SCHLESWIG-HOLSTEINISCHER LANDTAG **Drucksache 18/3224**
18. Wahlperiode 14.07.2015

Gesetzentwurf

der Landesregierung

Entwurf eines IT-Gesetzes für die Justiz des Landes Schleswig-Holstein (IT-Justizgesetz - ITJG)

Federführend ist das Ministerium für Justiz, Kultur und Europa

A. Problem

Gegenstand einer dienstgerichtlichen Klage von Richterinnen und Richtern des Landes Hessen war die Frage, ob die verfassungsrechtlich verankerte richterliche Unabhängigkeit dadurch verletzt wird, dass der Betrieb und die Administration des EDV-Netzes für den Rechtsprechungsbereich extern bei der Hessischen Zentrale für Datenverarbeitung (einer Oberbehörde der Landesfinanzverwaltung) und nicht bei den Gerichten selbst angesiedelt ist. Der Hessische Dienstgerichtshof für Richter hat diese Frage im Ergebnis zwar verneint, aber zugleich festgestellt, dass die Zentralisierung der Datenverarbeitung insoweit nur unter zwei Bedingungen zulässig ist (HessDGH, Urteil vom 20.04.2010 - DGH 4/08 -; bestätigt vom Bundesgerichtshof, Urteil vom 06.10.2011 - RiZ(R) 7/10 - und vom Bundesverfassungsgericht, Beschluss vom 17.01.2013 - 2 BvR 2576/11 -):

- Es sind verbindliche Regeln für den Umgang mit Dokumenten des richterlichen Entscheidungsprozesses festzulegen und
- deren Einhaltung wird durch den Minister der Justiz im gleichberechtigten Zusammenwirken mit gewählten Vertretern der Richter überprüft.

In Hessen wurde daraufhin das Gesetz zur Errichtung der Informationstechnik-Stelle der hessischen Justiz (IT-Stelle) und zur Regelung justiz-organisatorischer Angelegenheiten vom 16. Dezember 2011 (GVOBl. für das Land Hessen, S. 778) erlassen. Es überträgt die Zuständigkeit für die Wahrnehmung von Aufgaben im Bereich der Informationstechnik auf eine zu errichtende Landesbehörde (IT-Stelle der Justiz), überträgt die Fachaufsicht über die Hessische Zentrale für Datenverarbeitung im erforderlichen Umfang auf die Justiz und sieht die Einrichtung einer IT-Kontrollkommission vor, bestehend aus gewählten Vertretern der Richterschaft, Staatsanwaltschaft und der Rechtspflegerschaft.

Eine mit Hessen vergleichbare Situation besteht in Schleswig-Holstein:

Auf der Grundlage des Staatsvertrages über die Errichtung von Dataport als rechtsfähige Anstalt des öffentlichen Rechts zwischen dem Land Schleswig-Holstein und der Freien und Hansestadt Hamburg vom 27. August 2003 (GVOBl. Schl.-H. S. 557), zuletzt geändert durch Staatsvertrag vom 27. September 2013 (GVOBl. Schl.-H. S. 511), wurde mit Dataport ein zentraler IT-Dienstleister des

Landes eingesetzt und mit der Bereitstellung der erforderlichen Infrastruktur und dem Betrieb von (Fach-) Verfahren für die gesamte Landesverwaltung einschließlich der Gerichte und Staatsanwaltschaften betraut. Die Zuständigkeit für die Planung und den Einsatz der ressortübergreifenden Informations- und Kommunikationstechnik (IT) liegt gemäß aktueller Geschäftsverteilung der Landesregierung zentral im Geschäftsbereich des Ministerpräsidenten (Bekanntmachung vom 19. März 2013, GVOBl. Schl.-H. S. 121). Die näheren Bestimmungen sind im Organisationserlass ITSH des Ministerpräsidenten - Staatskanzlei - vom 25. April 2014 (Amtsbl. Schl.-H. S. 372) niedergelegt.

Zum Schutz der unabhängigen Stellung der Judikative als Dritte Gewalt findet der Organisationserlass ITSH auf den Bereich der Rechtsprechung und der Rechtspflege keine Anwendung; die diesbezüglichen Entscheidungen sind dem für Justiz zuständigen Ressort vorbehalten (Ziffer 2.4 OrgErl ITSH). Dessen ungeachtet wurden aus der Justiz heraus grundsätzliche Bedenken gegen die Einschaltung eines externen IT-Dienstleisters geltend gemacht und Forderungen nach einer justizeigenen Lösung diskutiert. In dem Wissen um die Bedeutung der richterlichen Unabhängigkeit und der besonderen Belange der Rechtspflege hat das Ministerium für Justiz, Kultur und Europa allerdings am 20. August 2013 entschieden, es auch bezüglich der IT-Organisation in der Justiz bei der o.g. Grundsatzentscheidung der Landesregierung zu belassen. Die zum Aufbau eines justizeigenen IT-Betriebs erforderliche Anzahl von Stellen für qualifiziertes IT-Personal ist vor dem Hintergrund des landesweit anstehenden Personalabbaus nicht zu erwirtschaften. Darüber hinaus würde das Land durch den Aufbau eines justizeigenen IT-Dienstleisters mit Qualitätsmerkmalen (z.B. Schutzbedarf „hoch“ nach BSI) analog zu Dataport auf die sich aus der Einrichtung eines zentralen IT-Dienstleisters ergebenden Synergieeffekte und die damit möglichen Kostensenkungen und Effizienzsteigerungen verzichten.

