Mitteilung des Senats
an die Bremische Bürgerschaft
vom 18. Oktober 2022

Der Senat überreicht der Bürgerschaft (Landtag) den Entwurf eines Gesetzes über den Einsatz der Informations- und Kommunikationstechnik bei Gerichten und Staatsanwaltschaften in der Justiz der Freien Hansestadt Bremen (IT-Justizgesetz – ITJG) mit der Bitte um Beschlussfassung.

Ziel des hier vorgelegten IT-Justizgesetzes ist es, die vorstehend dargestellten Anforderungen für die Justiz des Landes Bremen umzusetzen und mit der dadurch eingerichteten IT-Kontrollkommission die Überprüfungsmöglichkeit der Judikativen abzusichern. Zugleich soll die IT-Kontrollkommission auch die Aufsicht über die datenschutzkonforme Verarbeitung personenbezogener Daten im Bereich der rechtsprechenden Gewalt ausüben, die von der Aufsicht der Landesdatenschutzbeauftragten nicht erfasst ist. Der Senat beschließt zur Umsetzung dieses Ziels das als Anlage beigefügte Gesetz über den Einsatz der Informations- und Kommunikationstechnik bei Gerichten und Staatsanwaltschaften in der Justiz der Freien Hansestadt Bremen (IT-Justizgesetz – ITJG). Zu den wesentlichen Inhalten des ITJG gehört es, zur Überwachung der Einhaltung der Ziele und Vorschriften des Gesetzes ein unabhängiges Kontrollgremium (IT-Kontrollkommission) einzurichten (§ 2), zu schützende Daten und Prozesse zu definieren (§ 3), die IT-Kontrollkommission mit entsprechenden Kontrollbefugnissen auszustatten (§ 5), technische, betriebliche und organisatorische Maßnahmen festzulegen, die für die Datenverarbeitung maßgeblich sind (§ 6), Einsichts- und Eingriffsrechte in die geschützten Daten und Prozesse zu bestimmen (§ 7) und das Verhältnis des Gesetzes zu anderen Rechtsvorschriften zu klären (§ 8).

Der Gesetzentwurf mit Begründung ist als Anlage beigefügt.

Beschlussempfehlung:

Der Senat bittet die Bürgerschaft (Landtag) um Beratung und Beschlussfassung des Gesetzentwurfs.

Entwurf

Gesetz über den Einsatz der Informations- und Kommunikationstechnik bei Gerichten und Staatsanwaltschaften in der Justiz der Freien Hansestadt Bremen (IT-Justizgesetz – ITJG)

Vom …

Der Senat verkündet das nachstehende, von der Bürgerschaft (Landtag) beschlossene Gesetz:

§ 1

Regelungszweck

(1) Bei der Organisation und dem Betrieb von Informations- und Kommunikationstechnik (IT) für die Gerichte und Staatsanwaltschaften sind die richterliche Unabhängigkeit, die sachliche Unabhängigkeit der Rechtspflegerinnen und Rechtspfleger sowie das Legalitätsprinzip in der Strafverfolgung zu beachten und besonders zu schützen. Insbesondere sind die Integrität und die Vertraulichkeit der Entscheidungsprozesse geschützt und unbefugte Kenntnisnahmen zu verhindern. Zudem ist die Funktionsfähigkeit der Justiz zu sichern.

(2) Dieses Gesetz regelt zur Gewährleistung der Ziele nach Absatz 1 die organisatorischen und rechtlichen Rahmenbedingungen des IT-Betriebes der Gerichte, einschließlich des Staatsgerichtshofs, und der Staatsanwaltschaften.

(3) Zentraler IT-Dienstleister für die Gerichte und Staatsanwaltschaften ist der Informations- und Kommunikationsdienstleister Dataport, Anstalt öffentlichen Rechts.

§ 2

Verantwortlichkeit, Zuständige Behörde

(1) Die Senatorin für Justiz und Verfassung oder der Senator für Justiz und Verfassung trägt durch geeignete Maßnahmen für die Einhaltung der Ziele und Vorschriften dieses Gesetzes Sorge. Sie oder er ist die zuständige Behörde im Sinne dieses Gesetzes.

(2) Die Aktenhoheit liegt bei dem jeweils zuständigen Gericht beziehungsweise der jeweils zuständigen Staatsanwaltschaft.

(3) Die Einhaltung der Ziele und Vorschriften dieses Gesetzes wird durch ein unabhängiges Kontrollgremium (IT-Kontrollkommission) überwacht.

§ 3

Zu schützende Daten und Prozesse

(1) Zu schützen ist der gesamte Prozess der richterlichen, staatsanwaltschaftlichen sowie rechtspflegerischen Entscheidungsfindung und die Entscheidung selbst.

(2) Zu den zu schützenden Daten zählen im Rahmen der nach Absatz 1 geschützten Prozesse insbesondere:

1. Sämtliche erstellten, erhaltenen oder weiterverarbeiteten elektronischen Dokumente oder sonstigen Daten einschließlich aller Metadaten (Inhaltsdaten),

2. verfahrensbezogene Daten, die in Fachverfahren, in der elektronischen Akte oder in sonstigen Programmen oder Datenspeichern – auch nur zeitlich befristet – erfasst werden (Verfahrensdaten) und

3. systemintern automatisch erstellte Daten über die Benutzung der zur Verfügung stehenden IT (Logdaten).

(3) Inhaltsdaten, welche die richterliche, rechtspflegerische oder staatsanwaltschaftliche Entscheidungsfindung ganz oder teilweise dokumentieren, sowie Verfahrensdaten, die Rückschlüsse auf den Prozess der Entscheidungsfindung ermöglichen, sind besonders geschützt. Gleiches gilt für Entwürfe zu Urteilen, Beschlüssen und Verfügungen, die Arbeiten zu ihrer Vorbereitung, Annotationen zu Dokumenten und die Dokumente, die Beratungen und Abstimmungen betreffen, sowie die auf die IT-Nutzung bezogenen Log- und Metadaten der Richterinnen und Richter, Rechtspflegerinnen und Rechtspfleger, Staatsanwältinnen und Staatsanwälte sowie Amtsanwältinnen und Amtsanwälte.

§ 4

IT-Kontrollkommission

(1) Die IT-Kontrollkommission wird bei der zuständigen Behörde eingerichtet. Diese stellt der IT-Kontrollkommission die für die Wahrnehmung ihrer Aufgaben erforderlichen Mittel zur Verfügung und trägt die durch ihre Tätigkeit entstehenden Kosten.

(2) Die IT-Kontrollkommission besteht aus

1. zwei Richterinnen oder Richtern,

2. einer Staatsanwältin beziehungsweise einem Staatsanwalt oder einer Amtsanwältin beziehungsweise einem Amtsanwalt sowie

3. einer Rechtspflegerin beziehungsweise einem Rechtspfleger

als stimmberechtigten Mitgliedern. Jedes Mitglied nach Satz 1 Nummer 1 hat zwei Stimmen, die es nur einheitlich abgeben kann. Jedes Mitglied nach Satz 1 Nummer 2 und jedes Mitglied nach Satz 1 Nummer 3 hat eine Stimme.

(3) Beratende Mitglieder der Kommission sind

1. eine Vertretung der Senatorin für Finanzen oder des Senators für Finanzen,

2. eine Vertretung der zuständigen Behörde sowie

3. die oder der Informationssicherheitsbeauftragte der zuständigen Behörde.

(4) Ein Mitglied nach Absatz 2 Nummer 1 wird von den Richterräten der Gerichte der ordentlichen Gerichtsbarkeit gemeinsam und ein Mitglied von den Richterräten der Gerichte der Arbeits-, Finanz-, Sozial- und Verwaltungsgerichtsbarkeit gemeinsam, das Mitglied nach Absatz 2 Nummer 2 vom Personalrat der Staatsanwaltschaften und das Mitglied nach Absatz 2 Nummer 3 von den Personalräten der Gerichte und Staatsanwaltschaften gewählt. Zusätzlich ist für jeden Bereich eine Stellvertretung zu wählen.

(5) Die Amtszeit der stimmberechtigten Mitglieder beträgt vier Jahre. Für ausgeschiedene Mitglieder rücken die jeweiligen Stellvertretungen in die IT-Kontrollkommission nach. Die beratenden Mitglieder werden von der Senatorin für Finanzen oder dem Senator für Finanzen und der zuständigen Behörde benannt.

