtigungen,
2. Gewährleistung des oder Wiederherstellung eines sicheren Badbetriebes oder
3. Wahrnehmung oder Durchsetzung des Hausrechts insbesondere bei Verstößen gegen die Haus- und Badeordnung.“

2. Nach § 23 wird folgender § 24 eingefügt:

„§ 24 Videoüberwachung

(1) Die Beobachtung öffentlich zugänglicher Räume der Bäder mit Hilfe optisch-elektronischer Einrichtungen (Videoüberwachung) sowie die Verarbeitung der dadurch erhobenen personenbezogenen Daten ist zulässig, soweit sie

1. zur Kontrolle von Zugangsberechtigungen,
 2. zur Gewährleistung des oder Wiederherstellung eines sicheren Badbetriebes,
 3. zur Wahrnehmung oder Durchsetzung des Hausrechts insbesondere bei Verstößen gegen die Haus- und Badeordnung oder
 4. zum Schutz des Eigentums oder Besitzes
- erforderlich ist und keine Anhaltspunkte bestehen, dass überwiegende schutzwürdige Interessen der betroffenen Personen entgegenstehen.

(2) § 20 Absatz 2, 3 und 5 des Berliner Datenschutzgesetzes vom 13. Juni 2018 (GVBl. S. 418), das zuletzt durch Artikel 1 des Gesetzes vom [einsetzen: Datum und Fundstelle des Gesetzes zur Änderung des Berliner Datenschutzgesetzes und weiterer Rechtsvorschriften] geändert worden ist, in der jeweils geltenden Fassung gilt entsprechend.“

3. Der bisherige § 24 wird § 25.

Artikel 4

Änderung des Gesetzes über das Verfahren der Berliner Verwaltung

§ 6 Absatz 2 des Gesetzes über das Verfahren der Berliner Verwaltung vom 21. April 2016 (GVBl. S. 218), das zuletzt durch Artikel 5 des Gesetzes vom 11. Dezember 2025 (GVBl. S. 590) geändert worden ist, wird wie folgt gefasst:

„(2) Die Behörde ist zur Gestattung der Akteneinsicht nicht verpflichtet, soweit das Bekanntwerden des Inhalts der Akten dem Wohl des Bundes oder eines Landes Nachteile bereiten oder zu einer schwerwiegenden Gefährdung des Gemeinwohls führen würde. Dies ist in der Regel bei Akteninhalten über Einrichtungen, Anlagen oder Teile davon im Sinne des § 28 Absatz 1 des Katastrophenschutzgesetzes vom 7. Juni 2021 (GVBl. S. 610), das durch Artikel 7 Nummer 5 des Gesetzes vom 11. Dezember 2025 (GVBl. S. 590) geändert worden ist, in der jeweils geltenden Fassung, über staatliche Einrichtungen der kritischen Infrastruktur, die Einrichtungen nach § 28 Absatz 1 Katastrophenschutzgesetz entsprechen, über zur Aufrechterhaltung der Staats- und Regierungsfunktionen unabdingbar notwendige Einrichtungen, die einen mit Einrichtungen nach § 28 Absatz 1 Katastrophenschutzgesetz vergleichbaren Schutzbedarf aufweisen, sowie über zivile Objekte, deren Ausfall die zivile Verteidigungsfähigkeit dauerhaft einschränken würde oder denen neben der zivilen auch eine militärische Bedeutung zukommt, anzunehmen. Im Übrigen gelten die Regelungen der §§ 5 bis 12 des Berliner Informationsfreiheitsgesetzes vom 15. Oktober 1999 (GVBl. S. 561), das zuletzt durch Artikel 2 des Gesetzes vom [einsetzen: Datum und Fundstelle des Gesetzes zur Änderung des Berliner Datenschutzgesetzes und weiterer Rechtsvorschriften] geändert worden ist, in der jeweils geltenden Fassung entsprechend.“

Artikel 5

Änderung des Allgemeinen Sicherheits- und Ordnungsgesetzes

In § 17 Absatz 4 des Allgemeinen Sicherheits- und Ordnungsgesetzes in der Fassung der Bekanntmachung vom 11. Oktober 2006 (GVBl. S. 930), das zuletzt durch Artikel 2 des Gesetzes vom 11. Dezember 2025 (GVBl. S. 590) geändert worden ist, werden nach dem Wort „Umwelt“ ein Komma und die Wörter „eine Beeinträchtigung der Funktionsfähigkeit von Einrichtungen, Anlagen oder Teilen davon im Sinne des § 28 Absatz 1 des Katastrophenschutzgesetzes vom 7. Juni 2021 (GVBl. S. 610), das durch Artikel 7 Nummer 5 des Gesetzes vom 11. Dezember 2025 (GVBl. S. 590) geändert worden ist, in der jeweils geltenden Fassung, von staatlichen Einrichtungen der kritischen Infrastruktur, die Einrichtungen nach § 28 Absatz 1 Katastrophenschutzgesetz entsprechen, oder von zur Aufrechterhaltung der Staats- und Regierungsfunktionen unabdingbar notwendigen Einrichtungen, die einen mit Einrichtungen nach §

28 Absatz 1 Katastrophenschutzgesetz vergleichbaren Schutzbedarf aufweisen,“ und nach den Wörtern „illegale Beschäftigung“ ein weiteres Komma eingefügt.

Artikel 6

Änderung der Open Data Verordnung

§ 5 Absatz 1 Nummer 1 der Open Data Verordnung vom 7. Juli 2020 (GVBl. S. 622), die zuletzt durch Artikel 31 des Gesetzes vom 10. Juli 2025 (GVBl. S. 270) geändert worden ist, wird wie folgt gefasst:

„1. an ihnen kein oder nur ein eingeschränktes Zugangsrecht auf Grund gesetzlicher Regelungen, insbesondere gemäß den §§ 5, 9 bis 12 des Berliner Informationsfreiheitsgesetzes vom 15. Oktober 1999 (GVBl. S. 561), das zuletzt durch Artikel 2 des Gesetzes vom [einsetzen: Datum und Fundstelle des Gesetzes zur Änderung des Berliner Datenschutzgesetzes und weiterer Rechtsvorschriften] geändert worden ist, in der jeweils geltenden Fassung besteht oder ein Zugangsrecht erst nach der Beteiligung Dritter bestünde oder es sich um Informationen im Sinne des § 2 Absatz 3 des Berliner Informationsfreiheitsgesetzes handelt,“

Artikel 7

Inkrafttreten

Dieses Gesetz tritt am Tag nach der Verkündung im Gesetz- und Verordnungsblatt für Berlin in Kraft.

A. Begründung:

a) Allgemeiner Teil:

Seit der Neufassung des Berliner Datenschutzgesetzes im Jahr 2018 hat sich Änderungsbedarf ergeben, der sowohl aus der praktischen Anwendung des Gesetzes resultiert als auch aus Folgeänderungen aufgrund bundesrechtlicher Regelungen. Neben der Umsetzung dieser Anpassungen ist es auch Ziel des Gesetzentwurfs, zu einer Vereinfachung des Berliner Datenschutzrechts im Rahmen der europa- und bundesrechtlichen Vorgaben beizutragen. Dazu werden formale Anforderungen teilweise vereinfacht.

Die veränderte Sicherheitslage, insbesondere mehrere Anschläge auf die Elektrizitätsversorgung in Berlin erfordern eine Stärkung der Resilienz Kritischer Infrastruktur (KRITIS). Für KRITIS besteht weiterhin eine erhöhte, wenn auch abstrakte, Gefährdung. Insbesondere die zuletzt mehrfach betroffene Energieversorgung ist auch weiter als potenzielles Anschlagsziel zu sehen. Dieser Gefährdungssituation muss wirksam und nachhaltig entgegengetreten werden. Unter anderem weitgehende Transparenzpflichten stehen dazu in einem deutlichen Spannungsverhältnis. Die mit dem vorliegenden Gesetzentwurf beabsichtigten Änderungen stellen einen wirksamen und nachhaltigen Beitrag zur Stärkung der Resilienz Kritischer Infrastruktur dar, reagieren auf die veränderte Sicherheitslage und treten der Gefährdungssituation angemessen entgegen.

Auch weitere Gesetze, die teilweise seit längerer Zeit nicht mehr geändert wurden, bedürfen – auch im Hinblick auf den Schutz der KRITIS – einer Anpassung und ggf. punktuellen Überarbeitung.

b) Einzelbegründung:

Zu Artikel 1 (Änderung des BlnDSG):

Zu Nummer 1 (Änderung § 1 Absatz 2):

Es wird ein früheres Redaktionsversehen bei der Angabe der Fundstelle der JI-Richtlinie korrigiert.

Zu Nummer 2 (Änderung § 11):

Während es sich bei den §§ 19 und 20 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes (TDDDG) um datenschutzrechtliche Vorschriften handelt, die bereits von § 11 Nr. 1 BlnDSG erfasst sind, ist Gegenstand von § 25 TDDDG der Schutz der Integrität von Endeinrichtungen, insbesondere ist sein Schutzbereich nicht auf personenbezogene

Daten beschränkt. Das TDDDG enthält keine allgemeinen Regelungen dazu, in welchem Umfang den zuständigen Aufsichtsbehörden Befugnisse zur Gewährleistung der Einhaltung von § 25 TDDDG zustehen. Die Regelung schafft daher eine Grundlage für die Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI), auf der rechtssicher Untersuchungs- und Abhilfemaßnahmen im Anwendungsbereich des TDDDG getroffen werden können.

In der Folge ist § 13 Absatz 9 BlnDSG entsprechend anzupassen.

Zu Nummer 3 (Änderung § 13):

Es handelt sich um eine Folgeanpassung zu der Änderung in § 11 BlnDSG.

Zu Nummer 4 (Änderung § 19):

Ein Mehrwert des Einschubs der §§ 22 und 23 des Gesetzes betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie (KunstUrhG) ist nicht erkennbar. Ein vergleichbarer Hinweis auf das KunstUrhG ist zudem in keiner Parallelvorschrift in den Presse-, Datenschutz- und Mediengesetzen der anderen Länder enthalten. Es handelt sich mithin um eine Berliner Besonderheit. Dass im Landesrecht ein Verweis auf das KunstUrhG aufgenommen wurde, hat jedoch keinen Einfluss auf den weiteren Bestand dieses Bundesgesetzes. Dem Land Berlin kommt schon keine Gesetzgebungskompetenz für den Regelungsbereich des KunstUrhG zu. Der Einschub verdeutlicht nur, dass eine textbasierte Datenverarbeitung losgelöst von einer Bildberichterstattung zu beurteilen ist – selbst wenn beides innerhalb desselben journalistischen Beitrags stattfindet. Werden im Text eines journalistischen Beitrags personenbezogene Daten verwendet und dazu Bildnisse gezeigt, so kann für beide Bestandteile das Medienprivileg zur Anwendung kommen. Die Bildberichterstattung ist jedoch gesondert zu bewerten. Über diese klarstellende Funktion hinaus hat der Einschub keinen Mehrwert. Er ist daher zu streichen.

Zu Nummer 5 (Änderung § 20):

Zu Buchstabe a (Änderung § 20 Absatz 1):

Die Änderungen in Absatz 1 Satz 1 dienen der Klarstellung, dass das Erheben und Erfassen personenbezogener Daten in öffentlich zugänglichen Räumen per Videoüberwachung und die weitere Verarbeitung dieser personenbezogenen Daten auch außerhalb dieser öffentlich zugänglichen Räume zulässig ist.

Ebenso dient die Einfügung des Zwecks der Kontrolle von Zugangsberechtigungen der Klarstellung für Fälle, in denen dies nicht bereits vom Zweck der Wahrnehmung des Hausrechts erfasst ist.

Es ist weiterhin sowohl die Erforderlichkeit der Maßnahme nachzuweisen als auch eine Abwägung zwischen den schutzwürdigen Interessen der betroffenen Personen und der möglichen Videoüberwachung vorzunehmen.

Die Aufnahme von Satz 2 ist im Hinblick auf eine veränderte Sicherheitslage und in Reaktion auf mehrere Anschläge auf die Elektrizitätsversorgung notwendig. Die Regelung dient neben dem Schutz der Kritischen Infrastrukturen gerade auch dem Schutz der von diesen zu schützenden Individualrechtsgüter, wie vor allem der Unversehrtheit des Lebens und der Gesundheit der konkret betroffenen Bevölkerung. Die möglichen Folgewirkungen von Beeinträchtigungen der Kritischen Infrastrukturen auch auf die elementaren Individualrechtsgüter der Bevölkerung gebieten entsprechende Schutzvorkehrungen, die auch mit der vorgesehenen Regelung unterstützt werden sollen.

Kritische Infrastrukturen sind nach der Definition in § 28 Absatz 1 Katastrophenschutzgesetz „Einrichtungen, Anlagen oder Teile davon, die den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Entsorgung, Gesundheit, Wasser, Ernährung, Medien und Kultur oder Finanz- und Versicherungswesen angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden“.

Die Regelung bezieht sich auch auf staatliche Einrichtungen der kritischen Infrastruktur, die Einrichtungen nach § 28 Absatz 1 Katastrophenschutzgesetz entsprechen, und auf zur Aufrechterhaltung der Staats- und Regierungsfunktionen unabdingbar notwendige Einrichtungen, die einen mit Einrichtungen nach § 28 Absatz 1 Katastrophenschutzgesetz vergleichbaren Schutzbedarf aufweisen, weil diese gleichermaßen schutzbedürftig sind. Davon können insbesondere einzelne Einrichtungen der Sicherheitsbehörden und der Justiz betroffen sein.