Zur Sicherung der besonderen Belange der Justiz bedarf es deshalb auch in Schleswig-Holstein eines Gesetzes zur Regelung der organisatorischen Rahmenbedingungen der zentralen Ausstattung der Justiz mit der erforderlichen IT und deren Betreuung durch oberste Landesbehörden und andere externe Stellen.

Während sich das hessische Gesetz allerdings auf wenige Normen beschränken und die vom Dienstgerichtshof geforderten verbindlichen Regeln der steuernden Fachaufsicht über den externen IT-Dienstleister durch die obersten Landesbehörden überlassen kann, bedarf es vorliegend detaillierterer gesetzlicher Regelungen. Denn als Anstalt des öffentlichen Rechts unterliegt Dataport gemäß § 52 LVwG, § 10 Absatz 1 Dataport-Staatsvertrag nur einer Rechtsaufsicht. Die Übertragung öffentlicher Aufgaben auf einen rechtlich selbstständigen Verwaltungsträger gebietet ein Mindestmaß an Eigenverantwortlichkeit des Verwaltungsträgers und reduziert zugleich die Verantwortung des Staates. Insoweit muss sich der Staat zielorientiert lenkender gesetzlicher und vertraglicher Regelungen bedienen.

B. Lösung

Die sich aus der Entscheidung des Hessischen Dienstgerichtshofs ergebenden Anforderungen werden inhaltlich auf die in der schleswig-holsteinischen Landesverwaltung bestehenden IT-Organisationsstrukturen übertragen.

Ebenso wie in Hessen erfasst der Schutzbereich des IT-Justizgesetzes über die richterliche Unabhängigkeit (Art. 97 GG, Art. 50 Absatz 1 LV) hinaus auch die sachliche Unabhängigkeit im Bereich der fürsorgenden Rechtspflege (§ 9 RPflG) und die verschiedenen Tätigkeiten der Staatsanwaltschaft. Die Staatsanwaltschaft wird gemeinhin zwar der Exekutive zugeordnet, doch handelt es sich auch bei ihr um ein Organ der Rechtspflege. Hier gilt es, die vom Legalitätsprinzip getragene Ermittlungs- und Anklagetätigkeit (§§ 151 ff., 160 StPO) und das Vertrauen in eine von außen unbeeinflusste, objektive Tätigkeit der Staatsanwaltschaft zu schützen und zu stärken. Gerichte und Staatsanwaltschaften tragen den Rechtsstaat gemeinsam. Von daher erscheint es geboten, sie im Bereich der IT auch gemeinsam zu organisieren. Bei alledem ist die Funktionsfähigkeit der Justiz zu gewährleisten.

Für die mit den Schutzgütern des Gesetzes in Berührung kommenden Entscheidungsträger und IT-Administrationen außerhalb der Justiz werden verbindliche Handlungsvorgaben formuliert, Verwaltungsstrukturen angepasst und neue Kon-

trollstrukturen insbesondere gegenüber Dataport als zentralem externen IT-Dienstleister geschaffen:

- § 2 Absatz 2 greift die vom Hessischen Dienstgerichtshof entwickelten Bedingungen für den Umgang mit Dokumenten der Justiz durch eine Fremdadministration auf und überträgt sie auf die Verhältnisse der schleswig-holsteinischen IT-Strukturen.
- Gemäß § 4 Absatz 1 soll im Ministerium für Justiz, Kultur und Europa eigens für die Gerichte und Staatsanwaltschaften eine gemeinsame IT-Stelle (GemIT) eingerichtet werden. Die gesetzlichen Aufgaben der GemIT werden überwiegend bereits jetzt im zuständigen IT-Referat des Ministeriums wahrgenommen, bedürfen aber einer klareren Abgrenzung.
- § 5 sieht die Einrichtung einer unabhängigen IT-Kontrollkommission am Ministerium für Justiz, Kultur und Europa vor. Die Kommission wird mit sieben Mitgliedern besetzt (aus den fünf verschiedenen Gerichtsbarkeiten je ein/e Richter/in, ein/e Staatsanwalt/-anwältin und ein/e Rechtspfleger/in). Ihre wesentliche Aufgabe ist es, gemeinsam mit der dem Ministerium unterstehenden GemIT die Einhaltung der geltenden Vorschriften zu überprüfen und so das Vertrauen in die Wahrung der Unabhängigkeit der Justiz zu stärken.

Im Übrigen werden die Strukturen und Abläufe so gestaltet, dass die Justiz soweit wie möglich die Inhalte selbst bestimmen und auf den IT-Einsatz Einfluss nehmen kann.

C. Alternativen

Keine.

Der gebotene Schutz sowohl der Unabhängigkeit der rechtsprechenden Gewalt und der Gerichte (Art. 50 Absatz 1 und Art. 2 Absatz 3 LV) als auch der Objektivität einer von außen unbeeinflussten Ermittlungs- und Anklagetätigkeit der Staatsanwaltschaft speziell gegenüber den Gefahren beim Einsatz fremdadministrierter IT ist nur durch eine gesetzliche Regelung zu erlangen. Eine bloße Selbstverpflichtung der Landesregierung im Wege eines nur intern verbindlichen Erlasses über die Organisation der IT in der schleswig-holsteinischen Landes-

verwaltung reicht nach der o.g. Entscheidung des Hessischen Dienstgerichtshofes nicht aus.