(6) Die IT-Kontrollkommission trifft ihre Entscheidungen mit der Mehrheit der Stimmen der stimmberechtigten Mitglieder.

(7) Für die Beratung konkreter Vorgänge ist auf Antrag mindestens zweier – auch nicht stimmberechtigter – Mitglieder eine Vertreterin oder ein Vertreter der Leitung des betroffenen Gerichts oder der betroffenen Staatsanwaltschaft hinzuzuziehen.

(8) Die zuständige Behörde wird ermächtigt, weitere Einzelheiten, insbesondere zur Wahl und zur Amtszeit der stimmberechtigten Mitglieder sowie zur Beschlussfassung durch Rechtsverordnung zu regeln.

(9) Die IT-Kontrollkommission gibt sich eine Geschäftsordnung. Sie kann durch Beschluss Befugnisse auf einzelne Mitglieder übertragen.

(10) Die IT-Kontrollkommission dokumentiert in geeigneter Weise ihre Tätigkeit und die erzielten Ergebnisse und Erkenntnisse. Die Dokumentation ist auf Verlangen den Richter- und Personalvertretungen sowie der zuständigen Behörde zuzuleiten.

§ 5

Kontrollrechte der IT-Kontrollkommission

(1) Zum Schutz vor unbefugten Zugriffen und soweit dies zur Aufgabenerfüllung erforderlich ist, darf die IT-Kontrollkommission bei externen IT-Dienstleistern und Auftragsverarbeitern Kontrollen durchführen. Gegenstand der Kontrolle ist die Einhaltung der Vorschriften dieses Gesetzes, der bestehenden Verträge und aller sonstigen Bestimmungen, die der Bereitstellung von IT-Infrastrukturen, der

Betreuung der eingesetzten IT und der Gewährleistung der IT-Sicherheit in den Gerichten und Staatsanwaltschaften dienen. Das Kontrollrecht besteht auch bezüglich derjenigen Akten und Dokumente, die sich auf die Rechtsaufsicht über Dataport oder auf die Begründung und Ausgestaltung der Benutzungsverhältnisse zu Dataport oder auf die Verträge mit anderen externen IT-Dienstleistern und Auftragsverarbeitern beziehen und die einen wesentlichen Bezug zur Organisation und zum Einsatz von IT in den Gerichten und Staatsanwaltschaften haben. Soweit erforderlich, ist der IT-Kontrollkommission zu den vorgenannten Zwecken Zutritt zu gewähren und eine uneingeschränkte Auskunft und Einsicht zu gewährleisten. Das Grundrecht der Unverletzlichkeit der Wohnung (Artikel 13 Absatz 1 des Grundgesetzes) wird insoweit eingeschränkt. Die Dokumentation der berechtigten Inhaberinnen und Inhaber administrativer Zugänge sowie die Protokolle nach § 6 Absatz 3 stehen der IT-Kontrollkommission auf Verlangen zur Einsichtnahme zur Verfügung.

(2) Personenbezogene Daten dürfen im Rahmen von Kontrollen nach Absatz 1 nur eingesehen oder sonst verwendet werden, soweit dies zur Aufgabenerfüllung unerlässlich ist. Sofern der zentrale IT-Dienstleister Dataport betroffen ist, ist der oder die zentrale Informationssicherheitsbeauftragte der Senatorin für Finanzen oder des Senators für Finanzen einzubeziehen.

(3) Die IT-Kontrollkommission kann sowohl anlassbezogen als auch verdachtsunabhängig außerhalb von Kontrollen nach Absatz 1 zur Aufdeckung von Verstößen und Missbrauch, aber auch präventiv Einsicht in alle Datenverarbeitungsvorgänge nach §§ 6 und 7 nehmen und unter Beachtung der Regelung des Absatzes 2 alle dabei anfallenden Daten zur Erfüllung ihrer Aufgaben nach diesem Gesetz verarbeiten. Sie kann dabei ferner Einsicht in alle die IT betreffenden Verträge und Konzepte nehmen sowie Inaugenscheinnahmen der IT-Einrichtungen vornehmen. Soweit erforderlich, kann sie auch Auskünfte bei externen IT-Dienstleistern, Auftragsverarbeitern, der zuständigen Behörde sowie den mit der Verarbeitung von Justizdaten betrauten Beschäftigten einholen. Einsichtnahmen in besonders geschützte Daten und Prozesse gemäß § 3 Absatz 3 sind hierbei nur gestattet, soweit sie zur Aufgabenerfüllung erforderlich sind.

(4) Soweit dies zur ordnungsgemäßen Erfüllung ihrer Aufgaben erforderlich ist, kann die IT-Kontrollkommission sachkundige Dritte, auch aus den Gerichtsverwaltungen oder der zuständigen Behörde, hinzuziehen. Soweit die Hinzuziehung externer Sachverständiger im Einzelfall erforderlich ist, vergibt die zuständige Behörde unter Beteiligung der IT-Kontrollkommission die Aufträge und trägt die Kosten; Regressforderungen nach sonstigen Vorschriften bleiben unbenommen.

(5) Stellt die IT-Kontrollkommission Verstöße gegen die Bestimmungen dieses Gesetzes fest, so unterrichtet sie die zuständige Behörde, deren Informationssicherheitsbeauftragte oder Informationssicherheitsbeauftragten, die betroffene Dienststelle, den zentralen Informationssicherheitsbeauftragten oder die Informationssicherheitsbeauftragte der Senatorin für Finanzen oder des Senators für Finanzen sowie gegebenenfalls den jeweiligen IT-Dienstleister und, sofern sie das für geboten erachtet, die Betroffenen. Ferner fordert sie die verantwortlichen Stellen unter Setzung einer angemessenen Frist zur Mängelbeseitigung auf. Handelt es sich um einen erheblichen Verstoß oder erfolgt keine fristgerechte Mängelgewährleistung, so spricht die IT-Kommission eine Beanstandung aus. Die zuständige Behörde ist

verpflichtet, auf Beanstandungen im Rahmen ihrer Zuständigkeit angemessen zu reagieren und die IT-Kontrollkommission sowie die Leitungen der betroffenen Gerichte und Staatsanwaltschaften über ergriffene Maßnahmen zu unterrichten.

(6) Einzelne Amtsträgerinnen oder Amtsträger, die Leitungen der Gerichte und Staatsanwaltschaften sowie Richter- und Personalräte haben das Recht, sich bei Vorliegen eines Verdachts der Verletzung von Bestimmungen dieses Gesetzes oder mit konkreten Beschwerden an die IT-Kontrollkommission zu wenden.

(7) Die Mitglieder der IT-Kontrollkommission sind unter Fortzahlung der Dienstbezüge in erforderlichem Umfang von ihren dienstlichen Tätigkeiten freizustellen. Die zuständige Behörde wird ermächtigt, Näheres zur Freistellung durch Rechtsverordnung zu regeln.

§ 6

Technische, betriebliche und organisatorische Maßnahmen

(1) Im Anwendungsbereich des § 3 sind bei der Ausgestaltung der zur Verarbeitung von Daten eingesetzten Anwendungssoftware und dem Betrieb der IT die Grundsätze der Datensparsamkeit und Datenvermeidung zu beachten. Die in der Datenverarbeitung tätigen IT-Dienstleister, Auftragsverarbeiter sowie die zuständige Behörde und in der Datenverarbeitung tätige Dienststellen haben dafür Sorge zu tragen, dass eine sichere Verarbeitung der zu schützenden Daten unter Beachtung des Standes der Technik erfolgt.

(2) Bei dem Betrieb der IT und der Datenverarbeitung ist unter Beachtung des Standes der Technik insbesondere dafür Sorge zu tragen, dass unbefugte Einblicke und Eingriffe in die richterliche, rechtspflegerische und staatsanwaltschaftliche Tätigkeit unterbleiben.

(3) Zugriffe durch technische Administratorinnen und Administratoren der externen IT-Dienstleister und Auftragsverarbeiter sind revisionssicher zu protokollieren, es sei denn, der Zugriff erfolgt mit ausdrücklicher Einwilligung der oder des unmittelbar Berechtigten. Die Einwilligung soll protokolliert werden.

(4) Sicherheitsvorfälle sind der IT-Kontrollkommission, dem Informationssicherheitsbeauftragten oder der Informationssicherheitsbeauftragten der zuständigen Behörde und den Leitungen der betroffenen Gerichte oder Staatsanwaltschaften sowie der oder dem zentralen Informationssicherheitsbeauftragten der Senatorin für Finanzen oder des Senators für Finanzen zu melden. Die zuständige Behörde wird ermächtigt, Näheres durch Rechtsverordnung zu regeln.

