Schleswig-Holsteinischer Landtag

Umdruck 18/5724

01.03.2016

Vorlage für die Sitzung des Innen- und Rechtsausschusses

am 02.03.2016

Änderungsantrag

der Fraktion der PIRATEN

Entwurf eines IT-Gesetzes für die Justiz des Landes Schlewig-Holstein (IT-Justizgesetz - IT JG)

zu Drucksache 18/3224

Der Landtag wolle beschließen:

Der Gesetzentwurf der Landesregierung wird mit den folgenden Änderungen angenommen:

Gesetzentwurf der Landesregierung:	Änderungsantrag:

§ 2 Besondere Belange der Justiz	
(2) Die IT-Strukturen der Gerichte und Staatsanwaltschaften sind von denen der Landesverwaltung technisch zu trennen. Soweit die in den Gerichten und Staatsanwaltschaften zum Einsatz kommende IT von den in § 1 Absatz 1 genannten Stellen bereitgestellt und betreut wird, ist unter Beachtung des Stands der Technik, insbesondere der nachfolgenden Maßgaben sicherzustellen, dass jeglicher Einblick in die richterliche, rechtspflegerische oder staatsanwaltliche Tätigkeit unterbleibt: 1. Es sind berechtigte Inhaberinnen und Inhaber administrativer Zugänge zu bestimmen; die Bedingungen einer darüber hinaus erforderlichen Öffnung für weitere administrativ berechtigte Personen sind festzulegen; für den Fall einer unbefugten Öffnung ist eine Information der IT-Kontrollkommission (§ 5) und der betroffenen Gerichte und Staatsanwaltschaften sowie ein Verfahren zur Änderung der Zugangsgewährung vorzusehen; 2. die im Rahmen richterlicher, rechtspflegerischer oder staatsanwaltlicher Tätigkeit erstellten Dokumente dürfen von den Administratorinnen und Administratoren weder eingesehen noch an Dritte weitergegeben werden, insbesondere nicht an die in § 1 Absatz 1 genannten Stellen oder an die diesen nachgeordneten Stellen der Dienstaufsicht; 3. in gleicher Weise ist eine Weitergabe von Informationen über Merkmale oder Eigenschaften von den in Nummer 2 genannten	(2) Die IT-Strukturen der Gerichte und Staatsanwaltschaften sind von denen der Landesverwaltung technisch zu trennen. Soweit die in den Gerichten und Staatsanwaltschaften zum Einsatz kommende IT von den in § 1 Absatz 1 genannten Stellen bereitgestellt und betreut wird, ist unter Beachtung des Stands der Technik, insbesondere der nachfolgenden Maßgaben sicherzustellen, dass jeglicher Einblick in die richterliche, rechtspflegerische oder staatsanwaltliche Tätigkeit unterbleibt: 1. Es sind berechtigte Inhaberinnen und Inhaber administrativer Zugänge zu bestimmen; die Bedingungen einer darüber hinaus erforderlichen Öffnung für weitere administrativ berechtigte Personen sind festzulegen; für den Fall einer unbefugten Öffnung ist eine Information der IT-Kontrollkommission (§ 5) und der betroffenen Gerichte und Staatsanwaltschaften sowie ein Verfahren zur Änderung der Zugangsgewährung vorzusehen; 2. die im Rahmen richterlicher, rechtspflegerischer oder staatsanwaltlicher Tätigkeit erstellten Dokumente dürfen von den Administratorinnen und Administratoren weder eingesehen noch an Dritte weitergegeben werden, insbesondere nicht an die in § 1 Absatz 1 genannten Stellen oder an die diesen nachgeordneten Stellen der Dienstaufsicht; 3. in gleicher Weise ist eine **Einsichtnahme in oder** Weitergabe von Informationen über Merkmale oder Eigenschaften von den in