D. Kosten und Verwaltungsaufwand

1. Kosten

Für die Einrichtung der Geschäftsstelle der IT-Kontrollkommission im Ministerium für Justiz, Kultur und Europa (§ 5 Absatz 1) wird mit einem zusätzlichen Personalbedarf von bis zu 0,5 Arbeitskraftanteil (AKA) gerechnet. Darüber hinaus werden zusätzliche Sachausgaben für die IT-Kontrollkommission (Fortbildung, Reisekosten, Geschäftsbedarf) anfallen.

2. Verwaltungsaufwand

Weitergehender Verwaltungsaufwand als unter B. und D.1. dargestellt wird im Ministerium für Justiz, Kultur und Europa nicht entstehen. Für das Zentrale IT-Management der Landesverwaltung in der Staatskanzlei entstehen Unterrichtungs- und Beteiligungspflichten gegenüber dem Ministerium für Justiz, Kultur und Europa und der IT-Kontrollkommission, die vom Verwaltungsaufwand her als eher geringfügig zu bewerten sind.

3. Auswirkungen auf die private Wirtschaft

Dieser Gesetzentwurf hat keine direkten kostenmäßigen Auswirkungen oder Vollzugsaufwand in privaten Wirtschaftsunternehmen.

E. Länderübergreifende Zusammenarbeit

Eine länderübergreifende Zusammenarbeit besteht mittelbar durch die Errichtung und Unterhaltung von Dataport als Anstalt des öffentlichen Rechts auf der Grundlage eines Staatsvertrages zwischen dem Land Schleswig-Holstein, der Freien und Hansestadt Hamburg, der Freien Hansestadt Bremen und den Ländern Mecklenburg-Vorpommern, Niedersachsen und Sachsen-Anhalt. Eine auf das

Gesetzesvorhaben bezogene unmittelbare Zusammenarbeit mit anderen Ländern kommt wegen des Schutzgutes der besonderen Belange der (Landes-)Justiz nicht in Betracht.

F. Information des Landtages nach Artikel 28 der Landesverfassung

Der Gesetzentwurf ist dem Präsidenten des Schleswig-Holsteinischen Landtages mit Schreiben vom 30. April 2015 zur Unterrichtung übersandt worden.

G. Federführung

Die Federführung liegt beim Ministerium für Justiz, Kultur und Europa des Landes Schleswig-Holstein.

Gesetzentwurf

Entwurf eines IT-Gesetzes für die Justiz des Landes Schleswig-Holstein
(IT-Justizgesetz - ITJG)

Vom xx.xx.2015

Der Landtag hat das folgende Gesetz beschlossen:

§ 1
Geltungsbereich

(1) Dieses Gesetz regelt die organisatorischen Rahmenbedingungen der zentralen Ausstattung der Gerichte und Staatsanwaltschaften des Landes Schleswig-Holstein mit der erforderlichen Informations- und Kommunikationstechnik (IT) und deren Betreuung durch die für die Angelegenheiten der ressortübergreifenden IT zuständige oberste Landesbehörde und das für Justiz zuständige Ministerium des Landes, unterstützt durch Dataport, Anstalt des öffentlichen Rechts, und andere externe IT-Dienstleister.

(2) Der Staatsvertrag über die Errichtung von Dataport als rechtsfähige Anstalt des öffentlichen Rechts vom 27. August 2003 (GOVBl. Schl.-H. S. 557), zuletzt geändert durch Staatsvertrag vom 27. September 2013 (GVOBl. Schl.-H. S. 511), und die von den in Absatz 1 genannten obersten Landesbehörden begründeten Benutzungsverhältnisse mit Dataport bleiben unberührt.

§ 2
Besondere Belange der Justiz

(1) Bei der Organisation und dem Einsatz von IT in den Gerichten und Staatsanwaltschaften des Landes haben die in § 1 Absatz 1 genannten obersten Landesbehörden, unterstützt durch Dataport und andere externe IT-Dienstleister, die Funktionsfähigkeit der Justiz zu gewährleisten und die sonstigen, sich aus der richterlichen Unabhängigkeit, der sachlichen Unabhängigkeit der Rechtspflegerinnen und Rechtspfleger und dem für die Strafverfolgung geltenden Legalitätsprinzip ergebenden besonderen Belange der Justiz zu berücksichtigen und zu schützen. Bei der Einschaltung Dritter ist die Einhaltung dieses Gesetzes vertraglich sicherzustellen.

(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, insbe-

sondere 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 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;
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.

§ 3
Datenschutz, Mitbestimmung

Die Regelungen des Landesdatenschutzgesetzes (LDSG) vom 9. Februar 2000 (GVOBl. Schl.-H. S. 169), zuletzt geändert durch Gesetz vom 19. Juni 2014 (GVOBl. Schl-H. S. 105), und speziell bestehende Bestimmungen in Gesetzen und Verordnungen des Landes zum Datenschutz bleiben unberührt. Eine nach dem Landesrichtergesetz in der Fassung der Bekanntmachung vom 23. Januar 1992 (GVOBl. Schl.-

H. S. 46), zuletzt geändert durch Gesetz vom 13. Dezember 2013 (GVOBl. Schl.-H. S. 494), und dem Mitbestimmungsgesetz Schleswig-Holstein (MBG Schl.-H.) vom 11. Dezember 1990 (GVOBl. Schl.-H. S. 577), zuletzt geändert durch Artikel 12 des Gesetzes vom 11. Dezember 2014 (GVOBl. Schl.-H. S. 464,) vorgesehene Beteiligung der Personalvertretungen bleibt ebenfalls unberührt.