Die Zivile Verteidigungsfähigkeit beschreibt die Fähigkeit eines Staates, im äußeren Notstand den Zivilschutz, die Aufrechterhaltung der Staats- und Regierungsfunktionen, die Versorgung der Bevölkerung und der Streitkräfte sowie die Unterstützung der Streitkräfte sicherzustellen. Die Zivile Verteidigung fußt dabei auf den Vorsorgemaßnahmen des Katastrophenschutzes und dem Krisenmanagement der Länder. Gemeinsam mit der militärischen Verteidigung bildet sie das Fundament einer effektiven Gesamtverteidigung. Sie ist hierbei kein nachgelagerter Aspekt, sondern eine unverzichtbare Voraussetzung für das Funktionieren einer gesamtstaatlichen Sicherheitsvorsorge. Zivile Objekte sind zunächst alle nicht militärisch genutzten Gebäude und Gebäudekomplexe, Anlagen und Einrichtungen sowie Flächen. Schutzwürdig sind diese zum einen, soweit ihr Ausfall die zivile Verteidigungsfähigkeit dauerhaft einschränken würde. Eine Dauerhaftigkeit ist anzunehmen, wenn ein Ausfall nicht nur vorübergehend dazu führen würde, dass eines oder mehrere Schutzziele der Zivilen Verteidigung nicht mehr sichergestellt werden können. Zum anderen besteht eine Schutzwürdigkeit, wenn den zivilen Objekten neben der zivilen auch eine militärische Bedeutung zukommt. Dies wäre beispielsweise der Fall, wenn eine zivil genutzte Brücke im Verteidigungsfall entscheidend für militärische Truppenbewegungen oder Evakuierungen wird und dadurch zwar ein ziviles Objekt bleibt, diesem aber militärische Bedeutung zukommt.

Die Erforderlichkeit des Schutzes ist dabei nach räumlichen Kriterien zu bemessen und muss dem Grundsatz der Verhältnismäßigkeit genügen. Die Regelvermutung erleichtert den Begründungsaufwand für die Betreiberinnen und Betreiber der Einrichtungen und Anlagen Kritischer Infrastruktur.

Zu Buchstabe b (Änderung § 20 Absatz 2):

Um den Schutz der kritischen Einrichtungen, Anlagen oder Teile davon zu gewährleisten, kann es ggf. notwendig sein, für diesen Bereich auf die grundsätzlich vorgesehene frühzeitige Information über die erfolgende Verarbeitung personenbezogener Daten zu verzichten. Die Regelung bezieht sich auch auf staatliche Einrichtungen der kritischen Infrastruktur, die Einrichtungen nach § 28 Absatz 1 Katastrophenschutzgesetz entsprechen, und auf zur Aufrechterhaltung der Staats- und Regierungsfunktionen unabdingbar notwendige Einrichtungen, die einen mit Einrichtungen nach § 28 Absatz 1 Katastrophenschutzgesetz vergleichbaren Schutzbedarf aufweisen, weil diese gleichermaßen schutzbedürftig sind. Davon können insbesondere einzelne Einrichtungen der Sicherheitsbehörden und der Justiz betroffen sein. Die Regelung macht insofern Gebrauch von der gemäß Artikel 23 Absatz 1 Buchstabe c und i der Verordnung EU 2016/679 zugelassenen Beschränkung der Informationspflichten des Verantwortlichen nach Artikel 13 der Verordnung (EU) 2016/679.

Im Rahmen der notwendigen Erforderlichkeitsprüfung ist u. a. abzuwägen, ob der Zweck der Videoüberwachung (also der Schutz der kritischen Einrichtungen, Anlagen oder Teile davon oder zivilen Objekte im Sinne des Absatzes 1 Satz 2) durch eine Kennzeichnung als videoüberwachter Bereich beeinträchtigt werden könnte. Diese Abwägung rechtfertigt einen Verzicht auf die Kennzeichnung in den Fällen des Absatzes 1 Satz 2, wenn hierdurch der erforderliche Schutz beeinträchtigt würde. Letzteres wird etwa dann der Fall sein, wenn eine schutzbedürftige kritische Anlage erst durch eine entsprechende Kennzeichnung als solche wahrnehmbar wird. Durch den Verweis auf § 23 Absatz 2 Satz 1 und 2 BlnDSG wird klargestellt, dass die Entscheidung über das Absehen von der Kennzeichnung und damit von der Information die Leitung der öffentlichen Stelle oder eine von ihr bestimmte, bei der öffentlichen Stelle beschäftigte Person trifft und die Gründe für dieses Absehen zu dokumentieren und der oder dem behördlichen Datenschutzbeauftragten mitzuteilen sind.

Im Rahmen der Videoüberwachung werden Bilddaten der betroffenen Personen verarbeitet. Soweit davon auch besondere Kategorien personenbezogener Daten im Sinne des Artikel 9 der Verordnung (EU) 2016/679 betroffen sind, ist deren Verarbeitung nach Artikel 9 Absatz 2 Buchstabe g der Verordnung (EU) 2016/679 zulässig, da diese aus Gründen eines erheblichen öffentlichen Interesses erforderlich ist. Die Absätze 3 und 5 enthalten bereits Vorschriften, die eine zweckändernde Verarbeitung sowie die unverzügliche Löschung der personenbezogenen Daten regeln. Im Hinblick auf diese Regelungen werden die Risiken für die betroffenen Personen bei einem Absehen von der Kennzeichnungspflicht im Rahmen der Regelung in Absatz 2 zweiter Halbsatz als gering eingestuft. Die Unterrichtung der betroffenen Personen über das Absehen von der Kennzeichnungspflicht unterbleibt, da

auch eine solche Unterrichtung dem Zweck der Beschränkung abträglich wäre (Artikel 23 Absatz 2 Buchstabe h der Verordnung (EU) 2016/679).

Zu Nummer 6 (Änderung § 24):

In Artikel 23 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung - DSGVO) gibt es keine entsprechende Ausnahmeregelung für Daten, die zu Zwecken der Datensicherung oder der Datenschutzkontrolle gespeichert sind. Die betroffene Person soll sich ein umfassendes Bild machen können, welche Daten zu ihrer Person gespeichert werden. Bei diesen Daten handelt es sich nicht lediglich um Sicherheitskopien von Daten, die anderswo noch gespeichert sind. Vielmehr betrifft dies alle Daten, die aus dem aktiven Datenbestand entfernt wurden und - soweit sie personenbezogen sind - unter das Auskunftsrecht fallen.

Weiterhin besteht nach bisherigen Erkenntnissen für die Vorschrift in der Verwaltungspraxis kein Bedarf.

Zu Nummer 7 (Änderung § 26):

Mit der Änderung entfällt die formale Anforderung hinsichtlich der Art und Weise der Dokumentation. Die Dokumentationspflicht kann auch in anderer Form vollumfänglich erfüllt werden. Erhalten bleibt die Notwendigkeit zur Dokumentation der „zu treffenden technischen und organisatorischen Maßnahmen auf der Grundlage einer Risikoanalyse“. Die geeignete und konkrete Art der Umsetzung sollen dabei die Verantwortlichen selbst bestimmen; es bleibt den öffentlichen Stellen unbenommen, die Dokumentation weiterhin in einem Datenschutzkonzept durchzuführen. Zusätzlich soll es möglich werden, die Dokumentation auch in anderer Form vorzunehmen. Die hohen Anforderungen der DSGVO - u. a. zur Rechenschaftspflicht der Verantwortlichen über die von ihnen zu erfüllenden Pflichten (insbesondere aus den Artikeln 24, 25, 32 und 35 DSGVO) - bleiben dabei bestehen. Die Pflicht zur Dokumentation an sich und die inhaltlichen Anforderungen an die Dokumentation bleiben unberührt.

Zu Nummer 8 (Änderung § 48):

§ 48 Absatz 6 wird an den Wortlaut des Artikels 22 Absatz 4 der Richtlinie (EU) 2016/680 angepasst und macht damit deutlich, dass keine höheren formalen Anforderungen an die Abfassung der Verträge oder anderer Rechtsinstrumente nach § 48 Absatz 5 zu stellen sind als von Artikel 22 Absatz 4 der Richtlinie (EU) 2016/680 vorgesehen. Damit wird eine schnelle und aufwandsarme Abfassung neuer und die Anpassung bestehender Auftragsverarbeitungsverträge ermöglicht. Die Regelung folgt daher den Anforderungen des modernen und volldigitalisierten Schriftverkehrs und der digitalen Aktenhaltung.

Zu Nummer 9 (Änderung § 50):

Siehe Begründung zu Nummer 7.

Zu Nummer 10 (Änderung § 56):

§ 56 Absatz 1 Satz 2 Nummern 9 und 10 werden an den Wortlaut des Artikel 24 Absatz 1 Buchstaben h und i der Richtlinie (EU) 2016/680 angepasst und machen damit deutlich, dass keine höheren formalen Anforderungen an ein Verzeichnis von Verarbeitungstätigkeiten zu stellen sind als von Artikel 24 Absatz 1 Buchstabe h und i der Richtlinie (EU) 2016/680 vorgesehen.

Zu Nummer 11 (Änderung § 58):

Die Änderung in § 58 Satz 2 Nummer 5 BlnDSG dient der redaktionellen Anpassung an den Wortlaut des Artikel 6 lit d der JI-Richtlinie.

Zu Nummer 12 (Änderung § 67):

Es handelt sich um eine redaktionelle Anpassung. Damit orientiert sich § 67 BlnDSG am Wortlaut von Artikel 39 Absatz 1 lit. a) JI-Richtlinie und an § 81 Absatz 1 Bundesdatenschutzgesetz und die Formulierung „unbedingt erforderlich“ wird in den Regelungstext übernommen. Auch andere Länder setzen die europarechtlichen Vorgaben entsprechend um und haben gleichlautende Vorschriften in ihren Datenschutzgesetzen (vgl. § 76 Absatz 1 Hessisches Datenschutz- und Informationsfreiheitsgesetz, § 65 Absatz 1 Datenschutzgesetz Nordrhein-Westfalen, § 69 Absatz 1 Landesdatenschutzgesetz Rheinland-Pfalz, § 57 Absatz 1 Landesdatenschutzgesetz Schleswig-Holstein, § 60 Absatz 1 Thüringer Datenschutzgesetz, § 46 Absatz 1 Hamburgisches Gesetz über die Datenverarbeitung der Polizei). Somit dient die Anpassung auch der Förderung eines einheitlichen Rechtsverständnisses.

Zu Artikel 2 (Änderung des IFG):**Zu Nummer 1 (§ 2 Absatz 3 neu):**

Die Aufnahme von Absatz 3 ist im Hinblick auf eine veränderte Sicherheitslage und in Reaktion auf mehrere Anschläge auf die Elektrizitätsversorgung notwendig. Kritische Infrastrukturen sind nach der Definition in § 28 Absatz 1 Katastrophenschutzgesetz „Einrichtungen, Anlagen oder Teile davon, die den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Entsorgung, Gesundheit, Wasser, Ernährung, Medien und Kultur oder Finanz- und Versicherungswesen angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden“. Die Ausnahme bezieht sich auch auf Informationen, die für die Funktionsfähigkeit von staatlichen Einrichtungen der kritischen Infrastruktur, die Einrichtungen nach § 28 Absatz 1 Katastrophenschutzgesetz entsprechen, oder von zur Auf-

rechterhaltung der Staats- und Regierungsfunktionen unabdingbar notwendigen Einrichtungen, die einen mit Einrichtungen nach § 28 Absatz 1 Katastrophenschutzgesetz vergleichbaren Schutzbedarf aufweisen, von Bedeutung sind, weil diese gleichermaßen schutzbedürftig sind. Davon können insbesondere einzelne Einrichtungen der Sicherheitsbehörden und der Justiz betroffen sein.

Die Zivile Verteidigungsfähigkeit beschreibt die Fähigkeit eines Staates, im äußeren Notstand den Zivilschutz, die Aufrechterhaltung der Staats- und Regierungsfunktionen, die Versorgung der Bevölkerung und der Streitkräfte sowie die Unterstützung der Streitkräfte sicherzustellen. Die Zivile Verteidigung fußt dabei auf den Vorsorgemaßnahmen des Katastrophenschutzes und dem Krisenmanagement der Länder. Gemeinsam mit der militärischen Verteidigung bildet sie das Fundament einer effektiven Gesamtverteidigung. Sie ist hierbei kein nachgelagerter Aspekt, sondern eine unverzichtbare Voraussetzung für das Funktionieren einer gesamtstaatlichen Sicherheitsvorsorge. Zivile Objekte sind zunächst alle nicht militärisch genutzten Gebäude und Gebäudekomplexe, Anlagen und Einrichtungen sowie Flächen. Schutzwürdig sind diese zum einen, soweit ihr Ausfall die zivile Verteidigungsfähigkeit dauerhaft einschränken würde. Eine Dauerhaftigkeit ist anzunehmen, wenn ein Ausfall nicht nur vorübergehend dazu führen würde, dass eines oder mehrere Schutzziele der Zivilen Verteidigung nicht mehr sichergestellt werden können. Zum anderen besteht eine Schutzwürdigkeit, wenn den zivilen Objekten neben der zivilen auch eine militärische Bedeutung zukommt. Dies wäre beispielsweise der Fall, wenn eine zivil genutzte Brücke im Verteidigungsfall entscheidend für militärische Truppenbewegungen oder Evakuierungen wird und dadurch zwar ein ziviles Objekt bleibt, diesem aber militärische Bedeutung zukommt.