Dokumenten (Metadaten) und von systemintern automatisch erstellten Protokollen über die Benutzung der zur Verfügung stehenden IT (Logdateien) nicht zulässig;	Nummer 2 genannten Dokumenten (Metadaten) und von systemintern automatisch erstellten Protokollen über die Benutzung der zur Verfügung stehenden IT (Logdateien) nicht zulässig;
4. Ausnahmen von den Nummern 2 und 3 zugunsten des für Justiz zuständigen Ministeriums oder der ihm nachgeordneten Stellen der Dienstaufsicht sind nur zu Zwecken oder auf Veranlassung der jeweiligen Dienstaufsicht im Rahmen bestehender Gesetze zulässig; soweit Dokumente laufender Verfahren betroffen sind, sind die Ausnahmen nur zulässig, soweit dies zur Ausübung der Dienstaufsicht unerlässlich ist;	**4.** Ausnahmen von den Nummern 2 und 3 zugunsten des für Justiz zuständigen Ministeriums oder der ihm nachgeordneten Stellen der Dienstaufsicht sind nur zu Zwecken oder auf Veranlassung der jeweiligen Dienstaufsicht im Rahmen bestehender Gesetze zulässig; soweit Dokumente laufender Verfahren betroffen sind, sind die Ausnahmen nur zulässig, soweit dies zur Ausübung der Dienstaufsicht unerlässlich ist; **das Ministerium benachrichtigt die von Zugriffen betroffenen Personen unverzüglich auf direktem Wege und auf dem Dienstweg;**
5. im Übrigen dürfen die in Nummer 2 genannten Dokumente sowie die in Nummer 3 aufgeführten Metadaten und Logdateien von den Administratorinnen und Administratoren nur mit Zustimmung der betroffenen Verfasserin oder Nutzerin oder des betroffenen Verfassers oder Nutzers verwendet werden, es sei denn, die Verwendung ist für die Gewährleistung der Ordnungsmäßigkeit eines automatisierten Verfahrens oder sonst für den Betrieb der IT-Infrastruktur unerlässlich;	5. im Übrigen dürfen die in Nummer 2 genannten Dokumente sowie die in Nummer 3 aufgeführten Metadaten und Logdateien von den Administratorinnen und Administratoren nur mit Zustimmung der betroffenen Verfasserin oder Nutzerin oder des betroffenen Verfassers oder Nutzers verwendet werden, es sei denn, die Verwendung ist für die Gewährleistung der Ordnungsmäßigkeit eines automatisierten Verfahrens oder sonst für den Betrieb der IT-Infrastruktur unerlässlich;
6. jeder Zugriff ist zu protokollieren und dem für Justiz zuständigen Ministerium unverzüglich auf direktem Wege mitzuteilen; sofern auf individuell zuordnungsfähige Dokumente zugegriffen wurde, benachrichtigt das Ministerium die betroffene Verfasserin oder Nutzerin oder den betroffenen Verfasser oder Nutzer unverzüglich auf direktem Wege und auf dem Dienstweg.	**6.** jeder Zugriff ist zu protokollieren und dem für Justiz zuständigen Ministerium **sowie der IT-Kontrollkommission** unverzüglich auf direktem Wege mitzuteilen; sofern auf individuell zuordnungsfähige Dokumente zugegriffen wurde, benachrichtigt

	das Ministerium die betroffene Verfasserin oder Nutzerin oder den betroffenen Verfasser oder Nutzer unverzüglich auf direktem Wege und auf dem Dienstweg; **dies gilt entsprechend für Metadaten und Logdateien;** **7. Protokolle über die Benutzung der zur Verfügung stehenden IT (Logdateien) dürfen nur bei einem konkreten Verdacht des Missbrauchs zu dienstfremden Zwecken erstellt werden;** **8. die in Nummer 2 genannten Dokumente sowie die in Nummer 3 aufgeführten Metadaten und Logdateien dürften nicht zur Verhaltens- und Leistungskontrolle genutzt werden;** **9. werden die in Nummer 2 genannten Dokumente oder die in Nummer 3 aufgeführten Metadaten und Logdateien rechtswidrig übermittelt oder zur Kenntnis genommen, so unterliegen sie einem Verwertungsverbot;** **10. die in Nummer 2 genannten Dokumente sowie die in Nummer 3 aufgeführten Metadaten und Logdateien sind verschlüsselt zu speichern;** **11. Richtern, Rechtspflegern und Staatsanwälten ist die Möglichkeit zur verschlüsselten Ablage von Dokumenten und Daten zum persönlichen Gebrauch in der Form zu eröffnen, dass alleine der Ersteller über den zur Entschlüsselung erforderlichen Schlüssel verfügt.**
Begründung: *Zu Ziff. 3: Auch die Einsichtnahme in Metadaten und Protokolldateien wird grundsätzlich ausgeschlossen (vgl. NRV, Umdruck 18/5254). Entgegen der*	

Auffassung des Ministeriums lässt sich eine Einsichtnahme in Dateinamen durch Administratoren im Regelfall durchaus vermeiden, zumal eine getrennte Speicherung der Justizdaten ausdrücklich vorgeschrieben ist. Dies ist auch bundesgesetzlich so vorgegeben, wie sich aus der Entscheidung des Hessischen Dienstgerichtshofs vom 22.04.2010 (Az. DGH 4/08) ergibt.