§ 7

Behandlung der Daten und Prozesse

(1) Einsicht und Eingriffe in die in § 3 genannten Prozesse und Daten sind nur Berechtigten gestattet.

(2) Unmittelbar berechtigt sind die mit der Verfahrensbearbeitung betrauten Amtsträgerinnen und Amtsträger der Gerichte und Staatsanwaltschaften im Rahmen ihrer jeweiligen Zuständigkeit.

(3) Weitere Berechtigungen für Amtsträgerinnen und Amtsträger der Gerichte und Staatsanwaltschaften sowie für die Beschäftigten der in der Datenverarbeitung tätigen IT-Dienstleister und Auftragsverarbeiter und die zuständige Behörde folgen zudem aus der Einwilligung der in der Justiz unmittelbar berechtigten Amtsträgerinnen und Amtsträger nach Absatz 2, gesetzlichen Vorschriften, insbesondere auch zur Dienstaufsicht, unter Beachtung des Absatzes 7 sowie aus technischen Erfordernissen des IT-Betriebs.

(4) Abweichend von Absatz 2 und 3 sind Einsichten und Eingriffe in die in § 3 genannten Prozesse und Daten nur mit vorheriger einzelfallbezogener Genehmigung der IT-Kontrollkommission zulässig. Bei Gefahr im Verzug kann von Satz 1 abgewichen werden; die IT-Kontrollkommission ist unverzüglich in Kenntnis zu setzen.

(5) In der Datenverarbeitung tätige Auftragsverarbeiter erstellen Berechtigungskonzepte für ihren Zugriff auf Daten und Dokumente nach § 3.

(6) Die nach diesem Gesetz Berechtigten sind verpflichtet, im Rahmen ihrer Berechtigung erzeugte Daten und Dokumente vor unberechtigtem Zugriff zu schützen. Die Mitarbeiterinnen und Mitarbeiter der zuständigen Behörde dürfen entsprechende Daten einschließlich der Metadaten weder an nicht berechtigte Stellen innerhalb der Behörde noch an sonstige Behörden oder Dritte weitergeben; gesetzliche Herausgabepflichten von Daten bleiben unberührt. Die Daten werden ausschließlich streng zweckgebunden für den Betrieb der IT-Fachverfahren genutzt. Eine Auswertung oder Aufzeichnung von personenbezogenen- oder beziehbaren Daten zur Erstellung von Nutzungsprofilen oder zur Durchführung von Verhaltens- oder Leistungskontrollen von Bediensteten ist den Mitarbeiterinnen und Mitarbeitern der zuständigen Behörde untersagt; dies gilt nicht im Rahmen von Disziplinarverfahren und der Dienstaufsicht, soweit ein konkreter Verdacht missbräuchlichen Verhaltens besteht.

(7) Statistik im richterlichen Bereich der Justiz darf ausschließlich aus hinreichend aggregierten und anonymisierten Daten im Sinne des § 3 Absatz 2 Nummer 2 erstellt werden, soweit sie in Fachverfahren erfasst werden. Eine Weitergabe von nicht aggregierten Daten an andere Behörden oder ein Zugriff auf nicht aggregierte Daten durch sonstige Dritte ist unzulässig, soweit nicht ein Fall von Satz 4 vorliegt. Hiervon ausgenommen sind Daten, welche für die Aufarbeitung und Isolierung von Cyberangriffen benötigt werden. Zu anderen, auch statistischen Zwecken im nichtrichterlichen Bereich, können anonymisierte Daten im Sinne des § 3 Absatz 2 Nummer 1 und 2 bei hinreichender Beachtung der zu schützenden Interessen übermittelt oder freigegeben werden, wenn diese Daten – soweit möglich – aggregiert sind und sichergestellt ist, dass aus diesen kein Rückschluss auf einzelne Richterinnen und Richter gezogen wird und sie nicht für eine Beobachtung, Analyse und Kontrolle von Verhalten und Leistung der Richterinnen und Richter beziehungsweise Kollegialspruchkörper verwendet werden. Die für die Geschäftsverteilung und die Dienstaufsicht unter Berücksichtigung des § 1 Absätze 1 und 2 erforderlichen Daten gemäß § 3 Absatz 2 Nummer 2 stehen der jeweiligen Leitung des Gerichtes und dem Präsidium im Rahmen ihrer Zuständigkeit zur

Verfügung. Entsprechendes gilt für den Kollegialspruchkörper. Über weitergehende interne Auswertungen können die Leitungen der Gerichte und Staatsanwaltschaften mit den Richterräten und Personalvertretungen Dienstvereinbarungen schließen.

(8) Soweit für die Einrichtung und den Betrieb der IT Auftragsverarbeiter eingeschaltet werden, ist die Einhaltung der Vorschriften dieses Gesetzes sicherzustellen. Bei wesentlichen Veränderungen der Einrichtung oder des Betriebes der IT ist die IT-Kontrollkommission zu beteiligen.

§ 8

Verhältnis zu anderen Regelungen

(1) Den Regelungen dieses Gesetzes entgegenstehende Vorschriften des Bremischen Richtergesetzes, des Bremischen Beamtengesetzes, des Bremischen Personalvertretungsgesetzes sowie die Regelungen des Dataport-Staatsvertrags vom 27. August 2003 (Brem.GBl. 2005, S. 615), der zuletzt durch Staatsvertrag vom 29. November 2019 als Anlage des Gesetzes vom 31. März 2020 (Brem.GBl. S. 193, 194) geändert wurde, bleiben unberührt.

(2) Die Regelungen des zentralen IT-Managements und des zentralen IT-Sicherheitsmanagements der Freien Hansestadt Bremen bleiben unberührt. Bei Regelungswidersprüchen treffen die für das zentrale IT-Management und das zentrale IT-Sicherheitsmanagement zuständige senatorische Behörde und die Senatorin für Justiz und Verfassung oder der Senator für Justiz und Verfassung im Benehmen mit der IT-Kontrollkommission eine Regelung, die die in § 1 Absatz 1 genannten Ziele wahrt.

(3) Die jeweils anwendbaren datenschutzrechtlichen Regelungen bleiben von diesem Gesetz unberührt. Sie finden auf die Verarbeitung personenbezogener Daten vorrangig Anwendung.

(4) Spätestens vier Jahre nach seinem Inkrafttreten überprüft der Senat dieses Gesetz im Hinblick auf seine Anwendung und Auswirkungen. Im Anschluss berichtet der Senat der Bürgerschaft (Landtag) über das Ergebnis der Evaluation nach Satz 1.

§ 9

Inkrafttreten

Dieses Gesetz tritt am Tage nach seiner Verkündung in Kraft.

Signatur

Begründung

zum Entwurf des
Gesetzes über den Einsatz der Informations- und Kommunikationstechnik bei Gerichten und Staatsanwaltschaften in der Justiz der Freien Hansestadt Bremen

(IT-Justizgesetz – ITJG)

A. Allgemeiner Teil

Die Sicherstellung der Unabhängigkeit der Justiz als Dritte Gewalt im Staat mit ihren Ausprägungen der richterlichen Unabhängigkeit, der Sicherstellung des Legalitätsprinzips bei der Staatsanwaltschaft und der Wahrung der sachlichen Entscheidungsunabhängigkeit der Rechtspflegerinnen und Rechtspfleger bedarf im Bereich zentral organisierter elektronischer Datenverarbeitung einer gesetzlichen Absicherung. Das Bundesverfassungsgericht hat in seiner Entscheidung vom 17.01.2013 (Aktenzeichen 2 BvR 2576/11) dargestellt, dass die zentrale elektronische Datenverarbeitung die richterliche Unabhängigkeit nicht beeinträchtigt, wenn die Zugriffsmöglichkeiten der Exekutive gesetzlich beschränkt und deren Überprüfung durch die Judikative sichergestellt ist. Diese Anforderungen werden für die Justiz des Landes Bremen mit diesem Gesetz umgesetzt.

Mit dem Staatsvertrag über die Errichtung von Dataport als rechtsfähige Anstalt des öffentlichen Rechts vom 27. August 2003 (Brem.GBl. 2005, 615), zuletzt geändert durch Staatsvertrag vom 29. November 2019 als Anlage des Gesetzes vom 31. März 2020 (Brem.GBl. S. 193, 194), fungiert der Informations- und Kommunikationsdienstleister Dataport in der Freien Hansestadt Bremen als zentraler IT-Dienstleister für die Gerichte und Staatsanwaltschaften. Diese organisatorische Ausgestaltung hat zur Folge, dass die Gerichte und Staatsanwaltschaften in der Praxis grundsätzlich keine eigene, von der bremischen Landesverwaltung losgelöste IT-Infrastruktur besitzen.