Zu Nummer 2 (§ 9):

Zu Buchstaben a und b (Absatz 1 und 2):

Die bisherigen Regelungen des § 9 Absatz 1 und 2 des Informationsfreiheitsgesetzes (IFG) betreffen nur laufende Gerichtsverfahren und erlauben daher nicht, Informationen wegen eines bevorstehenden Gerichtsverfahrens nicht zugänglich zu machen. Mit der Änderung wird die diesbezüglich bestehende Regelungslücke im Hinblick auf zur unmittelbaren Vorbereitung einer rechtlichen Auseinandersetzung angefertigte Unterlagen geschlossen. Damit wird es den informationspflichtigen Stellen künftig möglich sein, bei noch vor einem Gerichtsverfahren zu entscheidenden Einsichtsanträgen ihre Unterlagen zur rechtlichen Bewertung möglicher Ansprüche zurückzuhalten. Die Formulierung stellt zugleich sicher, dass im vorprozessualen Stadium das Akteneinsichts- oder Aktenauskunftsverweigerungsrecht nur soweit und solange besteht, als durch das vorzeitige Bekanntwerden des Akteneinhalts nachteilige Auswirkungen für das Land Berlin bei der Vorbereitung und Durchfüh-

rung einer gerichtlichen oder außergerichtlichen Geltendmachung oder Abwehr von Ansprüchen unmittelbar und konkret zu befürchten sind. Das Vorliegen dieser Voraussetzungen ist im Einzelfall festzustellen. Die bloße mittelbare und fernliegende Möglichkeit nachteiliger Auswirkungen für das Land Berlin und die bloße abstrakte Möglichkeit einer gerichtlichen oder außergerichtlichen Geltendmachung oder Abwehr von Ansprüchen werden hierfür regelmäßig nicht ausreichen. Der Ausschluss des Rechts auf Akteneinsicht und Aktenauskunft ist zudem auf diejenigen Akten und Aktenbestandteile beschränkt, deren Bekanntwerden nachteilige Auswirkungen für das Land Berlin bei der Vorbereitung und Durchführung einer gerichtlichen oder außergerichtlichen Geltendmachung und Abwehr von Ansprüchen befürchten lassen.

Zu Buchstabe c (Absatz 3):

Zu Nummer 1:

Der neue Absatz 3 Nummer 1 nimmt die Vorgänge der Steuerverwaltung vom Informationsanspruch aus. Dabei sind sämtliche Stadien des Besteuerungsverfahrens von der Festsetzung bis zur Steuervollstreckung erfasst (siehe insoweit zur Parallelnorm des § 5 Nummer 4 Hamburgisches Transparenzgesetz (HmbTG) OVG Hamburg, Urteil vom 17. Dezember 2013, Az.: 3 Bf 236/10).

Absatz 3 Nummer 1 trägt dem § 30 der Abgabenordnung (AO) in der Fassung der Bekanntmachung vom 23. Januar 2025 (BGBl. 2025 I Nr. 24) gewährleisteten Steuergeheimnis Rechnung, dessen Einhaltung durch das allgemeine Persönlichkeitsrecht gemäß Artikel 2 Absatz 1 i.V.m. Artikel 1 Absatz 1 GG geboten ist (siehe hierzu BVerfG, Beschluss vom 06.05.2008 – Az.: 2 BvR 336/07, zitiert nach juris). Vor diesem Hintergrund ist der Gesetzgeber nicht gehalten, den Zugang zu steuerlichen Daten bei Informations- oder Auskunftsansprüchen einer freien Einzelfallabwägung durch die zuständige Behörde zu überantworten (vgl. BVerwG, Urteil vom 29.08.2019 – Az.: 7 C 33.17, zitiert nach juris, Randnummer 17).

Die Ausnahmenvorschrift ist aus verfassungsrechtlichen Gründen (Artikel 31 GG) auch deshalb geboten, weil der Bundesgesetzgeber absichtlich davon abgesehen hat, in der AO ein subjektives Recht auf Akteneinsicht während des laufenden Steuerverfahrens einzuführen, mit der Folge, dass auch der Steuerpflichtige insoweit nur einen Anspruch auf ermessensfehlerfreie Bescheidung seines Antrags auf Akteneinsicht hat (siehe dazu BFHE 202, Seite 231 f.; BFH, NJW-RR 2010, Seite 1160 f.) und weitergehende landesrechtliche Regelungen zum Auskunfts- und Akteneinsichtsrecht nach dem Grundsatz „Bundesrecht bricht Landesrecht“ verdrängt würden (dazu OVG Schleswig, NVwZ 2013, Seite 810 ff.).

Zudem bezweckt die Ausnahme, die Arbeitsfähigkeit der Steuerverwaltung zu schützen (siehe die Gesetzesbegründung zur Parallelnorm des §5 Nummer 4 HmbTG, Hamburgische Bürgerschaft, Drucksache 20/4466, Seite 17). Im Falle der Steuerverwaltung gilt es zu bedenken, dass die dortigen Akten neben den Daten des Steuerpflichtigen regelmäßig Kontrollmaterial, behördeninterne Vermerke und Anweisungen enthalten, deren Offenlegung das behördliche Ermittlungsinteresse beeinträchtigen könnte. So könnten sich beispielsweise Rückschlüsse auf die Kriterien von Plausibilitätskontrollen und Schlüssigkeitsprüfungen ergeben, auf welche der Steuerpflichtige in der Folge sein Steuererklärungsverhalten einstellen könnte. Dies wiegt umso schwerer, als der Auskunftsanspruch nach dem Berliner Informationsfreiheitsgesetz jeder Person unabhängig von einem konkreten berechtigten Interesse zusteht, so dass die Einsichtnahme nicht nur in den jeweils eigenen Steuervorgang möglich wäre, sondern von interessierter Seite (etwa durch Lohnsteuerhilfvereine und Angehörige steuerberatender Berufsgruppen) auch massenhaft Einsicht in Steuerakten genommen werden könnte, was die Gefahr der Entschlüsselung von Stichprobenkontrollen und ähnlichem deutlich erhöhen könnte (siehe zum Vorstehenden auch Maatsch/Schnabel, Kommentar zum Hamburgischen Transparenzgesetz, §5 HmbTG, Randnummer 22).

Hinzu kommt, dass Steuerakten in vielen Fällen außer den Daten des Steuerpflichtigen, der die Einsicht begehrt, auch Personen- und Steuerdaten Dritter beinhalten werden, die nicht selten ein beträchtliches Interesse an der Geheimhaltung auch gegenüber dem Steuerpflichtigen haben werden. Diese Daten im Einzelfall jeweils aussondern zu müssen, würde einen hohen Arbeitsaufwand mit sich bringen, der die Steuerverwaltung bei der Wahrnehmung ihrer sonstigen gesetzlichen Aufgaben behindern würde (so auch Maatsch/Schnabel, Kommentar zum Hamburgischen Transparenzgesetz, §5 HmbTG, Randnummer 23).

Schließlich folgt die Vorschrift der Regelungsabsicht des § 32e AO, mit dem der Bundesgesetzgeber ausdrücklich sicherstellt, dass die Bestimmungen der Verordnung (EU) 2016/679 und der AO zur Reichweite von Informations- und Auskunftsansprüchen der betroffenen Personen über geschützte Daten im Sinne des § 30 Absatz 2 AO nicht durch Informationsfreiheitsgesetze des Bundes oder der Länder umgangen werden können. Auch bei anderweitigen Informationszugangsansprüchen sollen die von der Verordnung (EU) 2016/679 und der AO aufgestellten datenschutzrechtlichen Rahmenbedingungen gelten und die Informationsfreiheitsgesetze des Bundes und der Länder bereichsspezifisch verdrängen (Gesetzesbegründung zu § 32e AO, Bundestagsdrucksache 18/12611).

Zu Nummer 2:

Zu Buchstabe a

Buchstabe a entspricht z. B. § 6 Absatz 4 erster Halbsatz des Akten- und Informationsgesetzes in Brandenburg und § 9 Absatz 3 des Informationsfreiheitsgesetzes des Bundes. Der vom Informationsfreiheitsgesetz verfolgte Zweck der Informationserlangung ist gegenüber einer Antragstellerin oder einem Antragsteller erfüllt, wenn diese oder dieser bereits über die begehrte Information verfügt oder sich diese Information in zumutbarer Weise aus allgemein zugänglichen Quellen beschaffen kann. Diese Vorschrift dient der Funktionsfähigkeit der Verwaltung, wenn die zuständige öffentliche Stelle mit Hinweis auf diese Bestimmung den Antrag ablehnen kann, aber auch grundsätzlich der Beschleunigung und Vereinfachung des Verfahrens.

Zu Buchstabe b und c:

Der weitere Ausnahmetatbestand soll dem besonderen Geheimnis- oder Vertraulichkeitsschutz dienen, da die davon erfassten Informationen wegen des damit verfolgten Schutzzwecks schutzwürdig sind und grundsätzlich nicht offenbart werden müssen. Es wird neben dem Berufs- oder besonderen Amtsgeheimnis insofern an konkret bestehende Vorschriften angeknüpft, die den besonderen Geheimnis- oder Vertraulichkeitsschutz festlegen.

Vergleichbare Regelungen finden sich beispielsweise in § 3 Nummer 4 des Informationsfreiheitsgesetzes des Bundes, in § 6 Absatz 2 Nummer 2 des Hamburgischen Transparenzgesetzes oder § 14 Absatz 1 Satz 2 Nummer 5 des Landestransparenzgesetzes Rheinland-Pfalz.

Zu Buchstabe d:

Diese Bestimmung ist erforderlich, weil bei den Behörden bereits wiederholt Auskunftsersuchen nach dem Berliner Informationsfreiheitsgesetz hinsichtlich der IT-Sicherheitskonzepte oder möglicher Notfallpläne gestellt worden sind. Solche Konzepte zur Erfüllung der vorgegebenen Sicherheitsvorkehrungen des Bundesamtes für Sicherheit in der Informationstechnik können nicht herausgegeben werden, ohne dadurch den sicheren Verwaltungsbetrieb zu gefährden. Eine mögliche Ablehnung, die auf den Ausschlussgrund des § 11 IFG und damit auf eine schwerwiegende Gefährdung des Gemeinwohls durch die Bekanntgabe der Information gestützt wird, birgt ein erhöhtes prozessuales Risiko. Denn für die Annahme dieses Ausschlussgrundes liegen die rechtlichen Hürden hoch, da dieser wie alle Ausnahmegesetze eng auszulegen ist. Da die Anwendung dieses Ablehnungsgrundes nicht ohne Prozessrisiko durchführbar ist, wird zugunsten der Rechtssicherheit und der Rechtsklarheit hier vergleichbar mit der Regelung in § 5 Absatz 1 Nummer 18 des Sächsischen Transparenzgesetzes und in § 14 Absatz 1 Nummer 7 des Landestransparenzgesetzes Rheinland-Pfalz eine gesonderte Regelung geschaffen.

Zu Nummer 3:

Nummer 3 dient dem Schutz der Handlungs- und Funktionsfähigkeit des Staates und damit auch den finanziellen und personellen Ressourcen von Behörden und Einrichtungen des Landes Berlin. Die Bestimmung korrespondiert etwa mit § 6 Absatz 4 zweiter Halbsatz des Akten- und Informationszugangsgesetzes in Brandenburg sowie § 14 Absatz 1 Satz 2 Nummer 12 des Landestransparenzgesetzes Rheinland-Pfalz. Ein Missbrauch des Informationsfreiheitsrechts liegt daher beispielsweise vor, wenn durch überbordende Anfragen die Kapazitäten einer informationspflichtigen Stelle gebunden werden sollen. Dies ist beispielsweise der Fall, wenn die Antragstellerin oder der Antragsteller oder mehrere antragstellende Personen einzeln oder koordiniert umfangreiche oder zahlreiche Anfragen stellen, um die staatliche Verwaltung oder die Sicherheitsbehörden an der Erfüllung ihrer sonstigen Aufgaben zu hindern. Auf einen Missbrauch kann in diesem Zusammenhang geschlossen werden, wenn sich aus der Gesamtschau der Umstände des Einzelfalls ergibt, dass die Antragstellung überwiegend erfolgt, um die behördliche Arbeitskraft zu binden. In Rede stehen querulatorische Informationsbegehren, deren Interesse erkennbar nicht auf die Erlangung der Information als solche gerichtet ist, sondern die offensichtlich auf gesetzesferne Ziele (zum Beispiel „Blockierung“ der Verwaltung) gerichtet sind.

Zu Artikel 3 (Änderung des Bäder-Anstaltsgesetzes):

Zu Nummer 1 (§ 23):

Satz 2 zählt beispielhaft Aufgaben auf, zu deren Erfüllung die Verarbeitung personenbezogener Daten erforderlich ist und konkretisiert dabei den Anwendungsbereich.

Zu Nummer 1:

Mit der Änderung der Tarifsatzung 2025 wurden verschiedene neue Tarifmodelle und Kartenarten eingeführt, deren Gültigkeit einer Kontrolle bedarf, welche personenbezogene Daten miteinschließt.

Dabei handelt es sich u. a. um die personalisierten Online-Tickets, die für den Eintritt in die Freibäder für ein ausgewähltes Zeitfenster erworben werden können, personalisierte Abonnement-Mitgliedschaften, die Badekarte im Ferienpass und Eintrittskarten für spezielle Aktionstarife.

Ebenso sind bei der Inanspruchnahme von Ermäßigungen die Nachweise wie Schwerbehindertenausweis, Ferienpass, Schülerausweis I und II, Studierendenausweis, Ausbildungsbescheinigung, Ehrenamtskarte, Nachweis für den Empfang von Sozialhilfe, Leistungen zur Grundsicherung im Alter, bei Erwerbsminderungen oder nach dem Asylbewerberleistungsgesetz beim Erwerb oder beim Einlass zu kontrollieren. Sofern die genannten Ausweise und Bescheinigungen nicht mit einem Lichtbild versehen sind, kann die Vorlage des Personalausweises verlangt werden.

Zu Nummer 2:

Darüber hinaus besteht beim Einlass in die Bäder die Berechtigung zur Sichtkontrolle, dass Identitätsnachweise mitgeführt werden (Ausweiskontrolle), soweit dies zur Gewährleistung des oder Wiederherstellung eines sicheren Badbetriebes erforderlich ist.