Zu Ziff. 4: Die Ergänzung stellt klar, dass die in Ziff. 6 vorgesehene Benachrichtigung von Zugriffen auch bei Zugriffen im Rahmen der Dienstaufsicht erfolgt. Die Informationstechnologie soll der Dienstaufsicht nicht die Möglichkeit verschaffen, unbemerkt auf eine Vielzahl von Akten, Dokumenten oder Metadaten zuzugreifen (vgl. Berlit, Umdruck 18/5238).

Zu Ziff. 6: Die Mitteilung auch an die IT-Kontrollkommission versetzt diese in die Lage, die Erforderlichkeit externer Zugriffe zu kontrollieren und darüber zu berichten. Die Benachrichtigung der Betroffenen von Zugriffen erfolgt wegen vergleichbarer Interessenlage zum Dokumentenzugriff auch, wenn auf Meta- oder Logdaten zugegriffen wird, die Auskunft über die IT-Nutzung von Richtern, Staatsanwälten oder Rechtspflegern geben.

Zu Ziff. 7: Entsprechend der Entscheidung des Hessischen Dienstgerichtshofs vom 22.04.2010 (Az. DGH 4/08) ist die Speicherung von Metadaten nur bei konkretem Verdacht des Missbrauchs zu dienstfremden Zwecken zulässig (vgl. auch NRV, Umdruck 18/5254). Eine verdachtsunabhängige Vorratsdatenspeicherung ist mit der richterlichen Unabhängigkeit unvereinbar.

Zu Ziff. 8: Das Verbot der Verhaltens- und Leistungskontrolle ist als vertrauensbildende Maßnahme im Zuge der Einführung extern verwalteter Informationstechnologie in der Justiz ausdrücklich aufzunehmen (vgl. Berlit, Umdruck 18/5238). Auch das Ministerium geht davon aus, dass eine solche Datenverwendung unzulässig wäre.

Zu Ziff. 9: Ein Verwertungsverbot rechtswidrig übermittelter oder sonst gewonnener Daten ist als vertrauensbildende Maßnahme im Zuge der Einführung extern verwalteter Informationstechnologie in der Justiz vorzusehen (vgl. Berlit, Umdruck 18/5238).

Zu Ziff. 10: Die Frage der Verschlüsselung wurde in der Anhörung vielfach angesprochen. Eine verschlüsselte Datenablage ist bereits jetzt Stand der Technik. Als vertrauensbildende Maßnahme wird sie gesetzlich vorgesehen, wie es der Gesetzgeber auch an anderer Stelle für besonders schutzwürdige Daten tut (vgl. § 113d TKG). In Betracht kommt zumindest eine Festplattenverschlüsselung, die unberechtigtem Zugriff von außen vorbeugt, etwa nach Aussonderung des Datenträgers. Eine merkliche Minderung der Leistungsfähigkeit der IT ist damit nicht verbunden.

Zu Ziff. 11: Geregelt wird die Möglichkeit zur verschlüsselten Ablage bestimmter Dokumente zum persönlichen Gebrauch (vgl. Berlit, Umdruck 18/5238). In Betracht kommen insbesondere vorbereitende Dokumente, die nicht Gegenstand der „offiziellen“ Gerichtsakte geworden sind (z.B. vorbereitende Notizen, Voten oder Urteilsentwürfe, die noch nicht in den Umlauf gegeben worden sind).