Als Anstalt des öffentlichen Rechts übt Dataport lediglich eine mittelbare Staatsverwaltung aus und unterliegt der gemeinsamen Aufsicht durch die Trägerländer. Die Aufsicht ist dabei strukturell auf eine Rechtmäßigkeitskontrolle beschränkt, da das Landesverwaltungsgesetz für Anstalten des öffentlichen Rechts grundsätzlich keine fachaufsichtliche Steuerung vorsieht. Dementsprechend erfolgt die Lenkung der Aufgabenerfüllung durch Dataport mittels des gesetzlich implementierten Staatsvertrags, Verwaltungsvorschriften sowie konkreten Verträgen.

Die mit dem Gesetz geschaffene IT-Kontrollkommission übt auch die Aufsicht über die datenschutzkonforme Verarbeitung personenbezogener Daten im Bereich der rechtsprechenden Gewalt aus, die von der Aufsicht der Landesdatenschutzbeauftragten nicht erfasst ist.

B. Besonderer Teil zu den einzelnen Bestimmungen

Zu § 1 (Regelungszweck)

Die Vorschrift beschreibt die Ziele und den Regelungsbereich des Gesetzes.

Zu Absatz 1

Es wird zunächst geregelt, dass der Anwendungsbereich des Gesetzes sich nur so weit erstreckt, wie tatsächlich Informations- und Kommunikationstechnik (IT) zur Anwendung kommt. Auf Papierakten, ausgedruckte oder handschriftliche Voten und sämtliche nicht elektronischen Dokumente findet das Gesetz keine Anwendung. Soweit hingegen IT zum Einsatz gelangt, findet das Gesetz umfassend auf alle Systeme, mit denen Daten und Dokumente nach § 3 verarbeitet werden, Anwendung; sowohl die technische Ausgestaltung (z. B. Hardware und Software) als auch die organisatorische Ausgestaltung des Betriebes (z. B. Räume, Personal, Prozesse) sind erfasst. Ferner regelt das Gesetz sowohl die Datenverarbeitung durch externe IT-Dienstleister und Auftragsverarbeiter als auch durch die zuständige Behörde inklusive der IT-Stelle Justiz sowie mit der Datenverarbeitung betraute Beschäftigte der Gerichte und Staatsanwaltschaften selbst, denn auch in diesem Bereich ist das gesetzlich vorgesehene Schutzniveau zu gewährleisten.

Zu gewährleisten ist ferner die Funktionsfähigkeit der Justiz in dem Sinne, dass die verantwortliche Behörde, soweit IT eingesetzt wird, zu gewährleisten hat, dass die benötigten Funktionen und Daten im benötigten und vertraglich zugesicherten Umfang zur Verfügung stehen (Ausfallsicherheit) und ein zielgerichtetes, effizientes und geschütztes Arbeiten (Benutzungsfähigkeit) ermöglicht wird.

Zu Absatz 2

Es handelt sich um eine Ergänzung der Bestimmung des Absatzes 1 Satz 1. Die Vorschrift stellt klar, dass das Gesetz sowohl technisch-organisatorische Maßnahmen regelt als auch rechtliche Rahmenbedingungen für die Nutzung der IT durch die Leitungen der Dienststellen und die zuständige Behörde inklusive der IT-Stelle Justiz setzt.

Zu § 2 (Verantwortlichkeit, Zuständige Behörde)

Die Vorschrift hält die unterschiedlichen Zuständigkeiten bei Organisation und Einsatz der IT fest.

Zu Absatz 1

Geregelt wird die grundsätzliche rechtliche Verantwortung der zuständigen Behörde für den Betrieb und die Organisation der IT. Zudem wird definiert, dass die Senatorin oder der Senator für Justiz und Verfassung die zuständige Behörde im Sinne dieses Gesetzes ist.

Im Geschäftsbereich der Senatorin oder des Senators für Justiz und Verfassung ist die IT-Stelle Justiz als zentrale fachliche Leitstelle für alle Gerichte und Staatsanwaltschaften zuständig. Die Zuständigkeit der IT-Stelle umfasst die Betreuung der Informations- und Kommunikationstechnik der Gerichte und Staatsanwaltschaften, insbesondere die Einführung, Pflege und Begleitung der Weiterentwicklung von Fachverfahren einschließlich der Systeme für den elektronischen Rechtsverkehr, die Betreuung der Anwenderinnen und Anwender, die Einführung der elektronischen Akte sowie die Ausstattung der Dienststellen mit Geräten und Software. Zudem berät die IT-Stelle Justiz bei Bedarf im Rahmen von Gremiensitzungen und koordiniert dienststellenübergreifende IT-Aufgaben für den Justizbereich.

Zu Absatz 2

Der Begriff der Aktenhoheit stellt klar, dass sich hinsichtlich der souveränen Verfügung der Gerichte über die Akten durch die fortschreitende Einführung der bzw. die zunehmende Umstellung auf IT nichts am bisherigen Zustand ändern darf. Der Grundsatz der Aktenhoheit ist ein Strukturelement der gerichtlichen Rechtsschutzgewährung; dementsprechend ist er ein zentraler Maßstab für die Ausgestaltung der gerichtlichen IT. Den Rechtsprechungsorganen muss die souveräne Verfügung über die Akten erhalten bleiben.

Zu Absatz 3

Zentrale Instanz zur Kontrolle der Gewährleistung der Ziele des Gesetzes ist die IT-Kontrollkommission (ITKK), deren Struktur, Aufgaben und Rechte insbesondere in § 4 und § 5 näher beschrieben werden. Die Einrichtung der Kommission setzt die Vorgaben der höchstrichterlichen Rechtsprechung um und dient dem umfassenden Schutz der in § 1 genannten Schutzgüter. Kontrollaufgaben bestehen dabei sowohl gegenüber der zuständigen Behörde, den Gerichtsleitungen, mit der Datenverarbeitung betrauten externen IT-Dienstleistern und Auftragsverarbeitern als auch mit der Datenverarbeitung betrauten Beschäftigten der Gerichte und Staatsanwaltschaften.

Die Vorschrift stellt zudem klar, dass die ITKK in ihrem Wirken Unabhängigkeit genießt; diese Unabhängigkeit erstreckt sich denknotwendig auch auf die jeweiligen Mitglieder der Kommission, soweit sie ihre Aufgaben nach diesem Gesetz wahrnehmen. Sie sind aber an die Vorgaben dieses Gesetzes gebunden, etwa was Vertraulichkeit und Verschwiegenheit betrifft.

Zu § 3 (Zu schützende Daten und Prozesse)

Die Norm konkretisiert, welche Daten und Abläufe auf welchem Niveau zu schützen sind. Sie ist eine der zentralen Vorschriften des Gesetzes.

Zu Absatz 1

Die Vorschrift definiert den sachlichen Schutzbereich des Gesetzes und greift dabei die Bestimmungen des § 1 auf. Geschützt sind im richterlichen, staatsanwaltlichen und rechtspflegerischen Bereich grundsätzlich alle Entscheidungen sowie insbesondere

deren Vorbereitung. Der Begriff der Vorbereitung ist dabei im weitesten Sinne zu verstehen. Alle vorbereitenden Arbeiten, seien es angefertigte Auswertungen von Literatur und Rechtsprechung, Notizen zu Dokumenten, Entscheidungs- oder Verfügungsentwürfe, Verfügungen, Voten – für die Bearbeiterin oder den Bearbeiter und / oder Dritte – oder sonstige der Vorbereitung dienende Dokumente und Prozesse, zählen dabei zum Bereich der Entscheidungsfindung. Entscheidung im Sinne der Vorschrift sind auch Zwischenentscheidungen. Zum staatsanwaltlichen Bereich gehört auch die Tätigkeit der Amtsanwältinnen und Amtsanwälte.