Infolge von wiederholten Gewaltvorfällen in der Sommerbadesaison 2023, insbesondere Gewaltvorkommnisse, die zu Badräumungen und -schließungen geführt haben, wurde die Arbeitsgruppe Sicherheit in Freibädern, u. a. bestehend aus Vertreterinnen und Vertretern der Senatsverwaltung für Inneres und Sport, der Polizei Berlin, der Berliner Bäder-Betriebe und der Senatsverwaltung für Bildung, Jugend und Familie gegründet. Unter der Federführung der Senatsverwaltung für Inneres und Sport erarbeitete die Arbeitsgruppe Sicherheit in Freibädern einen ganzheitlichen Maßnahmenkatalog aus Service, Prävention und Sicherheit zur Bewältigung der Lage.

Der Maßnahmenkatalog umfasst neben einer Reihe von Maßnahmen u. a. die Maßgabe, dass ein Einlass in die Sommerbäder nur erfolgt, wenn ein Identitätsnachweis mitgeführt wird (Ausweiskontrolle). Die Maßnahmen haben sich in Evaluationsrunden als erfolgreich erwiesen und dazu beigetragen, dass die Sommerbadesaison 2024 im Wesentlichen ohne Gewaltvorfälle verlief, was sich in der Gesamtstatistik (u. a. Badschließungen, Hausverbote, Polizeieinsätze) widerspiegelt.

Mit dem neuen Satz 2 wird klargestellt, dass eine Verarbeitung personenbezogener Daten zulässig ist, um sicherzustellen, dass bei einem Besuch im Sommer- oder Hallenbad ein Identitätsnachweis mitgeführt wird.

Die Sichtkontrolle, ob beim Eintritt in ein Bad ein Identitätsnachweis mitgeführt wird, berührt Datenschutzinteressen der Badegäste nur geringfügig, da bei einer Sichtkontrolle nur das Vorhandensein eines Identitätsnachweises überprüft wird. Auch findet im Anschluss an die Sichtung keine weitere Verarbeitung, insbesondere Speicherung, statt.

Im Gegenzug stärkt das Mitführen eines Identitätsnachweises die Sicherheit von Mitarbeitenden bzw. Besuchenden der Bäder, da im Fall von Gewalt- oder anderen Sicherheitsvorfällen die Wahrscheinlichkeit der Identifizierung der Tatverdächtigen sehr hoch ist. Darüber hinaus hat dies bereits einen präventiven abschreckenden Einfluss auf ggf. gewaltbereite Personen, die die Bäder aufsuchen.

Zu Nummer 3:

Das Mitführen eines Identitätsnachweises beim Besuch der Bäder ermöglicht es auch, anlassbezogen personenbezogene Hausverbote zu erteilen und durchzusetzen. Bei Verdacht eines zuvor erteilten Hausverbotes bzw. möglichem Wiedererkennen einer Person, der Hausverbot erteilt wurde, kann beim Einlass die Identität geprüft, ein Abgleich mit der Hausverbotsliste vorgenommen und dann ggf. der Zugang zum Bad verwehrt werden.

Zu Nummer 2 (§ 24 neu):

Absatz 1 zählt abschließend Zwecke auf, zu deren Erfüllung die Verarbeitung personenbezogener Daten mit Hilfe von Videoüberwachung zulässig ist.

Zu Nummer 1:

Im Zusammenhang mit der Kontrolle von Zugangsberechtigungen können Videoaufnahmen, insbesondere der Eingangsbereiche der Bäder, erforderlich sein, um unberechtigten Zutritten, wie beispielsweise dem Übersteigen der Drehkreuze, zu begegnen.

Zu Nummern 2 und 3:

Die Videoüberwachung der Bäder ist darüber hinaus erforderlich, um die Sicherheit von Mitarbeitenden bzw. Besuchenden der Bäder zu erhöhen, da im Fall von Gewalt- oder anderen Sicherheitsvorfällen in den Eingangsbereichen oder im Bad die Wahrscheinlichkeit der Identifizierung der Tatverdächtigen mit Hilfe der Aufnahmen sehr hoch ist. Dies hat auch bereits einen präventiven abschreckenden Einfluss auf ggf. gewaltbereite Personen, die die Bäder aufsuchen.

Der Maßnahmenkatalog der Arbeitsgruppe Sicherheit in Freibädern umfasste auch die Videoüberwachung im Eingangsbereich von fünf Sommerbädern. Die Maßnahmen haben sich insgesamt als erfolgreich erwiesen und dazu beigetragen, dass die Sommerbadesaison 2024 im Wesentlichen ohne Gewaltvorfälle verlief, was sich in der Gesamtstatistik (u. a. Badschließungen, Hausverbote, Polizeieinsätze) widerspiegelt.

Zu Nummer 4:

Zudem wird sichergestellt, dass Videoüberwachung zur Verhütung von Straftaten gegen das Eigentum bzw. Vermögen der Anstalt (Einbruchschutz, Zäune etc.) oder zu Lasten von Badegästen (z. B. Videoüberwachung der Schließfächer) eingesetzt werden kann. Der Aufnahmewinkel beschränkt sich dabei auf die Bereiche der Bäder, in denen Badegäste nicht in ihrer Intimsphäre betroffen sind.

Durch den Verweis auf § 20 Absatz 2, 3, und 5 BlnDSG wird sichergestellt, dass den Anforderungen an die Kennzeichnungspflicht und die unverzügliche Löschung Rechnung getragen wird und eine weitere Verarbeitung für Zwecke der Abwehr von Gefahren für die öffentliche Sicherheit oder zur Verfolgung von Straftaten gewährleistet bleibt.

Zu Nummer 3 (§ 25 neu):

Es handelt sich um eine redaktionelle Folgeänderung aus der Nummer 2.

Zu Artikel 4 (Änderung § 6 Absatz 2 Verwaltungsverfahrensgesetz):

Die Änderung des Absatzes 2 durch Aufnahme eines neuen Satz 1 und Satz 2 ist im Hinblick auf eine veränderte Sicherheitslage und in Reaktion auf mehrere Anschläge auf die Elektrizitätsversorgung notwendig. Kritische Infrastrukturen sind nach der Definition in § 28 Absatz 1 Katastrophenschutzgesetz „Einrichtungen, Anlagen oder Teile davon, die den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Entsorgung, Gesundheit, Wasser, Ernährung, Medien und Kultur oder Finanz- und Versicherungswesen angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden“. Die Regelung bezieht sich auch auf staatliche Einrichtungen der kritischen Infrastruktur, die Einrichtungen nach § 28 Absatz 1 Katastrophenschutzgesetz entsprechen, und auf zur Aufrechterhaltung der Staats- und Regierungsfunktionen unabdingbar notwendige Einrichtungen, die einen mit Einrichtungen nach § 28 Absatz 1 Katastrophenschutzgesetz vergleichbaren Schutzbedarf aufweisen, weil diese gleichermaßen schutzbedürftig sind. Davon können insbesondere einzelne Einrichtungen der Sicherheitsbehörden und der Justiz betroffen sein.

Die Zivile Verteidigungsfähigkeit beschreibt die Fähigkeit eines Staates, im äußeren Notstand den Zivilschutz, die Aufrechterhaltung der Staats- und Regierungsfunktionen, die Versorgung der Bevölkerung und der Streitkräfte sowie die Unterstützung der Streitkräfte sicherzustellen. Die Zivile Verteidigung fußt dabei auf den Vorsorgemaßnahmen des Katastrophenschutzes und dem Krisenmanagement der Länder. Gemeinsam mit der militärischen Verteidigung bildet sie das Fundament einer effektiven Gesamtverteidigung. Sie ist hierbei kein nachgelagerter Aspekt, sondern eine unverzichtbare Voraussetzung für das Funktionieren einer gesamtstaatlichen Sicherheitsvorsorge. Zivile Objekte sind zunächst alle nicht militärisch genutzten Gebäude und Gebäudekomplexe, Anlagen und Einrichtungen sowie Flächen. Schutzwürdig sind diese zum einen, soweit ihr Ausfall die zivile Verteidigungsfähigkeit dauerhaft einschränken würde. Eine Dauerhaftigkeit ist anzunehmen, wenn ein Ausfall nicht nur vorübergehend dazu führen würde, dass eines oder mehrere Schutzziele der Zivilen Verteidigung nicht mehr sichergestellt werden können. Zum anderen besteht eine Schutzwürdigkeit, wenn den zivilen Objekten neben der zivilen auch eine militärische Bedeutung zukommt. Dies ist beispielsweise der Fall, wenn eine zivil genutzte Brücke im Verteidigungsfall entscheidend für militärische Truppenbewegungen oder Evakuierungen wird und dadurch zwar ein ziviles Objekt bleibt, diesem aber militärische Bedeutung zukommt.

Durch die Verwendung des Wortes „soweit“ im neuen Absatz 2 Satz 1, wird klargestellt, dass die Gestattung der Akteneinsicht durch die Behörde nur in dem Umfang verweigert

werden darf, wie dies zur Wahrung des Staatswohls zwingend notwendig ist. Die Versagung der Akteneinsicht kann sich insbesondere auch auf einzelne Aktenbestandteile beschränken (Unkenntlichmachung einzelner Aktenbestandteile). Die Neuregelung in Absatz 2 Satz 2 begründet eine im konkreten Einzelfall widerlegbare Regelvermutung. Die Behörde hat ihre Entscheidung nach pflichtgemäßem Ermessen unter umfassender Berücksichtigung aller Umstände des konkreten Einzelfalls sowie sorgfältiger Abwägung der widerstreitenden Interessen nach dem Grundsatz der Verhältnismäßigkeit zu treffen.

Zu Artikel 5 (Änderung § 17 Absatz 4 ASOG)

Mehrere Angriffe auf Anlagen der Elektrizitätsversorgung oder andere kritische Anlagen in den vergangenen Monaten haben deutlich gemacht, dass derartige Taten das öffentliche Leben schwerwiegend und länger andauernd beeinträchtigen können, Leib und Leben einer Vielzahl vulnerabler Personen gefährden und damit geeignet sind, in der Folge auch den demokratischen Rechtsstaat zu destabilisieren.

Zur wirksamen Verhütung solcher schwerwiegenden Taten ist die Polizei auch auf Maßnahmen angewiesen, die einen erheblichen Eingriff in die Grundrechte der Betroffenen darstellen können und damit teilweise der Verhütung von Straftaten von erheblicher Bedeutung vorbehalten sind. Dies betrifft unter anderem Maßnahmen gemäß § 25 (Datenerhebung durch längerfristige Observation), § 25b (Datenerhebung durch den verdeckten Einsatz technischer Mittel außerhalb von Wohnungen) und § 25c ASOG (Datenerhebung durch den Einsatz verdeckter Ermittler oder von Vertrauenspersonen). Ohne die Möglichkeit, gegebenenfalls auch derartige Maßnahmen zu ergreifen, ist eine wirksame Straftatenverhütung insbesondere gegenüber hoch professionell arbeitenden und streng abgeschotteten Tätergruppen erheblich erschwert oder sogar unmöglich.

Die Strafbarkeit solcher Angriffe kann sich beispielsweise aus den §§ 316b, 317 und 318 StGB ergeben, die für sich genommen noch nicht zu den Straftaten erheblicher Bedeutung im Sinne des § 17 Abs. 3 Nr. 1 ASOG zählen. Kritische Infrastrukturen sind nach der Definition in § 28 Absatz 1 Katastrophenschutzgesetz „Einrichtungen, Anlagen oder Teile davon, die den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Entsorgung, Gesundheit, Wasser, Ernährung, Medien und Kultur oder Finanz- und Versicherungswesen angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden“. Die Regelung bezieht sich auch auf staatliche Einrichtungen der kritischen Infrastruktur, die Einrichtungen nach § 28 Absatz 1 Katastrophenschutzgesetz entsprechen, und auf zur

Aufrechterhaltung der Staats- und Regierungsfunktionen unabdingbar notwendige Einrichtungen, die einen mit Einrichtungen nach § 28 Absatz 1 Katastrophenschutzgesetz vergleichbaren Schutzbedarf aufweisen, weil diese gleichermaßen schutzbedürftig sind. Davon können insbesondere einzelne Einrichtungen der Sicherheitsbehörden und der Justiz betroffen sein. Durch die Formulierung „Straftaten, die sich auf eine [...] Beeinträchtigung der Funktionsfähigkeit von Einrichtungen, Anlagen oder Teilen davon [...], von staatlichen Einrichtungen der kritischen Infrastruktur, die Einrichtungen nach § 28 Absatz 1 Katastrophenschutzgesetz entsprechen, oder von zur Aufrechterhaltung der Staats- und Regierungsfunktionen unabdingbar notwendigen Einrichtungen, die einen mit Einrichtungen nach § 28 Absatz 1 Katastrophenschutzgesetz vergleichbaren Schutzbedarf aufweisen, [...] beziehen“ wird zum Ausdruck gebracht, dass gegen die kritische Infrastruktur gerichtete Straftaten mit einer geringen Strafandrohung (z. B.: Sachbeschädigung durch das Auftragen von Graffiti o. ä.) nicht genügen, um eine Ergreifung der genannten polizeilichen Maßnahmen zu rechtfertigen. Zudem bewirkt die in § 17 Abs. 4 ASOG geforderte Eignung zur Beeinträchtigung der Sicherheit der Bevölkerung – für deren Auslegung bezogen auf Straftaten gegen kritische Versorgungsanlagen im Wesentlichen die Auslegung des § 316b Abs. 3 StGB (z. B. Stoll in: v. Heintschel-Heinegg/Kudlich, BeckOK StGB, 67. Ed. Stand: 01.11.2025, § 316b Rn. 15 m. w. N.) herangezogen werden kann – eine Beschränkung präventiv-polizeilicher Befugnisse auf die Verhütung von Straftaten von größter Gefährlichkeit.

Im Übrigen handelt es sich um die Korrektur eines redaktionellen Fehlers.

Zu Artikel 6 (Änderung § 5 Open Data Verordnung).