§ 4
IT-Stellen

(1) Das für Justiz zuständige Ministerium organisiert und verantwortet den Einsatz der IT in den Gerichten und Staatsanwaltschaften. Zur Wahrnehmung der daraus folgenden Aufgaben richtet es im Ministerium die Gemeinsame Stelle für Informations- und Kommunikationstechnik der Gerichte und Staatsanwaltschaften (GemIT) ein, bestellt hierfür einen unabhängigen Sicherheitsbeauftragten und regelt die Geschäftsabläufe. Außerdem regelt es im Einvernehmen mit dem IT-Management der Landesverwaltung in der für die Angelegenheiten der ressortübergreifenden IT zuständigen obersten Landesbehörde die Zusammenarbeit mit diesem.

(2) Die Anwenderbetreuung erfolgt vor Ort durch eigene dezentrale IT-Stellen in den Gerichten und Staatsanwaltschaften. Die Aufgabenteilung zwischen der GemIT und den dezentralen IT-Stellen einschließlich der jeweiligen Aufgabenwahrnehmung im Verhältnis zu Dataport oder anderen externen IT-Dienstleistern regelt das für Justiz zuständige Ministerium nach Anhörung der IT-Kontrollkommission (§ 5) durch Rechtsverordnung. Dabei ist die GemIT für die grundlegenden Angelegenheiten der IT in den Gerichten und Staatsanwaltschaften zuständig. Soweit dies erforderlich ist oder zweckdienlich erscheint, können einzelne grundlegende Angelegenheiten organisatorischer, technischer und / oder fachlicher Art auch auf die dezentralen IT-Stellen übertragen werden. Zu diesem Zweck kann die Rechtsverordnung die Einrichtung von nachgeordneten Verfahrenspflegestellen und eine Zusammenarbeit verschiedener Gerichtsbarkeiten vorsehen.

(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.

(4) Soweit die für die Angelegenheiten der ressortübergreifenden IT zuständige oberste Landesbehörde im Rahmen der Rechtsaufsicht über Dataport Kontrollen

durchführt oder soweit durch diese oder andere öffentliche Stellen im Rahmen eines bestehenden Benutzungsverhältnisses zu Dataport oder anderen externen IT-Dienstleistern Kontrollen erfolgen, die den in Absatz 3 beschriebenen Kontrollbereich betreffen, ist die GemIT über die geplante Kontrolle rechtzeitig zu unterrichten und ihr eine Teilnahme zu ermöglichen. Unabhängig von ihrer Teilnahme ist sie über das Ergebnis der Kontrolle zeitnah zu unterrichten. Das Unabhängige Landeszentrum für Datenschutz unterrichtet die GemIT zeitnah über das Ergebnis durchgeführter Kontrollen gemäß § 41 LDSG.

(5) Die für die Angelegenheiten der ressortübergreifenden IT zuständige oberste Landesbehörde und die externen Dienstleister unterrichten die GemIT unverzüglich über Sicherheitsvorfälle, die auch oder ausschließlich die Justiz betreffen.

§ 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.

(2) Die IT-Kontrollkommission besteht aus Angehörigen der Gerichte und Staatsanwaltschaften des Landes. Folgende Mitbestimmungsgremien benennen aus diesem Kreis unverzüglich zu Beginn ihrer eigenen Amtsperiode je ein Mitglied:

1. der Bezirksrichterrat bei dem Schleswig-Holsteinischen Oberlandesgericht,
2. der Bezirksrichterrat bei dem Schleswig-Holsteinischen Oberverwaltungsgericht,
3. der Bezirksrichterrat bei dem Schleswig-Holsteinischen Landessozialgericht,
4. der gemeinsame Richterrat bei dem Landesarbeitsgericht Schleswig-Holstein,
5. der Richterrat bei dem Schleswig-Holsteinischen Finanzgericht,
6. der Hauptstaatsanwaltsrat bei dem für Justiz zuständigen Ministerium und
7. der Hauptpersonalrat bei dem für Justiz zuständigen Ministerium, der ein Mitglied aus den Reihen der Rechtspflegerinnen und Rechtspfleger benennt.

Die in Satz 2 genannten Mitbestimmungsgremien können zugleich jeweils eine Vertreterin oder einen Vertreter benennen. Für den Fall des endgültigen Ausscheidens eines Mitglieds erfolgt eine Nachbenennung.

(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, so-

weit diese Kenntnisse vermitteln, die für die Tätigkeit in der IT-Kontrollkommission erforderlich sind. § 37 Absatz 4 und 5 MBG Schl.-H. gilt entsprechend.

(4) Versäumnis von Arbeitszeit sowie die Nichterfüllung dienstplanmäßiger Leistungen, die zur ordnungsgemäßen Durchführung der Aufgaben der IT-Kontrollkommission nicht zu vermeiden sind, haben keine Minderung der Dienstbezüge und aller Zulagen zur Folge. Darüber hinaus sind die Mitglieder der IT-Kontrollkommission von ihrer dienstlichen Tätigkeit teilweise freizustellen, soweit es zur ordnungsgemäßen Durchführung ihrer Aufgaben erforderlich ist. § 36 Absatz 4, 6 und 7 MBG Schl.-H. gilt entsprechend.

