Gesetzblatt der Freien Hansestadt Bremen

2022	Verkündet am 20. Dezember 2022	Nr. 157

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

Vom 13. Dezember 2022

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.

Bremen, den 13. Dezember 2022

Der Senat