Die Ergänzung des § 5 Absatz 1 Nummer 1 ist im Hinblick auf eine veränderte Sicherheitslage und in Reaktion auf mehrere Anschläge auf die Elektrizitätsversorgung notwendig. Wegen der Bedeutung der Stärkung der Resilienz kritischer Infrastrukturen und bestimmter ziviler Objekte ist es notwendig, hier eine Ausnahme gleichlautend zu der im Berliner Informationsfreiheitsgesetz eingefügten Ausnahme einzuführen. Die Änderung der Rechtsverordnung durch den Gesetzgeber ist im Zusammenhang mit der Änderung des zum selben Sachbereich gehörenden Berliner Informationsfreiheitsgesetzes erforderlich.

Kritische Infrastrukturen sind nach der Definition in § 28 Absatz 1 Katastrophenschutzgesetz „Einrichtungen, Anlagen oder Teile davon, die den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Entsorgung, Gesundheit, Wasser, Ernährung, Medien und Kultur oder Finanz- und Versicherungswesen angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall

oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden“. Die Ausnahme bezieht sich auch auf Informationen, die für die Funktionsfähigkeit von staatlichen Einrichtungen der kritischen Infrastruktur, die Einrichtungen nach § 28 Absatz 1 Katastrophenschutzgesetz entsprechen, oder von zur Aufrechterhaltung der Staats- und Regierungsfunktionen unabdingbar notwendigen Einrichtungen, die einen mit Einrichtungen nach § 28 Absatz 1 Katastrophenschutzgesetz vergleichbaren Schutzbedarf aufweisen, von Bedeutung sind, weil diese gleichermaßen schutzbedürftig sind. Davon können insbesondere einzelne Einrichtungen der Sicherheitsbehörden und der Justiz betroffen sein.

Die Zivile Verteidigungsfähigkeit beschreibt die Fähigkeit eines Staates, im äußeren Notstand den Zivilschutz, die Aufrechterhaltung der Staats- und Regierungsfunktionen, die Versorgung der Bevölkerung und der Streitkräfte sowie die Unterstützung der Streitkräfte sicherzustellen. Die Zivile Verteidigung fußt dabei auf den Vorsorgemaßnahmen des Katastrophenschutzes und dem Krisenmanagement der Länder. Gemeinsam mit der militärischen Verteidigung bildet sie das Fundament einer effektiven Gesamtverteidigung. Sie ist hierbei kein nachgelagerter Aspekt, sondern eine unverzichtbare Voraussetzung für das Funktionieren einer gesamtstaatlichen Sicherheitsvorsorge. Zivile Objekte sind zunächst alle nicht militärisch genutzten Gebäude und Gebäudekomplexe, Anlagen und Einrichtungen sowie Flächen. Schutzwürdig sind diese zum einen, soweit ihr Ausfall die zivile Verteidigungsfähigkeit dauerhaft einschränken würde. Eine Dauerhaftigkeit ist anzunehmen, wenn ein Ausfall nicht nur vorübergehend dazu führen würde, dass eines oder mehrere Schutzziele der Zivilen Verteidigung nicht mehr sichergestellt werden können. Zum anderen besteht eine Schutzwürdigkeit, wenn den zivilen Objekten neben der zivilen auch eine militärische Bedeutung zukommt. Dies wäre beispielsweise der Fall, wenn eine zivil genutzte Brücke im Verteidigungsfall entscheidend für militärische Truppenbewegungen oder Evakuierungen wird und dadurch zwar ein ziviles Objekt bleibt, diesem aber militärische Bedeutung zukommt.

Zu Artikel 7:

Der Artikel regelt das Inkrafttreten des Gesetzes

c) Beteiligungen:

Dem Land Brandenburg wurde im Rahmen der frühzeitigen Verwaltungsbeteiligung die Gelegenheit zur Stellungnahme eingeräumt. Das Land Brandenburg hat von einer Stellungnahme abgesehen.

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI) wurde gemäß § 11 Absatz 2 Satz 2 des Berliner Datenschutzgesetzes angehört. Sie hat im Wesentlichen Kritik daran geübt, dass die Regelungen des Berliner Informationsfreiheitsgesetzes (IFG) zur Akteneinsicht und -auskunft mit dem vorliegenden Gesetzentwurf weiter eingeschränkt werden sollen, obwohl die Richtlinien der Regierungspolitik vorsähen, die hohen Standards des IFG zu erhalten und im Übrigen das IFG zu einem Transparenzgesetz ausgebaut werden solle. Weiterhin sah sie keinen Anlass für die mit dem Gesetzentwurf vorgesehene Ausnahme vom Akteneinsichts- und -auskunftsrecht nach dem IFG für Vorgänge der Steuerverwaltung sowie für die mit dem Gesetzentwurf vorgesehene Einschränkung des Akteneinsichts- und -auskunftsrechts nach dem IFG wegen Geheimhaltungs- und Vertraulichkeitsvorschriften. Zudem hat sie auf die Gefahr eines ausufernden Gebrauchs der mit dem Gesetzentwurf vorgesehenen, das Akteneinsichts- und -auskunftsrecht nach dem IFG einschränkenden Missbrauchsklausel aufmerksam gemacht.

Hinsichtlich der beabsichtigten Regelungen zur Stärkung der Resilienz der KRITIS im vorliegenden Gesetzentwurf hat die BlnBDI im Wesentlichen mitgeteilt, dass sie diese Regelungen grundsätzlich nicht für erforderlich hält, da bereits die bestehenden gesetzlichen Vorschriften im Rahmen der jeweiligen Einzelfallabwägung das angestrebte Ergebnis zuließen. Die Regelungen seien nicht geeignet, das angestrebte Ziel zu erreichen. Im Einzelnen merkt sie zur Aufnahme der Regelvermutung in § 20 Absatz 1 BlnDSG an, dass dies in aller Regel bereits jetzt Ergebnis der Abwägung sein dürfte und weiterhin eine Erforderlichkeitsprüfung notwendig ist.

Weiterhin stellt die BlnBDI klar, dass die beabsichtigte Ausnahme von der Kennzeichnungspflicht in § 20 Absatz 2 BlnDSG nicht auf Artikel 23 Absatz 1 Buchstabe d der Verordnung (EU) 2016/679 gestützt werden könne, da hier eine konkrete Gefahr vorausgesetzt werde. Sie merkt zusätzlich an, dass „öffentliche Sicherheit“ i. S. d. Artikel 23 Absatz 1 Buchstabe c der Verordnung (EU) 2016/679 europarechtlich auszulegen sei und im Wesentlichen den Schutz von Menschenleben meine. Im Übrigen genüge die beabsichtigte Regelung nicht den Anforderungen des Artikel 23 Absatz 2 der Verordnung (EU) 2016/679. Die BlnBDI weist darauf hin, dass der Verzicht auf die Erteilung datenschutzrechtlicher Informationen zu einer sog. heimlichen oder verdeckten Videoüberwachung führe und auch der Europäische Gerichtshof ausgeführt habe, dass eine solche Videoüberwachung unvereinbar mit dem Zweck der Verordnung (EU) 2016/679 sei, ein hohes Niveau des Schutzes der Grundfreiheiten und der Grundrechte natürlicher Personen zu gewährleisten (EuGH, Urteil vom 18. Dezember 2025, C-422/24, Rn. 41).

Hinsichtlich der beabsichtigten einschränkenden Regelungen zur Informationsfreiheit merkt die BlnBDI an, dass es aus ihrer Sicht nicht nachvollziehbar sei, dass die Informationsfreiheit in der öffentlichen Diskussion undifferenziert und pauschal als Sicherheitsrisiko

dargestellt werde, ohne auch ihre Bedeutung für den Rechtsstaat und die Demokratie zu erwähnen. Auch hier ließe eine Einzelfallabwägung im Rahmen der bestehenden gesetzlichen Regelungen das gewünschte Ergebnis bereits zu.

Auch für die beabsichtigten Änderungen der Open Data-Verordnung und des Verwaltungsverfahrensgesetzes gelte, dass wegen der dort jeweils bereits enthaltenen Verweise auf die Ausschlussgründe des Informationsfreiheitsgesetzes diese Regelungen nicht notwendig seien.

Hinsichtlich der beabsichtigten Änderung im ASOG teilt die BlnBDI mit, dass die Regelung möglichst restriktiv formuliert werden sollte, um auch im Gesetzeswortlaut klarzustellen, dass ausschließlich Straftaten von größter Gefährlichkeit erfasst sein sollen.

Im Übrigen hat sich die BlnBDI weiteres Vorbringen im parlamentarischen Verfahren vorbehalten.

Der Senat kann die Bedenken der Berliner Beauftragten für Datenschutz und Informationsfreiheit nachvollziehen, das IFG wird deshalb nur punktuell geändert. Die vorgeschlagenen Ausweitungen der Versagungsgründe sind sachlich und fachlich gerechtfertigt, z. B. um einer Herausgabe von nach dem Berliner Sicherheitsüberprüfungsgesetz eingestuftten Vorgängen besser begegnen zu können. Weiterhin ist die Ausnahme für Vorgänge der Steuerverwaltung gerechtfertigt und eine nur auf die Vorschriften der Abgabenordnung gestützte Verweigerung der Akteneinsicht oder -auskunft nach dem IFG begegnet aus Sicht des Senats prozessualen Risiken. Den Bedenken der BlnBDI wurde jedoch – auch hinsichtlich der beanstandeten Missbrauchsklausel – mit einer Überarbeitung der Formulierungen in Artikel 2 Nummer 2 (zu § 9 Absatz 3 IFG) des vorliegenden Gesetzentwurfs entgegengekommen. Hinsichtlich der Anmerkungen der BlnBDI zur Aufnahme der Regelvermutung in § 20 Absatz 1 BlnDSG (Artikel 1 Nummer 5 Buchstabe a)) stimmt der Senat dahingehend zu, dass die Erforderlichkeit weiterhin geprüft werden muss, die Erforderlichkeit des Schutzes auch nach räumlichen Kriterien zu prüfen ist und dem Grundsatz der Verhältnismäßigkeit genügen muss. Die Regelvermutung erleichtert lediglich den Begründungsaufwand für die Betreiberinnen und Betreiber der Einrichtungen und Anlagen Kritischer Infrastruktur. Dies wird bereits in der Begründung ausgeführt.

Aufgrund der Anmerkungen der BlnBDI zu Artikel 1 Nummer 5 Buchstabe b) (§ 20 Absatz 2 BlnDSG) wurde der Hinweis auf Artikel 23 Absatz 1 Buchstabe d der Verordnung (EU) 2016/679 aus der Begründung gestrichen. In der Begründung für die beabsichtigte Regelung wird bereits darauf eingegangen, dass die beabsichtigte Änderung gerade auch auf den Schutz von Menschenleben abzielt, da Ausfälle der entsprechenden Infrastruktureinrichtungen insbesondere mit Gefahren für Leib und Leben einer Vielzahl von betroffenen Personen u.a. in Krankenhäusern und Pflegeeinrichtungen einhergehen können. Zur Anmerkung der BlnBDI, die beabsichtigte Regelung genüge nicht den Anforderungen des Artikel 23 Absatz 2 der Verordnung (EU) 2016/679, führt der Senat aus, dass Regelungen hin-

sichtlich möglicher zweckändernder Verarbeitungen und zur Löschung der personenbezogenen Daten bereits in den bislang geltenden Regelungen des § 20 Absatz 3 und 5 BlnDSG enthalten sind. Ein Verweis auf Regelungen des § 23 Absatz 2 BlnDSG wurde aufgrund der Kritik der BlnBDI in den Gesetzentwurf eingefügt. Weitergehende Regelungen u. a. zur Befristung der zulässigen Verarbeitung der personenbezogenen Daten sind aus Sicht des Senats nicht angezeigt: Nach dem Regelungstext ist es notwendig, dass durch eine Kennzeichnung der erforderliche Schutz der genannten Einrichtungen beeinträchtigt ist. Sollte diese Voraussetzung, etwa durch eine Änderung der örtlichen Gegebenheiten, entfallen, wären damit auch die tatbestandlichen Voraussetzungen für das Absehen von der Kennzeichnungspflicht nicht mehr erfüllt. Hinsichtlich der von der BlnBDI angeführten Entscheidung des Europäischen Gerichtshof zur verdeckten Videoüberwachung (EuGH, Urteil vom 18. Dezember 2025, C-422/24, Rn. 41) verweist der Senat darauf, dass die zitierte Entscheidung die Erhebung personenbezogener Daten durch eine von Fahrkartenkontrolleuren im öffentlichen Personenverkehr getragene Körperkamera und die damit verbundene Fragestellung, ob zum Zeitpunkt der Datenerhebung auf diese hingewiesen werden müsse, betraf. Damit ist die EuGH-Entscheidung bereits im Ausgangspunkt nicht mit dem hier in Rede stehenden, mit einer Videoüberwachung bezweckten Schutz von Einrichtungen der Kritischen Infrastruktur vergleichbar. Ein generelles Verbot verdeckter Videoüberwachung lässt sich der EuGH-Entscheidung – insbesondere für Fallkonstellationen, in denen es um die Abwendung konkreter Gefährdung für Leib und Leben geht – nicht entnehmen.

Zu den Ausführungen der BlnBDI zum Informationsfreiheitsgesetz teilt der Senat mit, dass die Regelungen bewusst nicht in die Ausschlussgründe aufgenommen wurden, da damit eine behördliche, mit prozeduralen Pflichten versehene Einzelfallprüfung etwaiger Verweigerungsgründe einher gegangen wäre. Die beabsichtigte Regelung ist nun vergleichbar mit der für den Verfassungsschutz geltenden Bereichsausnahme in § 32 Abs. 3 Verfassungsschutzgesetz Berlin. Die Änderungen der Open Data-Verordnung und des Verwaltungsverfahrensgesetzes sind aus Sicht des Senats aus Klarstellungsgründen notwendig, da die Einrichtungen der KRITIS, die Objekte der zivilen Verteidigungsfähigkeit und die weiteren von den Regelungen betroffenen Einrichtungen nunmehr vom Geltungsbereich des Informationsfreiheitsgesetzes ausgenommen werden sollen. Hinsichtlich der Verweise auf die Ausschlussgründe des Informationsfreiheitsgesetzes in der Open Data-Verordnung und dem Verwaltungsverfahrensgesetz sollte keine Rechtsunsicherheit entstehen.