Ein Einblick der Dienstaufsicht oder anderer staatlicher Stellen in von einem Richter oder in seinem Auftrag von anderen Bediensteten im Rahmen seiner Recht sprechenden Tätigkeit bis zur abschließenden Entscheidung angefertigten Dokumente, wie Verfügungen, Beschlüsse, Notizen und Entwürfe (richterliche Dokumente), würde eine Beeinträchtigung der richterlichen Unabhängigkeit darstellen. Wenn aber der Dienstaufsicht ein sachlicher Einfluss auf solche vorbereitenden Entwürfe und Entscheidungen untersagt ist, so darf sie auch von deren Inhalt nicht eigenmächtig Kenntnis nehmen. Eine Kenntnisnahme von noch nicht für die Öffentlichkeit bestimmten richterlichen Dokumenten würde die erste Stufe einer möglichen Einflussnahme bedeuten und ist – wenn sie dem Richter bekannt würde – schon als solche geeignet, Einfluss auf den Kernbereich richterlicher Tätigkeit zu nehmen. *Sachlich, aber auch als „vertrauensbildende Maßnahme“ scheint es daher angezeigt, gerade im Bereich der (vorbereitenden) richterlichen, rechtspflegerischen oder staatsanwaltschaftlichen Tätigkeit außerhalb der elektronischen Akte eine verschlüsselte Ablage mit einem allein durch den jeweiligen Akteur zu verwaltenden kryptographischen Schlüssel verpflichtend anzubieten.*	
§ 4 IT-Stellen	
(3) Zum Schutz vor unbefugten Zugriffen darf die GemIT bei den externen IT-Dienstleistern Kontrollen durchführen. Gegenstand der Kontrolle ist die Einhaltung 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. Soweit erforderlich, ist der GemIT zu den vorgenannten Zwecken Zutritt zu gewähren und ein uneingeschränktes Auskunfts- und Einsichtsrecht zu gewährleisten. Personenbezogene Daten dürfen im Rahmen von Kontrollen auch ohne Kenntnis der Betroffenen erhoben werden. Dokumente, Dateien und Daten im Sinne des § 2 Absatz 2 Satz 2 Nummer 2 und 3 dürfen im Rahmen von Kontrollen hingegen nur eingesehen oder sonst verwendet werden, soweit dies zur Aufgabenerfüllung unerlässlich ist.	(3) Zum Schutz vor unbefugten Zugriffen darf die GemIT bei den externen IT-Dienstleistern Kontrollen durchführen. Gegenstand der Kontrolle ist die Einhaltung 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. Soweit erforderlich, ist der GemIT zu den vorgenannten Zwecken Zutritt zu gewähren und ein uneingeschränktes Auskunfts- und Einsichtsrecht zu gewährleisten. Personenbezogene Daten dürfen im Rahmen von Kontrollen auch ohne Kenntnis der Betroffenen erhoben werden. Dokumente, Dateien und Daten im Sinne des § 2 Absatz 2 Satz 2 Nummer 2 und 3 dürfen im Rahmen von Kontrollen hingegen nur eingesehen oder sonst verwendet werden, soweit **dies für die in Satz 2 genannten Zwecke** unerlässlich ist.

Begründung:

Die Änderung stellt klar, dass zur „Aufgabenerfüllung“ nicht etwa die ministeriale Aufgabe der Dienstaufsicht zu zählen ist, sondern ausschließlich die Kontrollaufgabe der GemIT (vgl. Berlit, Umdruck 18/5238). Der Datenzugriff im Rahmen der Dienstaufsicht ist an anderer Stelle des Gesetzes geregelt.

§ 5 IT-Kontrollkommission	
(1) Zum Schutz der richterlichen Unabhängigkeit, der sachlichen Unabhängigkeit der Rechtspflegerinnen und Rechtspfleger und des Legalitätsprinzips wird bei dem für Justiz zuständigen Ministerium eine unabhängige IT-Kontrollkommission eingerichtet. Das Ministerium hält eine Geschäftsstelle vor, stellt der IT-Kontrollkommission die für die Wahrnehmung ihrer Aufgaben notwendigen Sach- und Fachmittel zur Verfügung und trägt die durch ihre Tätigkeit entstehenden Kosten. § 34 MBG Schl.-H. gilt entsprechend.	(1) Zum Schutz der richterlichen Unabhängigkeit, der sachlichen Unabhängigkeit der Rechtspflegerinnen und Rechtspfleger und des Legalitätsprinzips wird bei dem für Justiz zuständigen Ministerium eine unabhängige IT-Kontrollkommission eingerichtet. **Die Mitglieder der Kontrollkommission sind bei der Wahrnehmung ihrer Kontrollaufgaben von fachlichen Weisungen aller Art freigestellt.** Das Ministerium hält eine Geschäftsstelle vor, stellt der IT-Kontrollkommission die für die Wahrnehmung ihrer Aufgaben notwendigen Sach- und Fachmittel zur Verfügung und trägt die durch ihre Tätigkeit entstehenden Kosten. § 34 MBG Schl.-H. gilt entsprechend. **Die IT-Kontrollkommission kann zum Einsatz von Informationstechnik in der Justiz Stellung nehmen, insbesondere zur allgemeinen IT-Strategie, der Ausstattung der Gerichte und Staatsanwaltschaften, der Infrastruktur sowie der länderübergreifenden Zusammenarbeit. Vor grundsätzlichen Entscheidungen ist ihr Gelegenheit zur Stellungnahme zu geben.**