(5) Die IT-Kontrollkommission überwacht die Einhaltung dieses Gesetzes, der bestehenden Verträge mit externen IT-Dienstleistern 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, durch die in § 1 Absatz 1 genannten Stellen. Die Unterrichtungs- und Beteiligungsverpflichtungen nach § 4 Absatz 4 und 5 gelten gegenüber der IT-Kontrollkommission entsprechend.

(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 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.

(7) Die IT-Kontrollkommission kann sich zur Erfüllung ihrer Aufgaben von sachkundigen Beschäftigten des Landes und vom Unabhängigen Landeszentrum für Datenschutz beraten lassen.

(8) Stellt die IT-Kontrollkommission Verstöße gegen die in Absatz 5 genannten Bestimmungen bei den in § 1 Absatz 1 genannten Stellen fest, fordert es diese unter Setzung einer angemessenen Frist zur Mängelbeseitigung auf. Werden die Verstöße in dieser Frist nicht abgestellt oder handelt es sich um erhebliche Verstöße, spricht die IT-Kontrollkommission eine Beanstandung aus und unterrichtet die zuständige Aufsichtsbehörde und / oder den jeweiligen Vertragspartner der externen IT-Dienstleister.

(9) Die IT-Kontrollkommission gibt sich eine Geschäftsordnung.

§ 6
Standard-IT und zentrale Dienste

(1) Die für die Angelegenheiten der ressortübergreifenden IT zuständige oberste Landesbehörde stellt die für die Landesverwaltung vorgehaltene Standard-IT und die nach Maßgabe des Landes-E-Government-Gesetzes vom 8. Juli 2009 (GVOBl. Schl.-H. S. 398) eingerichteten zentralen Dienste (Basisdienste) auch der Justiz zur Verfügung.

(2) Über den Einsatz der Standard-IT und ihrer einzelnen Funktionen sowie über die Nutzung der Basisdienste in den Gerichten und Staatsanwaltschaften entscheidet das für Justiz zuständige Ministerium nach Anhörung der IT-Kontrollkommission. Soweit erforderlich, können im Einvernehmen mit dem IT-Management der Landesverwaltung in der für die Angelegenheiten der ressortübergreifenden IT-Angelegenheiten zuständigen obersten Landesbehörde darüber hinaus die Einrichtung justizeigener Standards vorgesehen und die diesbezüglichen Modalitäten geregelt werden.

(3) Die Vorschriften des Landes-E-Government-Gesetzes und die auf dieser Grundlage getroffenen Bestimmungen gelten für den nach Absatz 2 erfolgenden Einsatz von Standard-IT und von Basisdiensten in den Gerichten und Staatsanwaltschaften entsprechend, soweit sich aus dem vorliegenden Gesetz nichts Abweichendes ergibt. Dabei haben die in § 1 Absatz 1 genannten obersten Landesbehörden auch im Verhältnis zu Dataport sicherzustellen, dass die Funktionsfähigkeit der Justiz nicht beeinträchtigt und die sonstigen besonderen Belange der Justiz gewahrt werden. Gleiches gilt für wesentliche Änderungen und Weiterentwicklungen an der Standard-IT und den Basisdiensten.

(4) Über beabsichtigte wesentliche Änderungen und Weiterentwicklungen an der Standard-IT oder an den Basisdiensten sind die GemIT und die IT-Kontrollkommission durch die für die Angelegenheiten der ressortübergreifenden IT zuständige oberste Landesbehörde frühzeitig zu unterrichten.

§ 7
Fachverfahren

(1) Für die in den Gerichten und Staatsanwaltschaften erforderlichen Fachverfahren begründet das für Justiz zuständige Ministerium nach Anhörung der IT-Kontrollkommission jeweils eigene Benutzungsverhältnisse gegenüber Dataport. Die Funktionsfähigkeit und die sonstigen besonderen Belange der Justiz sind vertraglich sicherzustellen.

(2) Überträgt das für Justiz zuständige Ministerium die Verantwortung für die Gewährleistung der Ordnungsmäßigkeit automatisierter Fachverfahren gemäß § 8 Absatz 2 LDSG durch Verordnung auf eine zentrale Stelle, bestimmt es in dieser Verordnung zugleich, dass die zentrale Stelle die ihr übertragenen Aufgaben unter ent-

sprechender Beachtung der Vorgaben des § 2 Absatz 2 Satz 2 und unter Mitwirkung entweder der IT-Kontrollkommission oder der jeweils beteiligten Stelle einschließlich der jeweils zuständigen Personalvertretung wahrzunehmen hat.

(3) Soweit die Wahrnehmung der mit der Justiz vertraglich vereinbarten Aufgaben durch Dataport der Rechtsaufsicht der für die Angelegenheiten der ressortübergreifenden IT zuständigen obersten Landesbehörde unterliegt, ist diese Rechtsaufsicht im Benehmen mit dem für Justiz zuständigen Ministerium auszuüben.

§ 8
Justizinterne Zugriffsrechte

Das für Justiz zuständige Ministerium erlässt im Benehmen mit der IT-Kontrollkommission Regelungen über justizinterne Zugriffsrechte auf die in § 2 Absatz 2 Satz 2 Nummer 2 genannten Dokumente und die dazu verfügbaren Metadaten sowie über den Zugang zu Logdateien sowie zu Vorkehrungen zur Sicherung der Zweckbindung und zum Schutz vor unbefugter Einsichtnahme.