Hinsichtlich der Kritik der BlnBDI zur beabsichtigten Änderung des § 17 Absatz 4 ASOG (Artikel 5) werden die Bedenken der BlnBDI nicht geteilt. Die aktuelle Fassung ist ausreichend restriktiv und es ergibt sich mit hinreichender Klarheit, dass ausschließlich Straftaten von größter Gefährlichkeit erfasst werden sollen.

Dem Rat der Bürgermeister hat die Vorlage gemäß § 29 Absatz 1 Landesorganisationsgesetz vorgelegen. Er hat sich mit ihrem Inhalt einverstanden erklärt.

B. Rechtsgrundlage:

Artikel 59 Absatz 2 der Verfassung von Berlin

C. Gesamtkosten:

Keine.

D. Auswirkungen auf die Gleichstellung der Geschlechter:

Die Regelungen wirken sich gleichermaßen auf alle Geschlechter aus.

E. Kostenauswirkungen auf Privathaushalte und/oder Wirtschaftsunternehmen:

Keine.

F. Auswirkungen auf die Zusammenarbeit mit dem Land Brandenburg:

Keine.

G. Auswirkungen auf den Klimaschutz und die Umwelt:

Keine.

H. Auswirkungen auf das elektronische Verwaltungshandeln:

Keine.

I. Auswirkungen auf den Haushaltsplan und die Finanzplanung:

a) Auswirkungen auf Einnahmen und Ausgaben:

Keine.

b) Personalwirtschaftliche Auswirkungen:

Keine.

J. Flächenmäßige Auswirkungen:

Keine.

Berlin, den 24. Februar 2026

Der Senat von Berlin

Franziska Giffey

.....
Bürgermeisterin

Iris Spranger

.....
Senatorin für Inneres und Sport

I. Gegenüberstellung der Gesetzestexte

Alte Fassung	Neue Fassung
<u>Berliner Datenschutzgesetz</u>	
§ 1 Zweck (1) [...] (2) Darüber hinaus erfolgt in den Teilen 1 und 3 dieses Gesetzes die Umsetzung der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 199 vom 4.5.2016, S. 89; L 127 vom 23.5.2018, S. 9). (3) [...].	§ 1 Zweck (1) [...] (2) Darüber hinaus erfolgt in den Teilen 1 und 3 dieses Gesetzes die Umsetzung der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4.5.2016, S. 89; L 127 vom 23.5.2018, S. 9). (3) [...].
§ 11 Aufgaben (1) Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat unbeschadet anderer in der Verordnung (EU) 2016/679 genannten Aufgaben die Aufgaben, 1. die Anwendung dieses Gesetzes und sonstiger Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften, zu überwachen und durchzusetzen, [...]	§ 11 Aufgaben (1) Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat unbeschadet anderer in der Verordnung (EU) 2016/679 genannten Aufgaben die Aufgaben, 1. die Anwendung dieses Gesetzes und sonstiger Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften sowie der §§ 19, 20 und 25 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982; 2022 I S. 1045), das zuletzt durch Artikel 10 des Gesetzes vom 9. Januar 2026 (BGBl. 2026 I Nr. 7) geändert worden ist, in der jeweils geltenden Fassung zu überwachen und durchzusetzen, [...]

§ 13 Befugnisse [...]	§ 13 Befugnisse [...] (9) Im Hinblick auf die Befugnisse der oder des Berliner Beauftragten für Datenschutz und Informationsfreiheit im Rahmen ihrer oder seiner Aufsichtstätigkeit über die Einhaltung der Bestimmungen der §§ 19, 20 und 25 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes findet Artikel 58 der Verordnung (EU) 2016/679 entsprechende Anwendung.
§ 19 Verarbeitung personenbezogener Daten zu Zwecken der freien Meinungsäußerung und der Informationsfreiheit (1) Soweit personenbezogene Daten in Ausübung des Rechts auf freie Meinungsäußerung und Informationsfreiheit zu journalistischen, künstlerischen oder literarischen Zwecken, einschließlich der rechtmäßigen Verarbeitung auf Grund der §§ 22 und 23 des Gesetzes betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie in der im Bundesgesetzblatt Teil III, Gliederungsnummer 440-3, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 3 § 31 des Gesetzes vom 16. Februar 2001 (BGBl. I S. 266) geändert worden ist, verarbeitet werden, gelten von Kapitel II bis VII sowie IX der Verordnung (EU) 2016/679 nur Artikel 5 Absatz 1 Buchstabe f sowie Artikel 24 und 32. Artikel 82 der Verordnung (EU) 2016/679 gilt mit der Maßgabe, dass die Haftung nur Schäden umfasst, die durch eine Verletzung des Datengeheimnisses oder durch unzureichende technische oder organisatorische Maßnahmen im Sinne des Artikels 5 Absatz 1 Buchstabe f der Verordnung (EU) 2016/679 eintreten. [...]	§ 19 Verarbeitung personenbezogener Daten zu Zwecken der freien Meinungsäußerung und der Informationsfreiheit (1) Soweit personenbezogene Daten in Ausübung des Rechts auf freie Meinungsäußerung und Informationsfreiheit zu journalistischen, künstlerischen oder literarischen Zwecken, einschließlich der rechtmäßigen Verarbeitung auf Grund der §§ 22 und 23 des Gesetzes betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie in der im Bundesgesetzblatt Teil III, Gliederungsnummer 440-3, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 3 § 31 des Gesetzes vom 16. Februar 2001 (BGBl. I S. 266) geändert worden ist, verarbeitet werden, gelten von Kapitel II bis VII sowie IX der Verordnung (EU) 2016/679 nur Artikel 5 Absatz 1 Buchstabe f sowie Artikel 24 und 32. Artikel 82 der Verordnung (EU) 2016/679 gilt mit der Maßgabe, dass die Haftung nur Schäden umfasst, die durch eine Verletzung des Datengeheimnisses oder durch unzureichende technische oder organisatorische Maßnahmen im Sinne des Artikels 5 Absatz 1 Buchstabe f der Verordnung (EU) 2016/679 eintreten. [...]
§ 20 Videoüberwachung (1) Die Verarbeitung personenbezogener Daten in öffentlich zugänglichen Räumen mit Hilfe optisch-elektronischer Einrichtungen (Videoüberwachung) ist zulässig, soweit sie zur Erfüllung einer im öffentli-	§ 20 Videoüberwachung (1) Die Beobachtung öffentlich zugänglicher Räume mit Hilfe optisch-elektronischer Einrichtungen (Videoüberwachung) sowie die Verarbeitung der dadurch erhobenen personenbezogenen Da-

chen Interesse liegenden Aufgabe oder zur Wahrnehmung des Hausrechts erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der betroffenen Personen überwiegen. (2) Videoüberwachte Bereiche sind so zu kennzeichnen, dass Personen vor dem Betreten über den Umstand der Videoüberwachung sowie über den Namen und die Kontaktdaten des Verantwortlichen informiert werden. [...]	ten ist zulässig, soweit sie zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe, zur Wahrnehmung des Hausrechts oder zur Kontrolle von Zugangsberechtigungen erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der betroffenen Personen überwiegen. Der erforderliche Schutz von Einrichtungen, Anlagen oder Teilen davon im Sinne des § 28 Absatz 1 des Katastrophenschutzgesetzes vom 7. Juni 2021 (GVBl. S. 610), das durch Artikel 7 Nummer 5 des Gesetzes vom 11. Dezember 2025 (GVBl. S. 590) geändert worden ist, in der jeweils geltenden Fassung, von staatlichen Einrichtungen der kritischen Infrastruktur, die Einrichtungen nach § 28 Absatz 1 Katastrophenschutzgesetz entsprechen, von zur Aufrechterhaltung der Staats- und Regierungsfunktionen unabdingbar notwendigen Einrichtungen, die einen mit Einrichtungen nach § 28 Absatz 1 Katastrophenschutzgesetz vergleichbaren Schutzbedarf aufweisen, sowie ziviler Objekte, deren Ausfall die zivile Verteidigungsfähigkeit dauerhaft einschränken würde oder denen neben der zivilen auch eine militärische Bedeutung zukommt, dient dem öffentlichen Interesse und geht schutzwürdigen Interessen der betroffenen Personen in der Regel vor. (2) Videoüberwachte Bereiche sind so zu kennzeichnen, dass Personen vor dem Betreten über den Umstand der Videoüberwachung sowie über den Namen und die Kontaktdaten des Verantwortlichen informiert werden. Satz 1 gilt nicht in den Fällen des Absatzes 1 Satz 2, soweit dies den erforderlichen Schutz von Einrichtungen, Anlagen oder Teilen davon oder ziviler Objekte im Sinne des Absatzes 1 Satz 2 beeinträchtigen würde; § 23 Absatz 2 Satz 1 und 2 gilt entsprechend. [...]
§ 24 Auskunftsrecht der betroffenen Person (1) Unbeschadet von § 17 Absatz 4 besteht das Recht der betroffenen Person auf Auskunft gemäß Artikel 15 der Verordnung (EU) 2016/679 nicht, sofern die Erteilung der Auskunft hinter dem öffentlichen Interesse an der Geheimhaltung oder einem	§ 24 Auskunftsrecht der betroffenen Person (1) Unbeschadet von § 17 Absatz 4 besteht das Recht der betroffenen Person auf Auskunft gemäß Artikel 15 der Verordnung (EU) 2016/679 nicht, sofern die Erteilung der Auskunft hinter dem öffentlichen Interesse an der Geheimhaltung oder einem

überwiegenden Geheimhaltungsinteresse Dritter aus zwingenden Gründen zurücktreten muss. Ein Fall des Satzes 1 liegt insbesondere vor, wenn die Erteilung der Auskunft 1. die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes erhebliche Nachteile bereiten würde, 2. die Verfolgung von Straftaten und Ordnungswidrigkeiten gefährden würde oder 3. dazu führen würde, dass Tatsachen, die nach einer öffentlichen Interessen dienenden Rechtsvorschrift oder zum Schutz der Rechte und Freiheiten anderer Personen geheim zu halten sind, aufgedeckt werden. Die betroffene Person kann keine Auskunft über personenbezogene Daten verlangen, die ausschließlich zu Zwecken der Datensicherung oder der Datenschutzkontrolle gespeichert sind und deren Verarbeitung durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist. [...]	überwiegenden Geheimhaltungsinteresse Dritter aus zwingenden Gründen zurücktreten muss. Ein Fall des Satzes 1 liegt insbesondere vor, wenn die Erteilung der Auskunft 1. die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes erhebliche Nachteile bereiten würde, 2. die Verfolgung von Straftaten und Ordnungswidrigkeiten gefährden würde oder 3. dazu führen würde, dass Tatsachen, die nach einer öffentlichen Interessen dienenden Rechtsvorschrift oder zum Schutz der Rechte und Freiheiten anderer Personen geheim zu halten sind, aufgedeckt werden. Die betroffene Person kann keine Auskunft über personenbezogene Daten verlangen, die ausschließlich zu Zwecken der Datensicherung oder der Datenschutzkontrolle gespeichert sind und deren Verarbeitung durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist. [...]
§ 26 Spezifische technische und organisatorische Maßnahmen zur Gewährleistung einer rechtmäßigen Verarbeitung [...] (2) Vor einer Entscheidung über den Einsatz oder eine wesentliche Änderung einer automatisierten Verarbeitung personenbezogener Daten sind die zu treffenden technischen und organisatorischen Maßnahmen auf der Grundlage einer Risikoanalyse zu ermitteln und in einem Datenschutzkonzept zu dokumentieren. Entsprechend der technischen Entwicklung und bei Änderungen der mit den Verarbeitungsvorgängen verbundenen Risiken ist die Ermittlung der Maßnahmen in angemessenen Abständen zu wiederholen. [...]	§ 26 Spezifische technische und organisatorische Maßnahmen zur Gewährleistung einer rechtmäßigen Verarbeitung [...] (2) Vor einer Entscheidung über den Einsatz oder eine wesentliche Änderung einer automatisierten Verarbeitung personenbezogener Daten sind die zu treffenden technischen und organisatorischen Maßnahmen auf der Grundlage einer Risikoanalyse zu ermitteln und in einem Datenschutzkonzept zu dokumentieren. Entsprechend der technischen Entwicklung und bei Änderungen der mit den Verarbeitungsvorgängen verbundenen Risiken ist die Ermittlung der Maßnahmen in angemessenen Abständen zu wiederholen. [...]
§ 48 Auftragsverarbeitung [] (5) Die Verarbeitung durch einen Auftragsverarbeiter hat auf der Grundlage eines Vertrags oder eines	§ 48 Auftragsverarbeitung [] (5) Die Verarbeitung durch einen Auftragsarbeiter hat auf der Grundlage eines Vertrags oder