Zu Absatz 2

Die Vorschrift konkretisiert, welche Daten im Rahmen der in Absatz 1 beschriebenen Entscheidungsprozesse regelmäßig anfallen, da sie entweder der Entscheidungsfindung zugrunde liegen bzw. für die Entscheidungsfindung oder Verfahrensbearbeitung aus den zugrunde liegenden Daten weiterverarbeitet (z. B. verdichtet oder extrahiert) oder im Verlauf der gerichtlichen oder staatsanwaltschaftlichen Verfahrensbearbeitung durch Beschäftigte oder (automatisiert) durch IT-Systeme der Justiz erzeugt werden. Dabei wird unterschieden zwischen

- Inhaltsdaten: Inhaltsdaten werden in der Regel zur Durchdringung des juristischen Sachverhalts benötigt. Hierbei handelt es sich in erster Linie um Dokumente (Schriftsätze aller Art) der Verfahrensbeteiligten oder Dritter (z. B. Ermittlungsakten, Beiakten), die über elektronische Eingangskanäle bei Gericht oder bei der Staatsanwaltschaft eingereicht oder über Briefpost, Telefax oder persönliches Erscheinen eingereicht und für die elektronische Bearbeitung bei Gericht oder bei der Staatsanwaltschaft digitalisiert (gescannt) werden, oder um Dokumente, die im Rahmen der Verfahrensbearbeitung erzeugt werden und zur Verfahrensakte gelangen (z. B. Verfügungen, Urteile, Beschlüsse). Zu den Inhaltsdaten gehören auch die mit den o.g. Dokumenten verbundenen Daten der qualifizierten elektronischen Signaturen, da diese die handschriftliche Unterschrift der die jeweiligen Inhalte verantwortenden Personen abbilden, sowie die bei der maschinellen Verarbeitung erzeugten Prüfprotokolle und Transfervermerke, welche inhaltliche Aussagen über den frist- und formgerechten Zugang der o.g. Dokumente bzw. über deren gesetzeskonforme Umwandlung enthalten. Auch auf den o.g. Dokumenten angebrachte Annotationen (z. B. elektronische Kommentare oder Unterstreichungen) werden zu Inhaltsdaten, sofern diese nicht nur temporär zum Zwecke der persönlichen Durchdringung des Sachverhaltes angebracht werden, sondern mit dem jeweiligen Dokument revisionssicher zur Akte gelangen sollen.

- Metadaten: In zweiter Linie können den o.g. Dokumenten durch die Einreicherin oder den Einreicher selbst oder bei der weiteren Verarbeitung bei Gericht oder Staatsanwaltschaft sog. Metadaten beigefügt werden. Metadaten sind strukturierte maschinenlesbare Datensätze, welche Informationen über Merkmale der o. g. Dokumente enthalten, wie zu deren Inhalt (z. B. Aktenzeichen, Name der Klägerin oder des Klägers- und Beklagtenname; vgl. z. B. § 2 Abs. 3 der Verordnung über die technischen Rahmenbedingungen des elektronischen Rechtsverkehrs und über das besondere elektronische Behördenpostfach [Elektronischer-Rechtsverkehr-Verordnung - ERVV])

oder zu der Struktur (z. B. Reihenfolge, Inhaltsverzeichnis, Anlagen) von mehreren Dokumenten eines Schriftsatzes oder einer Akte.

- Verfahrensbezogene Daten: Hierbei handelt es sich um manuell oder automatisiert erfasste oder weiterverarbeitete fachliche Daten, die zur Verwaltung der gerichtlichen oder staatsanwaltschaftlichen Verfahren oder der Akten benötigt werden, z. B. Anschriften der Verfahrensbeteiligten, den Verfahrensstand, die Benennung des Verfahrensgegenstandes, Fristen und Termine (z. B. Gerichtsverhandlungen), Verweise auf Akten, Schriftsätze oder Beweismittel, Eingangs- und Erledigungsdaten, die Art der Erledigung, das Aktenzeichen, das Erstellungsdatum oder die Aufbewahrungsdauer einer Akte etc.

- Logdaten: Hierbei handelt es sich um das automatisch geführte Protokoll bestimmter technischer Aktionen auf einem IT-System. Protokolldaten werden in der Regel erhoben, um Fehler oder Missbrauch erkennen, vermeiden oder aufklären zu können (z. B. unerlaubtes Eindringen in ein IT-System) oder um im Fall eines Fehlers oder eines unerwünschten Ergebnisses die Rücksetzung auf einen früheren Stand zu erlauben (z. B. „Rückgängig“-Aktion bei einem Schreibprogramm).

Zu Absatz 3

Für bestimmte Inhaltsdaten besteht die Notwendigkeit eines gesteigerten Schutzes.

Besonders zu schützen sind alle Daten, die den Prozess der Entscheidungsfindung in irgendeiner Weise dokumentieren, also Entscheidungsentwürfe, Entwürfe zu Verfügungen, Voten sowie alle der Vorbereitung dienenden Arbeiten wie Strukturierungsvorgänge, Recherchen und als persönlich gekennzeichnete Annotationen; dieser Bereich stellt – insbesondere bei der richterlichen, staatsanwaltschaftlichen und rechtspflegerischen Tätigkeit – den Kern der zu schützenden Güter dar. Einflüsse auf die Entscheidungsfindung müssen vermieden werden, was auch durch den Schutz „vorbereitender“ Dokumente erfolgt. Gewährleistet wird dies insbesondere durch §§ 6, 7 dieses Gesetzes, welche die technischen, betrieblichen und organisatorischen Maßnahmen sowie die Behandlung der Daten und Prozesse im Anwendungsbereich von § 3 regeln.

Zu § 4 (IT-Kontrollkommission)

Die Vorschrift regelt Einrichtung, Zusammensetzung, Arbeitsweise und Rechte der ITKK.

Absatz 1

Die Einrichtung der ITKK bei der zuständigen Behörde ist lediglich als organisatorische Anbindung zu verstehen und beschränkt die Unabhängigkeit der ITKK und ihrer Mitglieder nicht. Mit dieser Anbindung im Zusammenhang steht die Verpflichtung der zuständigen Behörde, der ITKK die nötigen Arbeitsmittel – insbesondere finanzielle

Ressourcen – zur Verfügung zu stellen. Zu den notwendigen Kosten der IT-Kontrollkommission zählen in diesem Zusammenhang insbesondere Kosten für notwendige Reisen oder Fortbildungen der Mitglieder sowie Teil-Freistellungen der Mitglieder von ihren sonstigen Regelaufgaben.

Die Mitglieder der IT-Kontrollkommission sollen nach Möglichkeit über ein gewisses technisches Grundverständnis verfügen oder jedenfalls bereit sein, sich dieses im Rahmen ihrer IT-Kontrollkommissionstätigkeit zu erwerben.

Zu Absatz 2

Hier wird die Besetzung der ITKK mit stimmberechtigten Mitgliedern festgelegt. Insgesamt besteht die ITKK aus vier stimmberechtigten Mitgliedern. Ausgangspunkt für die Schaffung der IT-Kontrollkommission ist die sog. „hessische Netzklage“, im Rahmen derer das Bundesverfassungsgericht bestimmte Grundlagen für die IT-Nutzung zur Absicherung der richterlichen Unabhängigkeit bestätigt hat. Daher wird dieser Schwerpunkt auch in der Stimmenverteilung berücksichtigt. Jedes der beiden richterlichen Mitglieder hat zwei Stimmen, die es nur einheitlich für oder gegen einen Entscheidungsvorschlag abgeben kann; eine Aufteilung der beiden Stimmen ist nicht zulässig. Die übrigen Mitglieder haben jeweils eine Stimme. Insgesamt können damit sechs Stimmen (vier richterliche und zwei nichtrichterliche Stimmen) abgegeben werden. Die richterlichen Mitglieder können unabhängig voneinander für oder gegen einen Entscheidungsvorschlag stimmen. Möglich ist es deshalb auch, dass z. B. ein richterliches Mitglied gemeinsam mit einem anderen Mitglied für einen Entscheidungsvorschlag und das andere richterliche Mitglied mit einem anderen Mitglied dagegen stimmt. Auch kann sich jedes Mitglied seiner Stimmen bzw. seiner Stimme enthalten. Das höhere Stimmgewicht der richterlichen Mitglieder stellt sicher, dass die Richterinnen bzw. Richter in der ITKK Entscheidungen herbeiführen können, ohne die nichtrichterlichen Mitglieder für ihren Standpunkt gewinnen zu müssen. Das unterschiedliche Stimmengewicht schützt die richterliche Unabhängigkeit und ermöglicht eine den Ressourcen des Landes Bremen angemessene Größe der Kommission.