§ 9
Inkrafttreten

Dieses Gesetz tritt am Tage nach seiner Verkündung in Kraft.

Das vorstehende Gesetz wird hiermit ausgefertigt und ist zu verkünden.

Kiel,

Torsten Albig

Ministerpräsident

Anke Spoorendonk

Ministerin
für Justiz, Kultur und Europa

Begründung:

I. Allgemein

Der Gesetzentwurf zieht die Konsequenzen aus der dienstgerichtlichen Entscheidung über die von Richterinnen und Richtern des Landes Hessen erhobene sog. hessische Netzklage. Gegenstand dieser Klage war die Frage, ob die verfassungsrechtlich gewährte und gebotene richterliche Unabhängigkeit dadurch verletzt wird, dass der Betrieb und die Administration des EDV-Netzes für den Rechtsprechungsbereich bei der Hessischen Zentrale für Datenverarbeitung (HZD), einer Oberbehörde der Landesfinanzverwaltung, und nicht bei den Gerichten angesiedelt ist.

Der Hessische Dienstgerichtshof für Richter gelangte zu der Auffassung, dass die richterliche Unabhängigkeit nicht allein dadurch verletzt wird, dass der Betrieb des EDV-Netzes einer anderen, nicht der justizeigenen Dienstaufsicht unterstehenden Stelle überlassen wird. Nach dem dortigen Konzept der Ministerialverwaltung sei es auch nicht geboten, den Betrieb des EDV-Netzes den Gerichten als Organen der Justizverwaltung zu übertragen. Es sei deshalb auch nicht erforderlich, „das EDV-Netz für die … Justiz technisch-organisatorisch und auch hinsichtlich des Administrationspersonals von der Datenverarbeitung für die übrige Landesverwaltung zu trennen und dem Minister der Justiz zu unterstellen.“ Allerdings hat der Dienstgerichtshof in seiner Entscheidung (HessDGH, Urteil vom 20.04.2010 - DGH 4/08 -, in juris) festgestellt, dass die Zentralisierung der Datenverarbeitung nur unter der Bedingung zulässig ist,

- dass verbindliche Regeln für den Umgang mit Dokumenten des richterlichen Entscheidungsprozesses festgelegt werden und
- dass deren Einhaltung durch den Minister der Justiz im gleichberechtigten Zusammenwirken mit gewählten Vertretern der Richter überprüft wird.

Mit dieser Maßgabe wurde das Urteil rechtskräftig (Bundesgerichtshof, Urteil vom 06.10.2011 - RiZ(R) 7/10 -; Bundesverfassungsgericht, Beschluss vom 17.01.2013 - 2 BvR 2576/11 -). Auf der Grundlage dieser Rechtsprechung ist davon auszugehen, dass allein die Zentralisierung der elektronischen Datenverarbeitung noch keinen Eingriff in die richterliche Unabhängigkeit begründet, weil sie Richterinnen und Richtern keinen ausreichenden Anlass gibt, aus Sorge um ein unkontrollierbares Beobachtet werden von der Verwendung ihrer Dienstcomputer oder des EDV-Netzes Abstand zu nehmen.

Eine mit Hessen vergleichbare Situation besteht in Schleswig-Holstein:

Auf der Grundlage des Staatsvertrages über die Errichtung von Dataport als rechtsfähige Anstalt des öffentlichen Rechts zwischen dem Land Schleswig-Holstein und der Freien und Hansestadt Hamburg vom 27. August 2003 (GVOBl. Schl.-H. S. 557), zuletzt geändert durch Staatsvertrag vom 27. September 2013 (GVOBl. Schl.-H. S. 511), wurde mit Dataport ein zentraler IT-Dienstleister des Landes eingesetzt und

mit der Bereitstellung der erforderlichen Infrastruktur und dem Betrieb von (Fach-) Verfahren für die gesamte Landesverwaltung einschließlich der Gerichte und Staatsanwaltschaften betraut. Die Zuständigkeit für die Planung und den Einsatz der ressortübergreifenden Informations- und Kommunikationstechnik (IT) liegt gemäß aktueller Geschäftsverteilung der Landesregierung zentral im Geschäftsbereich des Ministerpräsidenten - Staatskanzlei -, wo auch die Funktion CIO (Chief Information Officer) eingerichtet ist (Bekanntmachung vom 19. März 2013, GVOBl. Schl.-H. S. 121). Die Organisation des ressortübergreifenden Einsatzes von Informations- und Kommunikationstechnologien (IT) und der Zusammenarbeit des Zentralen und Dezentralen IT-Managements in der Landesverwaltung Schleswig-Holstein ist im Erlass des Ministerpräsidenten - Staatskanzlei - vom 25. April 2014 geregelt (OrgErl ITSH, Amtsbl. Schl.-H. S. 372). Zum Schutz der unabhängigen Stellung der Judikative als Dritte Gewalt findet der Organisationserlass ITSH – ebenso wie das Gesetz zur elektronischen Verwaltung für Schleswig-Holstein (Landes-E-Government-Gesetz - EGovG) vom 8. Juli 2009 (GVOBl. Schl.-H. S. 398) gemäß § 1 Satz 4 EGovG - auf den Bereich der Rechtsprechung und der Rechtspflege keine Anwendung; die diesbezüglichen Entscheidungen sind dem für Justiz zuständigen Ressort vorbehalten (Ziffer 2.4 OrgErl ITSH).