anderen Rechtsinstruments zu erfolgen, der oder das den Auftragsverarbeiter an den Verantwortlichen bindet und der oder das den Gegenstand, die Dauer, die Art und den Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Rechte und Pflichten des Verantwortlichen festlegt. Der Vertrag oder das andere Rechtsinstrument haben insbesondere vorzusehen, dass der Auftragsverarbeiter [...] (6) Der Vertrag im Sinne des Absatzes 5 ist schriftlich oder elektronisch abzufassen. [...]	eines anderen Rechtsinstruments zu erfolgen, der oder das den Auftragsverarbeiter an den Verantwortlichen bindet und der oder das den Gegenstand, die Dauer, die Art und den Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Rechte und Pflichten des Verantwortlichen festlegt. Der Vertrag oder das andere Rechtsinstrument haben insbesondere vorzusehen, dass der Auftragsverarbeiter [...] (6) Der Vertrag im Sinne des Absatzes 5 oder das andere Rechtsinstrument nach Absatz 5 ist schriftlich oder elektronisch abzufassen. [...]
§ 50 Anforderungen an die Sicherheit der Datenverarbeitung [...] (4) Vor einer Entscheidung über den Einsatz oder eine wesentliche Änderung einer automatisierten Verarbeitung personenbezogener Daten sind die zu treffenden technischen und organisatorischen Maßnahmen auf der Grundlage einer Risikoanalyse zu ermitteln und in einem Datenschutzkonzept zu dokumentieren. Entsprechend der technischen Entwicklung und bei Änderungen der mit den Verarbeitungsvorgängen verbundenen Risiken ist die Ermittlung der Maßnahmen in angemessenen Abständen zu wiederholen. [...]	§ 50 Anforderungen an die Sicherheit der Datenverarbeitung [...] (4) Vor einer Entscheidung über den Einsatz oder eine wesentliche Änderung einer automatisierten Verarbeitung personenbezogener Daten sind die zu treffenden technischen und organisatorischen Maßnahmen auf der Grundlage einer Risikoanalyse zu ermitteln und in einem Datenschutzkonzept zu dokumentieren. Entsprechend der technischen Entwicklung und bei Änderungen der mit den Verarbeitungsvorgängen verbundenen Risiken ist die Ermittlung der Maßnahmen in angemessenen Abständen zu wiederholen. [...]
§ 56 Verzeichnis von Verarbeitungstätigkeiten (1) Der Verantwortliche hat ein Verzeichnis aller Kategorien von Verarbeitungstätigkeiten zu führen, die in seine Zuständigkeit fallen. Dieses Verzeichnis hat die folgenden Angaben zu enthalten: [...] 9. die vorgesehenen Fristen für die Löschung oder die Überprüfung der Erforderlichkeit der Speicherung der verschiedenen Kategorien personenbezogener Daten,	§ 56 Verzeichnis von Verarbeitungstätigkeiten (1) Der Verantwortliche hat ein Verzeichnis aller Kategorien von Verarbeitungstätigkeiten zu führen, die in seine Zuständigkeit fallen. Dieses Verzeichnis hat die folgenden Angaben zu enthalten: [...] 9. wenn möglich, die vorgesehenen Fristen für die Löschung oder die Überprüfung der Erforderlichkeit der Speicherung der verschiedenen Kategorien personenbezogener Daten,

10. eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß § 50 und [...]	10. wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß § 50 und [...]
§ 58 Unterscheidung zwischen verschiedenen Kategorien betroffener Personen Der Verantwortliche hat bei der Verarbeitung personenbezogener Daten so weit wie möglich zwischen den verschiedenen Kategorien betroffener Personen zu unterscheiden. Dies betrifft insbesondere folgende Kategorien: 1. Personen, gegen die ein begründeter Verdacht besteht, dass sie eine Straftat begangen haben, 2. Personen, gegen die ein begründeter Verdacht besteht, dass sie in naher Zukunft eine Straftat begehen werden, 3. strafrechtlich Verurteilte, 4. Opfer einer Straftat oder Personen, bei denen bestimmte Tatsachen darauf hindeuten, dass sie Opfer einer Straftat sein könnten, und 5. andere Personen im Zusammenhang mit einer Straftat oder Personen, die mit den in den Nummern 1 bis 3 genannten Personen in Kontakt oder in Verbindung stehen.	§ 58 Unterscheidung zwischen verschiedenen Kategorien betroffener Personen Der Verantwortliche hat bei der Verarbeitung personenbezogener Daten so weit wie möglich zwischen den verschiedenen Kategorien betroffener Personen zu unterscheiden. Dies betrifft insbesondere folgende Kategorien: 1. Personen, gegen die ein begründeter Verdacht besteht, dass sie eine Straftat begangen haben, 2. Personen, gegen die ein begründeter Verdacht besteht, dass sie in naher Zukunft eine Straftat begehen werden, 3. strafrechtlich Verurteilte, 4. Opfer einer Straftat oder Personen, bei denen bestimmte Tatsachen darauf hindeuten, dass sie Opfer einer Straftat sein könnten, und 5. andere Personen im Zusammenhang mit einer Straftat, wie insbesondere Personen, die bei Ermittlungen in Verbindung mit der betreffenden Straftat oder beim anschließenden Strafverfahren als Zeuginnen oder Zeugen in Betracht kommen oder Personen, die Hinweise zur Straftat geben können oder Personen, die mit den in den Nummern 1 bis 3 genannten Personen in Kontakt oder in Verbindung stehen.
§ 67 Sonstige Datenübermittlung an Empfänger in Drittstaaten (1) Der Verantwortliche kann bei Vorliegen der übrigen für die Datenübermittlung in Drittstaaten geltenden Voraussetzungen im besonderen Einzelfall personenbezogene Daten unmittelbar an nicht in § 64 Absatz 1 Nummer 1 genannte Stellen in Drittstaaten übermitteln, wenn die Übermittlung für die Erfüllung seiner Aufgaben erforderlich ist und	§ 67 Sonstige Datenübermittlung an Empfänger in Drittstaaten (1) Der Verantwortliche kann bei Vorliegen der übrigen für die Datenübermittlung in Drittstaaten geltenden Voraussetzungen im besonderen Einzelfall personenbezogene Daten unmittelbar an nicht in § 64 Absatz 1 Nummer 1 genannte Stellen in Drittstaaten übermitteln, wenn die Übermittlung für die

[...]	Erfüllung seiner Aufgaben unbedingt erforderlich ist und [...]
<u>Berliner Informationsfreiheitsgesetz</u>	
§ 2 Anwendungsbereich (1) Dieses Gesetz regelt die Informationsrechte gegenüber den Behörden und sonstigen öffentlichen Stellen (insbesondere nicht rechtsfähige Anstalten, Krankenhausbetriebe, Eigenbetriebe und Gerichte) des Landes Berlin, den landesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts (§ 44 des Landesorganisationsgesetzes vom 10. Juli 2025 (GVBl. S. 270) in der jeweils geltenden Fassung) und gegenüber Privaten, die mit der Ausübung hoheitlicher Befugnisse betraut sind (öffentliche Stellen). Für die Gerichte und die Behörden der Staatsanwaltschaft gilt dieses Gesetz nur, soweit sie Verwaltungsaufgaben erledigen. (2) Der Zugang zu Informationen über die Umwelt bestimmt sich nach den Regelungen in § 18 a. ./.	§ 2 Anwendungsbereich (1) Dieses Gesetz regelt die Informationsrechte gegenüber den Behörden und sonstigen öffentlichen Stellen (insbesondere nicht rechtsfähige Anstalten, Krankenhausbetriebe, Eigenbetriebe und Gerichte) des Landes Berlin, den landesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts (§ 44 des Landesorganisationsgesetzes vom 10. Juli 2025 (GVBl. S. 270) in der jeweils geltenden Fassung) und gegenüber Privaten, die mit der Ausübung hoheitlicher Befugnisse betraut sind (öffentliche Stellen). Für die Gerichte und die Behörden der Staatsanwaltschaft gilt dieses Gesetz nur, soweit sie Verwaltungsaufgaben erledigen. (2) Der Zugang zu Informationen über die Umwelt bestimmt sich nach den Regelungen in § 18 a. (3) Dieses Gesetz gilt nicht, soweit Informationen über Einrichtungen, Anlagen oder Teile davon im Sinne des § 28 Absatz 1 des Katastrophenschutzgesetzes vom 7. Juni 2021 (GVBl. S. 610), das durch Artikel 7 Nummer 5 des Gesetzes vom 11. Dezember 2025 (GVBl. S. 590) geändert worden ist, in der jeweils geltenden Fassung, Informationen, die für die Funktionsfähigkeit von staatlichen Einrichtungen der kritischen Infrastruktur, die Einrichtungen nach § 28 Absatz 1 Katastrophenschutzgesetz entsprechen, oder von zur Aufrechterhaltung der Staats- und Regierungsfunktionen unabdingbar notwendigen Einrichtungen, die einen mit Einrichtungen nach § 28 Absatz 1 Katastrophenschutzgesetz vergleichbaren Schutzbedarf aufweisen, von Bedeutung sind, oder Informationen über zivile Objekte, deren Ausfall die zivile Verteidigungsfähigkeit dauerhaft einschränken würde oder denen neben der zivilen auch eine militärische Bedeutung zukommt, betroffen sind.

§ 9	§ 9
Schutz besonderer öffentlicher Belange, der Rechtsdurchsetzung und der Strafverfolgung (1) Das Recht auf Akteneinsicht oder Aktenauskunft besteht nicht, soweit und solange durch das vorzeitige Bekanntwerden des Akteninhalts der Erfolg bevorstehender behördlicher Maßnahmen, insbesondere von Überwachungs- und Aufsichtsmaßnahmen, ordnungsbehördlichen Anordnungen und Maßnahmen der Verwaltungsvollstreckung vereitelt wird oder ein vorzeitiges Bekanntwerden des Akteninhalts nach der besonderen Art der Verwaltungstätigkeit mit einer ordnungsgemäßen Aufgabenerfüllung unvereinbar ist. Das Gleiche gilt, soweit und solange durch das vorzeitige Bekanntwerden des Akteninhalts der Erfolg eines Ermittlungsverfahrens wegen einer Straftat oder einer Ordnungswidrigkeit gefährdet werden kann oder nachteilige Auswirkungen für das Land Berlin bei der Durchführung eines laufenden Gerichtsverfahrens zu befürchten sind. (2) Die öffentliche Stelle kann die Akteneinsicht oder Aktenauskunft unter Berufung auf Absatz 1 nur für die Dauer von drei Monaten verweigern, wegen laufender Gerichtsverfahren nur bis zu deren rechtskräftigem Abschluss. Die Entscheidung ist entsprechend zu befristen. Nach Ablauf der Frist hat die öffentliche Stelle auf Antrag erneut zu entscheiden. Eine weitere Vorenthaltung der Akteneinsicht oder Aktenauskunft ist nur zulässig, wenn die Voraussetzungen nach Absatz 1 weiterhin vorliegen. ./.	Schutz besonderer öffentlicher Belange, der Rechtsdurchsetzung und der Strafverfolgung (1) Das Recht auf Akteneinsicht oder Aktenauskunft besteht nicht, soweit und solange durch das vorzeitige Bekanntwerden des Akteninhalts der Erfolg bevorstehender behördlicher Maßnahmen, insbesondere von Überwachungs- und Aufsichtsmaßnahmen, ordnungsbehördlichen Anordnungen und Maßnahmen der Verwaltungsvollstreckung vereitelt wird oder ein vorzeitiges Bekanntwerden des Akteninhalts nach der besonderen Art der Verwaltungstätigkeit mit einer ordnungsgemäßen Aufgabenerfüllung unvereinbar ist. Das Gleiche gilt, soweit und solange durch das vorzeitige Bekanntwerden des Akteninhalts der Erfolg eines Ermittlungsverfahrens wegen einer Straftat oder einer Ordnungswidrigkeit gefährdet werden kann, nachteilige Auswirkungen für das Land Berlin bei der Durchführung eines laufenden Gerichtsverfahrens zu befürchten sind oder nachteilige Auswirkungen für das Land Berlin bei der Vorbereitung und Durchführung einer gerichtlichen oder außergerichtlichen Geltendmachung oder Abwehr von Ansprüchen unmittelbar zu befürchten sind . (2) Die öffentliche Stelle kann die Akteneinsicht oder Aktenauskunft unter Berufung auf Absatz 1 nur für die Dauer von drei Monaten verweigern, wegen laufender Gerichtsverfahren sowie der Vorbereitung und Durchführung einer gerichtlichen oder außergerichtlichen Geltendmachung nur bis zum rechtskräftigen Abschluss der Gerichtsverfahren oder bis zur Beendigung der außergerichtlichen Geltendmachung oder Abwehr von Ansprüchen. Die Entscheidung ist entsprechend zu befristen. Nach Ablauf der Frist hat die öffentliche Stelle auf Antrag erneut zu entscheiden. Eine weitere Vorenthaltung der Akteneinsicht oder Aktenauskunft ist nur zulässig, wenn die Voraussetzungen nach Absatz 1 weiterhin vorliegen. (3) Über Absatz 1 und 2 hinaus besteht das Recht auf Akteneinsicht oder Aktenauskunft nicht 1. für Vorgänge der Steuerverwaltung, 2. für Informationen,

	a) über die die Antragstellerin oder der Antragsteller bereits verfügt oder die in zumutbarer Weise aus allgemein zugänglichen Quellen beschafft werden können, b) die einer Geheimhaltungs- und Vertraulichkeitspflicht durch Einstufung als Verschlussache nach § 6 Absatz 1 und 2 des Berliner Sicherheitsüberprüfungsgesetzes vom 25. Juni 2001 (GVBl. S. 243), das zuletzt durch Artikel 3 des Gesetzes vom 13. Juni 2018 (GVBl. S. 418) geändert worden ist, in der jeweils geltenden Fassung oder nach der Geschäftsordnung des Abgeordnetenhauses von Berlin unterfallen, c) die einem Berufs- oder besonderen Amtsgeheimnis unterliegen oder d) deren Bekanntwerden die IT-Sicherheit oder die IT-Infrastruktur der in § 2 Absatz 1 genannten öffentlichen Stellen gefährden könnte, oder 3. wenn der Antrag offensichtlich missbräuchlich, insbesondere zum Zweck der Vereitelung oder Verzögerung von Verwaltungshandlungen, erfolgt.
<u>Bäder-Anstaltsgesetz</u>	
§ 23 Verarbeitung personenbezogener Daten Die Verarbeitung personenbezogener Daten ist zulässig, wenn sie zur Erfüllung der in diesem Gesetz genannten Aufgaben erforderlich ist.	§ 23 Verarbeitung personenbezogener Daten Die Verarbeitung personenbezogener Daten ist zulässig, wenn sie zur Erfüllung der in diesem Gesetz genannten Aufgaben erforderlich ist. Die Verarbeitung ist insbesondere zulässig zur 1. Kontrolle der Gültigkeit von Eintrittskarten oder Zugangsberechtigungen, 2. Gewährleistung des oder Wiederherstellung eines sicheren Badbetriebes oder 3. Wahrnehmung oder Durchsetzung des Hausrechts insbesondere bei Verstößen gegen die Haus- und Badeordnung.
§ 24 Inkrafttreten, Außerkrafttreten Dieses Gesetz tritt am Tage nach der Verkündung im Gesetz- und Verordnungsblatt für Berlin in Kraft. Es tritt mit Ablauf des Tages außer Kraft, an welchem die durch den Formwechsel gemäß § 22 entstandene private Gesellschaft in das Handelsregister eingetragen wird. Der in Satz 2 genannte Tag	§ 24 Videoüberwachung (1) Die Beobachtung öffentlich zugänglicher Räume der Bäder mit Hilfe optisch-elektronischer Einrichtungen (Videoüberwachung) sowie die Verarbeitung der dadurch erhobenen personenbezogenen Daten ist zulässig, soweit sie 1. zur Kontrolle von Zugangsberechtigungen,