Zu Absatz 3

Absatz 3 regelt die Besetzung mit drei beratenden Mitgliedern ohne Stimmrecht. Die beratenden Mitglieder sollen die Kommission einerseits als „Sachverständige“ in die Lage versetzen, Sachverhalte und Hintergründe aufzuklären. Andererseits sollen sie als Schnittstellen zu den Verantwortlichen für eine schnelle und unkomplizierte Kommunikation zu den für die IT-Infrastruktur verantwortlichen Behörden dienen.

Zu Absatz 4

Absatz 4 regelt die Art und Weise der Wahl der ITKK-Mitglieder sowie deren Stellvertretungen.

Zu Absatz 5

Der Absatz regelt die Amtszeit sowie das Vorgehen bei vorzeitigem Ausscheiden eines oder mehrerer Mitglieder. Zudem wird die Benennung der beratenden Mitglieder geregelt.

Zu Absatz 6

Die Vorschrift regelt die Beschlussfassung in der ITKK. Sie vermeidet im Zusammenspiel mit Absatz 2 das Auftreten etwaiger Zweifelsfragen. Dies gilt etwa im Zusammenhang mit Stimmenthaltungen, die zulässig sind. Erhält ein Entscheidungsvorschlag nicht die Mehrheit der Stimmen der stimmberechtigten Mitglieder, ist der Vorschlag nicht angenommen.

Zu Absatz 7

Die Vorschrift dient dazu, dass der Sachverstand der Leitungen der Gerichte und Staatsanwaltschaften bei Bedarf nutzbar gemacht werden kann. Die Vorschrift ist als Minderheitsrecht ausgestaltet. Die Vertreterin oder der Vertreter der Leitung muss nicht zwingend ein Mitglied der Leitung selbst sein; die Leitungen der Gerichte und Staatsanwaltschaften können im Einzelfall oder generell geeignete Vertreterinnen oder Vertreter für diese Zwecke bestimmen. Die Hinzuziehung erfolgt zur Beratung konkreter Vorgänge ohne Stimmrecht.

Zu Absatz 8

Der Absatz enthält eine Verordnungsermächtigung für die zuständige Behörde. Potentiell zu regelnde Materien sollen mit Blick auf die nötige Flexibilität im Verordnungswege erfolgen. Geregelt werden können Einzelheiten insbesondere zu folgenden Bereichen:

- Wahl und Amtszeit der stimmberechtigten Mitglieder: Hier kann beispielsweise geregelt werden, dass die Mitglieder der ITKK nach Ende der Amtszeit im Amt bleiben, bis neue Mitglieder gewählt sind. Ferner können Regelungen zum Umgang mit fehlerbehafteten Wahlen, zu Elternzeiten, Mutterschutz, etc. getroffen werden.
- Bestimmung der beratenden Mitglieder
- Beschlussfassung der ITKK: Geregelt werden könnten z.B. Ladungsfristen vor Beschlüssen oder die Möglichkeit der Beschlussfassung im Umlaufverfahren.

Zu Absatz 9

Die ITKK ist verpflichtet, die Einzelheiten ihrer Arbeitsweise durch eine Geschäftsordnung zu regeln; diese Verpflichtung dient der Sicherstellung effizienter Arbeit.

Überdies wird es der ITKK ermöglicht, einzelne Aufgaben oder Befugnisse generell oder im Einzelfall durch – grundsätzlich jederzeit widerrufbaren – Beschluss auf einzelne Mitglieder oder auch mehrere einzelne Mitglieder zu übertragen. Auch dies dient

der Verbesserung der Arbeitsfähigkeit. Näheres kann und sollte in der Geschäftsordnung geregelt werden.

Zu Absatz 10

Die ITKK ist verpflichtet, ihre Arbeit und die gewonnenen Erkenntnisse sowie erzielte Ergebnisse so zu dokumentieren, dass eine Dritte oder ein Dritter in die Lage versetzt wird, die Arbeit, den Arbeitsumfang und den jeweils aktuellen Kenntnis- und Ergebnissachstand ohne weiteres nachzuvollziehen. Die Dokumentation ist jederzeit auf Verlangen an die zuständige Behörde oder die Richter- und Personalvertretungen herauszugeben. Die Angabe eines Grundes für die Einsichtnahme ist hierbei nicht notwendig.

Zu § 5 (Kontrollrechte der IT-Kontrollkommission)

Die Vorschrift regelt die Rechte und Pflichten der ITKK.

Zu Absatz 1, 2 und 3

Konstituiert wird ein umfassendes Zutritts-, Auskunfts- und Einsichtsrecht der ITKK hinsichtlich aller Datenverarbeitungsvorgänge, vertraglichen Regelungen, Konzepten, der Infrastruktur und Einrichtungen gegenüber dem zentralen IT-Dienstleister Dataport, allen weiteren IT-Dienstleistern, Auftragsverarbeitern, den in der Datenverarbeitung tätigen Dienststellen der Justiz, dem zuständigen Ressort für zentrale IT-Angelegenheiten (dem Senator oder der Senatorin für Finanzen) sowie gegenüber der zuständigen Behörde, auch unabhängig von konkreten Anlässen. Dieses Recht ist zur Wahrnehmung der Aufgaben unerlässlich und darf grundsätzlich nicht beschränkt werden. Administratorinnen und Administratoren im Sinne des Gesetzes sind primär Beschäftigte der in der Datenverarbeitung tätigen IT-Dienstleister, Auftragsverarbeiter sowie der zuständigen Behörde, die zwecks der Organisation oder des Betriebes der zur Verarbeitung von Daten und Dokumenten nach § 3 genutzten IT-Systeme über technische Berechtigungen verfügen.

Inhaltliche Beschränkungen ergeben sich einerseits lediglich im Hinblick auf die Einsichtnahme in und die Verwendung von personenbezogenen Daten, die nur zulässig sind, wenn sie für die Erfüllung der Kontrollaufgaben der ITKK nach Absatz 1 unerlässlich sind (Absatz 2). Eine inhaltliche Beschränkung ergibt sich andererseits außerhalb von Kontrollen nach Absatz 1 vor allem im Hinblick auf die durch § 3 Absatz 3 besonders geschützten Daten und Prozesse, bei denen ein Erforderlichkeitsvorbehalt konstituiert wird. Erforderlich im Sinne der Vorschrift können aber zum Beispiel auch verdachtsunabhängige Routinekontrollen sein.

Die Gewährung dieser umfangreichen und generell nicht bzw. wenig beschränkten Einsichtsrechte schließt es allerdings nicht aus, dass besonders schutzwürdige Daten geschwärzt werden können; der Fokus der Arbeit der ITKK liegt in der Kontrolle der ordnungsgemäßen Datenverarbeitung und der Sicherstellung der Unabhängigkeit der genannten Berufsgruppen.

Nach Absatz 3 Satz 3 besteht ein Auskunftsrecht der ITKK gegenüber externen IT-Dienstleistern, Auftragsverarbeitern, der zuständigen Behörde sowie den mit der Verarbeitung von Justizdaten betrauten Beschäftigten und nach Absatz 4 Satz 1 ein Recht auf Hinzuziehung sachkundiger Dritter, auch aus den Gerichtsverwaltungen oder der zuständigen Behörde. Eine Erforderlichkeit zur Hinzuziehung kann sich z. B. ergeben, wenn die sachkundigen Beschäftigten mangels entsprechender Ressourcen keine Zeit für eine sachgerechte bzw. zeitnahe Beratung der ITKK finden, wenn keine Kapazitäten für eine mehrtägige Kontrolle vorhanden sind.

Zu Absatz 4

Es wird hier einerseits eine Vorgabe hinsichtlich der Arbeitsweise der ITKK gemacht, andererseits werden der ITKK Kompetenzen eingeräumt. Auch die Arbeit einer Kontrollkommission hat sich an die Haushaltsgrundsätze der der Wirtschaftlichkeit und Sparsamkeit (§ 7 LHO) zu halten. Vor der kostenauslösenden Beauftragung externer Sachverständiger sind sachkundige Beschäftigte wie beispielsweise der oder die behördliche Datenschutzbeauftragte, der oder die Informationssicherheitsbeauftragte des Ressorts oder Mitarbeiter:innen der IT-Stelle Justiz einzubinden. Auch die fachliche Kompetenz der Landesbeauftragten für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen oder des zentralen IT-Managements der Senatorin oder des Senators für Finanzen kann bei Bedarf von der Kontrollkommission zu Rate gezogen werden. Die Heranziehung externen Sachverstandes muss erforderlich sein und begründet werden, bedeutet aber nicht, dass die ITKK bei der Sachverhaltsermittlung der Entscheidungsgewalt der zuständigen Behörde unterworfen wäre. Es wird davon ausgegangen, dass die Mitglieder der IT-Kontrollkommission in erster Linie die Kontrollaufgaben selbst und persönlich wahrnehmen. Die Hinzuziehung interner oder externer sachkundiger Dritter sollte demnach nicht den Regelfall, sondern die Ausnahme darstellen. Im Zuge der in § 8 Abs. 4 geregelten Evaluation des Gesetzes besteht zudem die Möglichkeit, etwaigen Anpassungsbedarf zu prüfen.