Diese organisatorische Ausgestaltung hat zur Folge, dass die Gerichte und Staatsanwaltschaften in der Praxis keine eigene, von der Landesverwaltung losgelöste IT-Infrastruktur unterhalten. Unter Verweis auf die unabhängige Stellung der Judikative als Dritte Gewalt wurden deshalb aus der schleswig-holsteinischen Justiz heraus Bedenken gegen die Einschaltung eines externen IT-Dienstleisters geltend gemacht und Forderungen nach einer justizeigenen Lösung diskutiert. In dem Wissen um die Bedeutung der richterlichen Unabhängigkeit und der besonderen Belange der Rechtspflege hat das Ministerium für Justiz, Kultur und Europa nach der abschließenden Entscheidung des Bundesverfassungsgerichts über die Netzklage (a.a.O.) am 20. August 2013 entschieden, es auch bezüglich der IT-Organisation in der Justiz bei der o.g. Grundsatzentscheidung der Landesregierung zu belassen, um die sich aus der Einrichtung eines zentralen IT-Dienstleisters des Landes ergebenden Synergieeffekte auch insoweit nutzen zu können. Die zum Aufbau eines justizeigenen IT-Betriebs erforderliche Anzahl von Stellen für qualifiziertes IT-Personal ist vor dem Hintergrund des landesweit anstehenden Personalabbaus nicht zu erwirtschaften. Darüber hinaus würde das Land durch den Aufbau eines justizeigenen IT-Dienstleisters mit Qualitätsmerkmalen (z.B. Schutzbedarf „hoch“ nach BSI) analog zu Dataport auf die mit den genannten Synergien möglichen Kostensenkungen und Effizienzsteigerungen verzichten.

In Anlehnung an das Gesetz zur Errichtung der Informationstechnik-Stelle der hessischen Justiz (IT-Stelle) und zur Regelung justizorganisatorischer Angelegenheiten vom 16. Dezember 2011 (GVOBl. für das Land Hessen, 2011, S. 778) bedarf es deshalb zur Sicherung der besonderen Belange der Justiz auch in Schleswig-Holstein eines eigenen Gesetzes.

Anders als in Hessen kann der gebotene Schutz allerdings nicht im Rahmen fachaufsichtlicher Maßnahmen sichergestellt werden, sondern muss vorrangig lenkend durch zielorientierte gesetzliche und vertragliche Regelungen erfolgen. Denn die HZD arbeitet im Gegensatz zu Dataport als betriebswirtschaftlich geführter Landesbetrieb nach § 26 LHO Hessen und ist insoweit unselbständiger Teil der hessischen Landesverwaltung. Sie untersteht der Fach- und Dienstaufsicht des hessischen Finanzministeriums und im Bereich der Justiz der Fachaufsicht des Justizministers. Die Kontrolle obliegt der durch Gesetz eingerichteten IT-Stelle der hessischen Justiz unter Mitwirkung einer eigens hierfür eingerichteten IT-Kontrollkommission (vgl. §§ 1, 2 und 3 des o.g. Gesetzes).

Als Anstalt des öffentlichen Rechts übt Dataport nur eine mittelbare Staatsverwaltung aus und unterliegt der gemeinsamen Aufsicht durch die Trägerländer; Aufsichtsbehörde ist „das für ressortübergreifende IT-Angelegenheiten zuständige Ministerium des Landes Schleswig-Holstein“ (§ 42 Absatz 2 LVwG, § 10 Absatz 1 Dataport-Staatsvertrag) - nach der hier im Gesetz verwendeten Formulierung „die für die Angelegenheiten der ressortübergreifenden IT zuständige oberste Landesbehörde“. Die Aufsicht über Anstalten des öffentlichen Rechts erstreckt sich gemäß § 52 LVwG darauf, dass Gesetz und Satzung beachtet und die der Anstalt übertragenen Aufgaben erfüllt werden. Bei dieser Aufsicht handelt es sich um eine Rechtsaufsicht (Friedersen in: Praxis der Kommunalverwaltung, LVwG, § 51 Anm. 1). Maßstab sind diejenigen objektiven Rechtssätze, die auf das zu kontrollierende Verwaltungshandeln Anwendung finden (Kluth in: Wolff/ Bachof/ Stober/ Kluth, Verwaltungsrecht, Bd. II, 7. Aufl., 2010, S. 891). Die Übertragung öffentlicher Aufgaben auf einen rechtlich selbstständigen Verwaltungsträger schafft eine Distanz zwischen Staat und Verwaltungsträger, die ein Mindestmaß an Eigenverantwortlichkeit des Verwaltungsträgers verlangt und spiegelbildlich die Verantwortung des Staates reduziert. Die entsprechende Aufsicht ist deshalb strukturell auf eine Rechtmäßigkeitskontrolle beschränkt (Pieper, Aufsicht. Verfassungs- und verwaltungsrechtliche Strukturanalyse, 2006, S. 405; Burgi, Selbstverwaltung angesichts von Europäisierung und Ökonomisierung, VVDStRL 62 [2003], S. 437). Eine fachaufsichtliche Steuerung sieht das Landesverwaltungsgesetz für Anstalten des öffentlichen Rechts weder grundsätzlich und allgemein noch konkret im Falle von Dataport vor (vgl. auch Gutachten Burgi vom 11.05.2006 S. 45) und kann daher auch durch das IT-Justizgesetz nicht installiert werden.