des Außerkrafttretens ist im Gesetz- und Verordnungsblatt für Berlin bekannt zu machen.	2. zur Gewährleistung des oder Wiederherstellung eines sicheren Badbetriebes, 3. zur Wahrnehmung oder Durchsetzung des Hausrechts insbesondere bei Verstößen gegen die Haus- und Badeordnung oder 4. zum Schutz des Eigentums oder Besitzes erforderlich ist und keine Anhaltspunkte bestehen, dass überwiegende schutzwürdige Interessen der betroffenen Personen entgegenstehen. (2) § 20 Absatz 2, 3 und 5 des Berliner Datenschutzgesetzes vom 13. Juni 2018 (GVBl. S. 418), das zuletzt durch Artikel 1 des Gesetzes vom [einsetzen: Datum und Fundstelle des Gesetzes zur Änderung des Berliner Datenschutzgesetzes und weiterer Rechtsvorschriften] geändert worden ist, in der jeweils geltenden Fassung gilt entsprechend.
./.	§ 25 Inkrafttreten, Außerkrafttreten Dieses Gesetz tritt am Tage nach der Verkündung im Gesetz- und Verordnungsblatt für Berlin in Kraft. Es tritt mit Ablauf des Tages außer Kraft, an welchem die durch den Formwechsel gemäß § 22 entstandene private Gesellschaft in das Handelsregister eingetragen wird. Der in Satz 2 genannte Tag des Außerkrafttretens ist im Gesetz- und Verordnungsblatt für Berlin bekannt zu machen.
<u>Gesetz über das Verfahren der Berliner Verwaltung</u>	
§ 6 - Akteneinsicht durch Beteiligte (1) Die Behörde hat den Beteiligten Einsicht in die das Verfahren betreffenden Akten zu gestatten. Bis zum Abschluss des Verwaltungsverfahrens gilt Satz 1 nicht für Entwürfe zu Entscheidungen sowie für die Arbeiten zu ihrer unmittelbaren Vorbereitung. (2) Die Regelungen der §§ 5 bis 12 des Berliner Informationsfreiheitsgesetzes gelten entsprechend.	§ 6 - Akteneinsicht durch Beteiligte (1) Die Behörde hat den Beteiligten Einsicht in die das Verfahren betreffenden Akten zu gestatten. Bis zum Abschluss des Verwaltungsverfahrens gilt Satz 1 nicht für Entwürfe zu Entscheidungen sowie für die Arbeiten zu ihrer unmittelbaren Vorbereitung. (2) Die Behörde ist zur Gestattung der Akteneinsicht nicht verpflichtet, soweit das Bekanntwerden des Inhalts der Akten dem Wohl des Bundes oder eines Landes Nachteile bereiten oder zu einer schwerwiegenden Gefährdung des Gemeinwohls führen würde. Dies ist in der Regel bei Akteneinhalten über Einrichtungen, Anlagen oder Teile davon im Sinne des § 28 Absatz 1 des Katastrophenschutzgesetzes vom 7. Juni 2021 (GVBl. S. 610), das durch Artikel 7 Nummer 5 des Gesetzes vom

	11. Dezember 2025 (GVBl. S. 590) geändert worden ist, in der jeweils geltenden Fassung, über staatliche Einrichtungen der kritischen Infrastruktur, die Einrichtungen nach § 28 Absatz 1 Katastrophenschutzgesetz entsprechen, über zur Aufrechterhaltung der Staats- und Regierungsfunktionen unabdingbar notwendige Einrichtungen, die einen mit Einrichtungen nach § 28 Absatz 1 Katastrophenschutzgesetz vergleichbaren Schutzbedarf aufweisen, sowie über zivile Objekte, deren Ausfall die zivile Verteidigungsfähigkeit dauerhaft einschränken würde oder denen neben der zivilen auch eine militärische Bedeutung zukommt, anzunehmen. Im Übrigen gelten die Regelungen der §§ 5 bis 12 des Berliner Informationsfreiheitsgesetzes vom 15. Oktober 1999 (GVBl. S. 561), das zuletzt durch Artikel 2 des Gesetzes vom [einsetzen: Datum und Fundstelle des Gesetzes zur Änderung des Berliner Datenschutzgesetzes und weiterer Rechtsvorschriften] geändert worden ist, in der jeweils geltenden Fassung entsprechend.
<u>Allgemeines Sicherheits- und Ordnungsgesetz</u>	
§ 17 - Allgemeine Befugnisse; Begriffsbestimmungen (1) Die Ordnungsbehörden und die Polizei können die notwendigen Maßnahmen treffen, um eine im einzelnen Falle bestehende Gefahr für die öffentliche Sicherheit oder Ordnung (Gefahr) abzuwehren, soweit nicht die §§ 18 bis 51b ihre Befugnisse besonders regeln. [...] (4) Straftaten, die sich auf eine Schädigung der Umwelt oder auf gemeinschaftswidrige Wirtschaftsformen, insbesondere illegale Beschäftigung beziehen und geeignet sind, die Sicherheit der Bevölkerung zu beeinträchtigen, stehen Straftaten von erheblicher Bedeutung im Sinne des Absatzes 3 gleich.	§ 17 - Allgemeine Befugnisse; Begriffsbestimmungen (1) Die Ordnungsbehörden und die Polizei können die notwendigen Maßnahmen treffen, um eine im einzelnen Falle bestehende Gefahr für die öffentliche Sicherheit oder Ordnung (Gefahr) abzuwehren, soweit nicht die §§ 18 bis 51b ihre Befugnisse besonders regeln. [...] (4) Straftaten, die sich auf eine Schädigung der Umwelt, eine Beeinträchtigung der Funktionsfähigkeit von Einrichtungen, Anlagen oder Teilen davon im Sinne des § 28 Absatz 1 des Katastrophenschutzgesetzes vom 7. Juni 2021 (GVBl. S. 610), das durch Artikel 7 Nummer 5 des Gesetzes vom 11. Dezember 2025 (GVBl. S. 590) geändert worden ist, in der jeweils geltenden Fassung, von staatlichen Einrichtungen der kritischen Infrastruktur, die Einrichtungen nach § 28 Absatz 1 Katastrophenschutzgesetz entsprechen, oder von zur Aufrechterhaltung der Staats- und Regierungsfunktionen unabdingbar

	notwendigen Einrichtungen, die einen mit Einrichtungen nach § 28 Absatz 1 Katastrophenschutzgesetz vergleichbaren Schutzbedarf aufweisen, oder auf gemeinschaftswidrige Wirtschaftsformen, insbesondere illegale Beschäftigung, beziehen und geeignet sind, die Sicherheit der Bevölkerung zu beeinträchtigen, stehen Straftaten von erheblicher Bedeutung im Sinne des Absatzes 3 gleich.
<u>Open Data Verordnung</u>	
§ 5 - Ausnahmen (1) Informationen dürfen nicht bereitgestellt werden, wenn 1. an ihnen kein oder nur ein eingeschränktes Zugangsrecht auf Grund gesetzlicher Regelungen, insbesondere gemäß den §§ 5, 9 bis 12 des Berliner Informationsfreiheitsgesetzes vom 15. Oktober 1999 (GVBl. S. 561), das zuletzt durch Artikel 21 des Gesetzes vom 2. Februar 2018 (GVBl. S. 160) geändert worden ist, in der jeweils geltenden Fassung, besteht oder ein Zugangsrecht erst nach der Beteiligung Dritter bestünde, [...]	§ 5 - Ausnahmen (1) Informationen dürfen nicht bereitgestellt werden, wenn 1. an ihnen kein oder nur ein eingeschränktes Zugangsrecht auf Grund gesetzlicher Regelungen, insbesondere gemäß den §§ 5, 9 bis 12 des Berliner Informationsfreiheitsgesetzes vom 15. Oktober 1999 (GVBl. S. 561), das zuletzt durch Artikel 2 des Gesetzes vom [einsetzen: Datum und Fundstelle des Gesetzes zur Änderung des Berliner Datenschutzgesetzes und weiterer Rechtsvorschriften] geändert worden ist, in der jeweils geltenden Fassung besteht oder ein Zugangsrecht erst nach der Beteiligung Dritter bestünde oder es sich um Informationen im Sinne des § 2 Absatz 3 des Berliner Informationsfreiheitsgesetzes handelt, [...]

II. Wortlaut der zitierten Rechtsvorschriften

Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz - TDDDG

§ 19 Technische und organisatorische Vorkehrungen

(1) Anbieter von digitalen Diensten haben durch technische und organisatorische Vorkehrungen sicherzustellen, dass der Nutzer von digitalen Diensten

1. die Nutzung des Dienstes jederzeit beenden kann und
2. digitale Dienste geschützt gegen Kenntnisnahme Dritter in Anspruch nehmen kann.

(2) Anbieter von digitalen Diensten haben die Nutzung von digitalen Diensten und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer von digitalen Diensten ist über diese Möglichkeit zu informieren.

(3) Die Weitervermittlung zu einem anderen Anbieter von digitalen Diensten ist dem Nutzer anzuzeigen.

(4) Anbieter von digitalen Diensten haben, soweit dies technisch möglich und wirtschaftlich zumutbar ist, im Rahmen ihrer jeweiligen Verantwortlichkeit für geschäftsmäßig angebotene digitale Dienste durch technische und organisatorische Vorkehrungen sicherzustellen, dass

1. kein unerlaubter Zugriff auf die technischen Einrichtungen, die sie für das Angebot ihrer digitalen Dienste nutzen, möglich ist und
2. die technischen Einrichtungen nach Nummer 1 gesichert sind gegen Störungen, auch gegen solche, die durch äußere Angriffe bedingt sind.

Vorkehrungen nach Satz 1 müssen den Stand der Technik berücksichtigen. Eine Vorkehrung nach Satz 1 ist insbesondere die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens. Anordnungen des Bundesamtes für Sicherheit in der Informationstechnik nach § 7d Satz 1 BSI-Gesetz bleiben unberührt.

§ 20 Verarbeitung personenbezogener Daten Minderjähriger

Hat ein Anbieter von digitalen Diensten zur Wahrung des Jugendschutzes personenbezogene Daten von Minderjährigen erhoben, etwa durch Mittel zur Altersverifikation oder andere technische Maßnahmen, oder anderweitig gewonnen, so darf er diese Daten nicht für kommerzielle Zwecke verarbeiten.

§ 25 Schutz der Privatsphäre bei Endeinrichtungen

(1) Die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind, sind nur zulässig, wenn der Endnutzer auf der Grundlage von klaren und umfassenden Informationen eingewilligt hat. Die Information des Endnutzers und die Einwilligung haben gemäß der Verordnung (EU) 2016/679 zu erfolgen.

(2) Die Einwilligung nach Absatz 1 ist nicht erforderlich,

1. wenn der alleinige Zweck der Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der alleinige Zweck des Zugriffs auf bereits in der Endeinrichtung des Endnutzers gespeicherte Informationen die Durchführung der Übertragung einer Nachricht über ein öffentliches Telekommunikationsnetz ist oder
2. wenn die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der Zugriff auf bereits in der Endeinrichtung des Endnutzers gespeicherte Informationen unbedingt erforderlich ist, damit der Anbieter eines digitalen Dienstes einen vom Nutzer ausdrücklich gewünschten digitalen Dienst zur Verfügung stellen kann.

Katastrophenschutzgesetz

§ 28 Pflichten der Betreiberinnen und Betreiber Kritischer Infrastrukturen

- (1) Die Betreiberinnen und Betreiber von Einrichtungen, Anlagen oder Teilen davon, die
 1. den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Entsorgung, Gesundheit, Wasser, Ernährung, Medien und Kultur oder Finanz- und Versicherungswesen angehören und
 2. von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden,sind verpflichtet, mit den Katastrophenschutzbehörden zusammenzuarbeiten.

Berliner Sicherheitsüberprüfungsgesetz

§ 6 Verschlussachen

(1) Verschlussachen sind im öffentlichen Interesse geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse unabhängig von ihrer Darstellungsform. Sie werden entsprechend ihrer Schutzbedürftigkeit von einer amtlichen Stelle oder auf deren Veranlassung eingestuft.

(2) Eine Verschlussache ist

1. STRENG GEHEIM, wenn die Kenntnisnahme durch Unbefugte den Bestand oder lebenswichtige Interessen der Bundesrepublik Deutschland oder eines ihrer Länder gefährden kann,
2. GEHEIM, wenn die Kenntnisnahme durch Unbefugte die Sicherheit der Bundesrepublik Deutschland oder eines ihrer Länder gefährden oder ihren Interessen schweren Schaden zufügen kann,

3. VS-VERTRAULICH, wenn die Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder schädlich sein kann,
4. VS-NUR FÜR DEN DIENSTGEBRAUCH, wenn die Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder nachteilig sein kann.

(3) ...