Begründung:

In Satz 2 wird klarstellend geregelt, dass die Mitglieder der IT-Kontrollkommission bei ihrer Tätigkeit von fachlichen Weisungen aller Art – sowohl solchen des Ministeriums als auch solchen des entsendenden Mitbestimmungsgremiums – freigestellt sind. Diese Klarstellung ist angezeigt, weil sie ihre Aufgaben nicht in richterlicher Unabhängigkeit wahrnehmen.

Nach dem vom Richterbund befürworteten Vorschlag der Neuen Richtervereinigung soll die IT-Kontrollkommission auch allgemein zum Einsatz von Informationstechnik in der Justiz Stellung nehmen können, um die richterliche Unabhängigkeit im Zeitalter der Informationsgesellschaft zu schützen (Sätze 5 und 6). Die Informationstechnologie prägt die richterliche Tätigkeit zunehmend und ist für die Justiz von immer höherer Bedeutung. Solange die Selbstverwaltung der Justiz nicht realisiert ist, wird Vertretern der Justiz wenigstens ein Anhörungsrecht zur Wahrung der besonderen Belange der dritten Staatsgewalt eingeräumt. Die Frage der verbindlichen Mitbestimmung an der Gestaltung der Informationstechnologie durch Mitbestimmungsgremien ist davon unabhängig zu sehen und zu regeln.	
(3) Die Mitglieder der IT-Kontrollkommission sind unter Fortzahlung der Dienstbezüge und unter Übernahme der Kosten für die Teilnahme an Schulungs- und Bildungsveranstaltungen bis zu zwanzig Arbeitstage je Amtszeit vom Dienst freizustellen, soweit diese Kenntnisse vermitteln, die für die Tätigkeit in der IT-Kontrollkommission erforderlich sind. § 37 Absatz 4 und 5 MBG Schl.-H. gilt entsprechend.	(3) Die Mitglieder der IT-Kontrollkommission sind unter Fortzahlung der Dienstbezüge und unter Übernahme der Kosten für die Teilnahme an Schulungs- und Bildungsveranstaltungen **im erforderlichen Umfang** vom Dienst freizustellen, soweit diese Kenntnisse vermitteln, die für die Tätigkeit in der IT-Kontrollkommission erforderlich sind. § 37 Absatz 4 und 5 MBG Schl.-H. gilt entsprechend.
Begründung: *Die Änderung erfolgt auf Anregung der Richterverbände. Wenn die IT-Kontrollkommission schon nicht mit Fachleuten besetzt werden muss, so müssen ihre Mitglieder sich wenigstens im erforderlichen Umfang die erforderlichen Kenntnisse verschaffen können, um ihrer Kontrollfunktion gerecht werden zu können. Die unabhängige IT-Kontrollkommission ist das Herzstück des Gesetzentwurfes. Ihre Funktionsfähigkeit setzt entsprechende Kenntnisse voraus. Die Freistellung ist beschränkt auf die Vermittlung von Kenntnissen, die für die Tätigkeit in der Kommission erforderlich sind.*	
(6) Soweit zur Aufgabenerfüllung erforderlich, ist der IT-Kontrollkommission von den in § 1 Absatz 1 genannten Stellen zu den vorgenannten Zwecken Zutritt zu gewähren und ein uneingeschränktes Auskunfts- und Einsichtsrecht zu gewährleisten. Dieses Recht 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	(6) Soweit zur Aufgabenerfüllung erforderlich, ist **jedem Mitglied** der IT-Kontrollkommission von den in § 1 Absatz 1 genannten Stellen zu den vorgenannten Zwecken Zutritt zu gewähren und ein uneingeschränktes Auskunfts- und Einsichtsrecht zu gewährleisten. Dieses Recht 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 beziehen und die einen wesentlichen Bezug zur Organisation und zum Einsatz von IT in den Gerichten und Staatsanwaltschaften haben. Personenbezogene Daten sowie Dokumente, Dateien und Daten im Sinne des § 2 Absatz 2 Satz 2 Nummer 2 und 3 dürfen im Rahmen von Kontrollen auch ohne Kenntnis der Betroffenen erhoben oder eingesehen werden.	