Zu Absatz 5

Die Vorschrift regelt Unterrichtungspflichten der ITKK bei der Feststellung von Verstößen sowie ferner weitere Rechte. Die Unterrichtung der Betroffenen steht im pflichtgemäßen Ermessen der ITKK. So hat sie je nach den Umständen die berechtigten Interessen der Betroffenen an einer Unterrichtung mit den Belangen einer erfolgreichen Umsetzung der Kontrollmaßnahme abzuwägen.

Der ITKK werden keine exekutiven Befugnisse verliehen. Die zuständige Behörde ist aber zu einer angemessenen Reaktion auf Beanstandungen verpflichtet. Das Spektrum angemessener Reaktionen umfasst eine Vielzahl denkbarer Maßnahmen, etwa die Geltendmachung vertraglicher Ansprüche gegenüber externen Datenverarbeitern bis hin zur Kündigung, die Einleitung strafrechtlicher oder ggfs. dienstaufsichtsrechtlicher Verfahren, Abmahnungen etc.

Zu Absatz 6

Die Vorschrift begründet das Recht für Beschäftigte der Dienststellen der Justiz, Personal- und Richterräte sowie Dienststellenleitungen, sich mit konkreten Anliegen an die ITKK zu wenden. Die Gewährung dieses Rechts dient nicht nur den Interessen der Berechtigten, sondern auch der Effektivität der Arbeit der ITKK. Aufsichts- und Kontrollinstanzen gewinnen in der Regel einen nennenswerten Teil ihrer relevanten Erkenntnisse aus Meldungen Dritter.

Zu Absatz 7

Die Mitglieder der ITKK sind grundsätzlich entweder (teilweise) von ihrer dienstlichen Tätigkeit freizustellen oder angemessen für ihren Aufwand zu entschädigen. Die Entscheidung darüber, welche Mitglieder in welchem Umfange freigestellt werden, trifft die zuständige Behörde. Sie hat dabei die Gewährleistung der Arbeitsfähigkeit der ITKK sicherzustellen, aber auch die Haushaltsgrundsätze der Wirtschaftlichkeit und Sparsamkeit zu beachten. Eine Freistellung von insgesamt 30 Arbeitstagen pro Jahr (15%) und Mitglied erlaubt jährlich 4 Prüfungen mit einer Dauer von 1 Woche pro Prüfung (1 Tag Prüfung, 4 Tage Vor- und Nachbereitung) sowie zusätzlich noch anlassbezogene Prüfungen sowie notwendige Schulungen und Fortbildungen im Umfang von jeweils ca. 5 Tagen pro Jahr. Hinzu kommt der Aufwand auf Seiten der IT-Stelle oder der IT-Sicherheitsbeauftragten / des IT-Sicherheitsbeauftragten, die Anliegen der ITKK zu bearbeiten und zu beantworten.

Zu § 6 (Technische, betriebliche und organisatorische Maßnahmen)

Die Vorschrift trifft Regelungen technisch-organisatorischer und betrieblicher Art.

Zu Absatz 1

Die allgemeinen Grundsätze der Datensparsamkeit und Datenvermeidung gelten auch im Regelungsbereich dieses Gesetzes. Es ist nur das an Daten zu erfassen, was zur Erledigung einer Fachaufgabe und zum sicheren, effizienten, barrierefreien und ergonomischen Betrieb der IT erforderlich ist.

Adressat dieser Vorschrift sind die in der Datenverarbeitung tätigen IT-Dienstleister, Auftragsverarbeiter sowie die zuständige Behörde und in der Datenverarbeitung tätige Dienststellen.

Diese Stellen haben, so der weitere Regelungsgehalt der Vorschrift, immer eine sichere Verarbeitung anhand des Standes der Technik zu gewährleisten. Zu diesem Zweck müssen gegebenenfalls, wenn sich sicherheitsrelevante technische Neuerungen oder Probleme ergeben, Soft- und ggfs. auch Hardware sowie betriebliche Prozesse entsprechend angepasst werden.

Zu Absatz 2

Eingriff im Sinne des Gesetzes ist dabei im weitesten Sinne zu verstehen. Der Begriff beschreibt in technischer Hinsicht jede denkbare, über bloße Einsichtnahme hinausgehende Art, mit einem Datum umzugehen, einschließlich seiner Veränderung, unabhängig davon, wer ihn vornimmt.

Daneben bezeichnet er Eingriffe im allgemeinen Sprachgebrauch, also Einwirkungen auf Prozesse, etwa der Entscheidungsfindung.

Zu Absatz 3

Diese Vorschrift richtet sich an die in der Datenverarbeitung tätigen Mitarbeiter:innen mit Administrationsrechten. Eine revisionssichere Protokollierung eines administrativen Zugriffs liegt dann vor, wenn in nicht veränderbarer Weise protokolliert ist, mit welcher administrativen Kennung auf welches IT-System (z.B. eine Serveranwendung, eine Datenbank oder ein Endgerät wie ein PC oder ein Notebook) zu welchem Zeitpunkt zugegriffen wird. Die Protokollierung kann dabei (abhängig vom Einsatz der Administratorin beziehungsweise des Administrators und dem IT-System, auf das zugegriffen wird) auf unterschiedliche Weise erfolgen, etwa als Aufzeichnung der Aktivitäten der Administratorin oder des Administrators (z.B. durch Videoprotokollierung), als Papierdokument mit Abzeichnung durch die oder den Zugreifenden und unmittelbar Berechtigten i.S.v. § 3 Absatz 5 oder durch IT-interne (organisatorische) Kontrollmechanismen wie etwa ein 4-Augen-Prinzip (Unterschriften von zwei Administratorinnen oder Administratoren). Nähere Vorgaben für die Protokollierung in Abhängigkeit davon, auf welches IT-System zugegriffen wird, können mittels Rechtsverordnung erlassen werden. Soweit die oder der unmittelbar Berechtigte einwilligt, ist eine Protokollierung nicht zwingend erforderlich. Dies deckt in erster Linie die Hilfestellung einer Administratorin oder eines Administrators beim Benutzer:innensupport ab, der in der Regel unter Aufsicht und mit Willen des Berechtigten erfolgt. Soweit mit vertretbarem Aufwand möglich, soll die Zustimmung der oder des unmittelbar Berechtigten protokolliert werden.

Zu Absatz 4

Die Schutzziele des Gesetzes können nur dann erreicht werden, wenn – nie auszuschließende – Ereignisse oder Prozesse, die den Zielen zuwiderlaufen, auch bekannt werden, damit reagiert werden kann. Daher ist jede / jeder aufgerufen, Verstöße zu melden. Wer Kenntnis von einem sicherheitsrelevanten Ereignis erlangt, hat dieses binnen angemessener Frist den genannten Stellen mitzuteilen. Die Beurteilung der Frage, ob es sich um ein sicherheitsrelevantes Ereignis handelt, sowie die Angemessenheit der Meldefrist haben sich in erster Linie am Gewicht des Vorfalles und der daraus resultierenden Konsequenzen (z. B. Schadenseintritt, Anzahl der Betroffenen, Schwere der Folgen) zu orientieren. Es bietet sich an, die Art der möglichen Ereignisse (z. B. unbefugte Zugriffe im Einzelfall, generelle Sicherheitslücken oder andere Gefährdungen und die Zuordnung der auszuführenden Handlungen) in einer ergänzenden Rechtsverordnung zu regeln, um einer Überflutung mit irrelevanten Meldungen

geeignet vorzubeugen bzw. die Meldungen in Bezug auf ggf. erst zukünftig entstehende Risikobereiche in geeigneter Weise anpassen zu können.

Zu § 7 (Behandlung der Daten und Prozesse)

Die Vorschrift regelt umfassend die „rechtliche Berechtigung“ im Hinblick auf die Schutzgüter des § 3 und stellt damit eine weitere zentrale Norm des Gesetzes dar. Sie bestimmt die unmittelbar Berechtigten und regelt weitere Fälle der Berechtigung.

Zu Absatz 1

Die Vorschrift stellt klar, dass nur (rechtlich) Berechtigte Daten im Sinne des § 3 einsehen und in diese Daten oder in § 3 geschützte Prozesse eingreifen dürfen.

Zu Absatz 2

Absatz 2 regelt inhaltlich, wer primär berechtigt ist. Dies sind die Amtsträgerinnen und Amtsträger der Gerichte und Staatsanwaltschaften, welche das jeweilige Verfahren im Rahmen ihrer Zuständigkeit bearbeiten.

Zu Absatz 3

Absatz 3 stellt klar, dass sich weitere Berechtigungen für Amtsträgerinnen und Amtsträger der Gerichte und Staatsanwaltschaften, Beschäftigte der in der Datenverarbeitung tätigen IT-Dienstleister und Auftragsverarbeiter sowie die zuständige Behörde ergeben können. Diese folgen aus der Einwilligung der in Absatz 2 genannten primär Berechtigten, gesetzlichen Vorschriften, der Dienstaufsicht sowie technischen Erfordernissen des IT-Betriebs.

Technische Erfordernisse sind insbesondere dann gegeben, wenn ein Eingriff zur Aufrechterhaltung der Funktionsfähigkeit (hierzu gehören auch notwendige Maßnahmen im Bereich der IT-Sicherheit, wie z. B. die Prüfung auf Schadsoftware oder die Herstellung von Datensicherungen) notwendig ist. Absatz 3 stellt auch für die Belange der Dienstaufsicht eine Rechtsgrundlage für Einsichten und Eingriffe dar. Dies betrifft etwa die Einsichtnahme in elektronische Verfahrensakten (Inhalts-/Meta- und Verfahrensdaten) im Zusammenhang mit Disziplinarverfahren und zur Erteilung dienstlicher Beurteilungen.

Zu Absatz 4

Satz 1 regelt die Befugnis für Einsichten und Eingriffe für den Fall, dass eine Berechtigung nach den Absätzen 2 oder 3 nicht vorliegt. Sie setzt grundsätzlich eine vorherige einzelfallbezogene Genehmigung der IT-Kontrollkommission voraus. Gefahr im Verzug meint eine unmittelbar bevorstehende Gefahr für die Schutzgüter des § 1 Abs. 1 und des § 3 und kommt insbesondere dann zum Tragen, wenn durch unerlaubte Zugriffe eine Gefahrensituation bevorsteht, die zur Abwendung der Gefahr ein sofortiges Handeln erfordert.

Zu Absatz 5

Die Vorschrift dient der besseren Kontrolle der in der Datenverarbeitung tätigen Auftragsverarbeiter, welche Daten der Justiz verarbeiten und hierdurch über technische Eingriffsmöglichkeiten verfügen. Unabhängig davon, ob eine entsprechende vertragliche Vereinbarung getroffen wurde, sind die Vorgaben des Art. 5 Abs. 1 Buchstabe c DSGVO zu beachten („Datenminimierung").

Zu Absatz 6

Der Absatz stellt klar, dass eine Weitergabe der genannten Daten an unberechtigte Stellen durch die zuständige Behörde unzulässig ist und die Daten ausschließlich zweckgebunden für den Betrieb der IT-Fachverfahren genutzt werden. Auch Verhaltens- oder Leistungskontrollen aufgrund der gewonnenen Daten sind ausdrücklich untersagt. Hingewiesen sei auf einen Beschluss des BVerfG, wonach ein teilweiser Zugriff auch auf richterliche Daten im Rahmen der Dienstaufsicht zulässig ist. Das BVerfG führt aus: „Auch die Speicherung und Weitergabe sogenannter Metadaten richterlicher Dokumente wie Autor und Erstellungszeitpunkt sind unzulässig, soweit nicht der konkrete Verdacht eines Missbrauchs des EDV-Netzes zu dienstfremden Zwecken besteht." (BVerfG, Nichtannahmebeschluss vom 17. Januar 2013 – 2 BvR 2576/11 –, juris, Rn. 10).

Zu Absatz 7

Hier wird die Zulässigkeit der Datenerhebung im richterlichen Bereich geregelt. Es wird hierbei sichergestellt, dass der Schutz der richterlichen Unabhängigkeit vor unzulässiger Kontrolle eingehalten wird, indem möglichst nur aggregierte Daten genutzt werden, welche keinen Rückschluss auf die Tätigkeit einzelner Richterinnen und Richter zulassen. Die aggregierten Daten dürfen auch nicht für Beobachtungs- und Kontrollzwecke genutzt werden.

Zu Absatz 8

Da externe IT-Dienstleister und Auftragsverarbeiter nicht zwingend ihren Sitz in Bremen haben und auf sie möglicherweise – wie im Falle von Dataport, das nach § 1 Absatz 2 Satz 3 des Dataport-Staatsvertrages schleswig-holsteinischem Recht unterliegt – bremisches Landesrecht nicht anwendbar ist, muss die Einhaltung der Vorschriften des Gesetzes mitunter gesondert sichergestellt werden. Das heißt, soweit dieses Gesetz nicht direkt gilt, müssen seine Regelungen vertraglich umgesetzt werden.

Zu § 8 (Verhältnis zu anderen Regelungen)

Die Norm regelt das Verhältnis des Gesetzes zu anderen Gesetzen, Vorschriften und Regelungen.

Zu Absatz 1

Die Regelung bestimmt, dass den Regelungen dieses Gesetzes entgegenstehende landesgesetzliche Vorschriften und solche des Dataport-Staatsvertrages unberührt bleiben. Das Gesetz soll im Rahmen der bereits bestehenden gesetzlichen und untergesetzlichen Regelungen dafür Sorge tragen, dass hierbei die richterliche Unabhängigkeit, das Legalitätsprinzip der Staatsanwaltschaft und die sachliche Unabhängigkeit der Rechtspflegerinnen und Rechtspfleger gewährleistet bleiben und dass dies durch Kontrollen der IT-Kontrollkommission überprüft werden kann. Die Regelungen des Dataport-Staatsvertrages sind für das Land Bremen bindend; sie können und sollen durch dieses Gesetz nicht beschränkt oder verändert werden.

Zu Absatz 2

Die Regelung dient der Klarstellung, dass die zentralen Regelungen des IT-Managements und des zentralen IT-Sicherheitsmanagements der Freien Hansestadt Bremen von der zuständigen Behörde anerkannt werden. Sollte es zu Regelungswidersprüchen im Einzelfall kommen, werden die Senatorin oder der Senator für Finanzen und die zuständige Behörde im Benehmen mit der ITKK ggf. eine Sonderregelung treffen oder einen Dispens erteilen. Die Regelungen des zentralen IT-Managements erweitern nicht die Zugriffsmöglichkeiten der Exekutive. Durch die zentralen Regelungen des IT-Managements werden Sicherheitsstandards geschaffen und umgesetzt, welche u.a. den unbefugten Zugriff auf Daten verhindern sollen (z. B. durch eine Passwort-Sicherheitsrichtlinie). Sie schützen den richterlichen Bereich vor unzulässiger Einsichtnahme und Beeinflussung.

Zu Absatz 3

Absatz 3 stellt klar, dass es sich bei Vorschriften dieses Gesetzes nicht um datenschutzrechtliche Vorschriften handelt. Vielmehr werden durch dieses Gesetz ausschließlich technische, betriebliche und organisatorische Maßnahmen und damit technische Sicherheitsstandards zum Schutz der richterlichen, staatsanwaltschaftlichen und rechtspflegerischen Tätigkeit festgeschrieben. Das IT-Justiz-Gesetz trifft damit keine Regelungen, die gesetzlichen datenschutzrechtlichen Regelungen zuwiderlaufen, sondern schützt im Einklang mit geltendem Datenschutzrecht die richterliche Unabhängigkeit. Datenschutzrechtliche Regelungen schützen nicht nur die Daten von externen Personen, sondern dienen auch dem Schutz der Daten der Richterschaft.

Zu Absatz 4

Die Evaluationsverpflichtung trifft den Senat. Die Überprüfung hat spätestens vier Jahre nach dem Inkrafttreten zu beginnen, der Senat kann sie aber, wenn ihm das tunlich erscheint, auch früher einleiten.

Zu § 9 (Inkrafttreten)

Die Norm regelt das Inkrafttreten des Gesetzes.