externen IT-Dienstleistern beziehen und die einen wesentlichen Bezug zur Organisation und zum Einsatz von IT in den Gerichten und Staatsanwaltschaften haben. Personenbezogene Daten sowie Dokumente, Dateien und Daten im Sinne des § 2 Absatz 2 Satz 2 Nummer 2 und 3 dürfen im Rahmen von Kontrollen auch ohne Kenntnis der Betroffenen erhoben oder eingesehen werden. **Die Mitglieder der IT-Kontrollkommission sind zum Stillschweigen über ihnen bekannt gewordene personenbezogene Daten verpflichtet, soweit deren Bekanntgabe nicht nach Absatz 8 erforderlich ist.**
Begründung: *Die Änderung in Satz 1 stellt klar, dass sich die Befugnisse der IT-Kontrollkommission nicht nur auf die Kommission im Ganzen, sondern auf jedes Mitglied beziehen. Eine Beschränkung allein auf die IT-Kontrollkommission als Kollektivgremium* *wäre nicht praxisgerecht.* *Die Anfügung eines weiteren Satzes regelt klarstellend und spezialgesetzlich den Schutz personenbezogener Daten, weil die wahrgenommenen personenbezogenen Daten im Bereich der richterlichen Unabhängigkeit besonders sensibel sind und das allgemeine Datenschutzrecht diverse Öffnungsklauseln enthält, die keine Anwendung finden sollen (vgl. Berlit, Umdruck 18/5238).*	
(7) Die IT-Kontrollkommission kann sich zur Erfüllung ihrer Aufgaben von sachkundigen Beschäftigten des Landes und vom Unabhängigen Landeszentrum für Datenschutz beraten lassen.	(7) Die IT-Kontrollkommission kann sich zur Erfüllung ihrer Aufgaben von sachkundigen Beschäftigten des Landes und vom Unabhängigen Landeszentrum für Datenschutz beraten lassen. **Soweit darüber hinaus erforderlich, kann sie unabhängige Sachverständigenauskünfte einholen.**
Begründung: *Die Änderung erfolgt auf Anregung der Richterverbände. Das Land hält mit dem ULD zwar hervorragenden Sachverstand vor. Es sind aber Konstellationen denkbar, in denen gleichwohl die Möglichkeit der unabhängigen Sachverständigenauskunft bestehen sollte, etwa bei Meinungsverschiedenheiten zwischen ULD und IT-Kontrollkommission oder bei außerordentlichen*	

Spezialfragen. Die Aufgabe der IT-Kontrollkommission ist mit dem Schutz der richterlichen Unabhängigkeit eine andere als die des ULD. Daraus kann sich ein unterschiedlicher Blickwinkel auf Sachverhalte ergeben.	
	(10) Die IT-Kontrollkommission veröffentlicht jährlich einen Bericht über ihre Tätigkeit und die vorgefundenen Mängel.
Begründung: *In der Anhörung wurde ein Tätigkeitsbericht der IT-Kontrollkommission allseits als wünschenswert angesehen. In anderen Bundesländern ist teilweise das Problem aufgetreten, dass selbst fortbestehende, schwerwiegende Mängel nicht veröffentlicht werden dürfen (vgl. Schild, Umdruck 18/5184). Die Mitglieder der Justiz, deren Interessen die Kommission wahrnehmen soll, haben ein berechtigtes Interesse an der Offenlegung solcher Mängel. Dasselbe gilt für den Landtag als Kontrollorgan der Landesregierung.*	

Patrick Breyer