Stattdessen ist die Tätigkeit Dataports zielorientiert durch gesetzliche und vertragliche Regelungen zu lenken. Mithilfe eines entsprechend gestalteten Lenkungsmittels ist es bis zu einem gewissen Grad möglich, auch außerrechtliche bzw. sachlich-politische Maßstäbe und Ziele aufzugreifen, die als solche im Rahmen der Rechtsaufsicht gerade keine Berücksichtigung finden: Soweit diese Kriterien, etwa durch die Verwendung „dehnbarer“ Rechtsbegriffe, Aufnahme in die entsprechende Lenkungsnorm finden, wird hierdurch wiederum der Maßstab für die nachgängige Rechtsaufsicht definiert (Kahl, Die Staatsaufsicht, 2000, S. 358, 542 f.; Jestaedt in: Erichsen/

Ehlers, Allgemeines Verwaltungsrecht, 14. Aufl., 2010, S. 331; vgl. Looschelder in: Isensee/ Kirchhof, HbdStR, Bd. III, 1988, S. 544).

Die Lenkung der Aufgabenerfüllung durch Dataport geschieht durch den per Gesetz implementierten Staatsvertrag, durch Verwaltungsvorschriften und durch konkrete Verträge. Die aus verfassungsrechtlichen Gründen erforderlichen Regeln für den Umgang mit Dokumenten des richterlichen Entscheidungsprozesses und für die Kontrolle des externen IT-Dienstleisters durch die Ministerin oder den Minister der Justiz im gleichberechtigten Zusammenwirken mit gewählten Vertreterinnen und Vertretern der Richterinnen und Richter sind deshalb im IT-Justizgesetz zu schaffen. Zudem sind die Prozesse der elektronischen Verarbeitung von Informationen und Daten und der Einsatz von IT innerhalb der Justiz so zu gestalten, dass die Justiz soweit wie möglich die Inhalte selbst bestimmen kann. Dabei werden die sich aus der Entscheidung des Hessischen Dienstgerichtshofs ergebenden Anforderungen zum Schutze der richterlichen Unabhängigkeit (Art. 97 GG, Art. 50 Absatz 1 LV) auf den Schutz der sachlichen Unabhängigkeit im Bereich der fürsorgenden Rechtspflege (§ 9 RPflG) und auf die verschiedenen Tätigkeiten der Staatsanwaltschaft erstreckt. Letztere wird gemeinhin zwar der Exekutive zugeordnet, doch handelt es sich auch bei ihr um ein Organ der Rechtspflege. Hier gilt es, die vom Legalitätsprinzip getragene Ermittlungs- und Anklagetätigkeit (§§ 151 ff., 160 StPO) und das Vertrauen in eine von außen unbeeinflusste, objektive Tätigkeit der Staatsanwaltschaft zu schützen und zu stärken. Gerichte und Staatsanwaltschaften tragen den Rechtsstaat gemeinsam. Von daher erscheint es geboten, sie im Bereich der IT auch gemeinsam zu organisieren.

II. Zu den einzelnen Vorschriften

zu § 1

Absatz 1

Der Geltungsbereich des IT-Justizgesetzes beschränkt sich auf die organisatorischen Rahmenbedingungen beim Einsatz von Informations- und Kommunikationstechnik (IT) in den Gerichten und Staatsanwaltschaften des Landes.

Nicht zu den „Gerichten und Staatsanwaltschaften des Landes“ gehört das Schleswig-Holsteinische Landesverfassungsgericht als eigenständiges Verfassungsorgan (Art. 51 LV). Insoweit kann das für Justiz zuständige Ministerium nicht unmittelbar tätig werden. Allerdings sieht § 12 Absatz 1 LVerfGG vor, dass sich das Landesverfassungsgericht der „Geschäftseinrichtungen der Gerichte des Landes bedienen“ kann. Damit hat es auch im Bereich der IT die Möglichkeit, sich der im Land vorhandenen Justizinfrastrukturen einschließlich der bestehenden technischen Hilfsmittel zu bedienen.

Der Begriff Informations- und Kommunikationstechnik (IT) umfasst alle technischen Systeme, die dazu bestimmt sind, Informationen und Daten zu verarbeiten, zu erfassen oder zu übertragen, soweit diese zur Abwicklung der Arbeitsabläufe in den Gerichten und Staatsanwaltschaften benötigt und eingesetzt werden (Programme, Verfahren, Dienste o.ä.; vgl. Ziffer 2.1 OrgErl ITSH).

Das Gesetz richtet sich an diejenigen Stellen außerhalb der Justiz, die diese IT zentral beschaffen, bereitstellen und betreuen. Wahrgenommen werden diese Aufgaben durch zwei oberste Landesbehörden, unterstützt von Dataport als zentralem IT-Dienstleister des Landes und deren Unterauftragnehmern und anderen IT-Dienstleistern:

1. Für die Angelegenheiten der ressortübergreifenden IT zuständige oberste Landesbehörde ist nach der aktuellen Geschäftsverteilung der Landesregierung der Ministerpräsident – Staatskanzlei -, wo auch die Aufgaben des Chief Information Officers (CIO) der Landesregierung wahrgenommen werden (Bekanntmachung vom 19. März 2013, GVOBl. Schl.-H. S. 121). Dieser organisiert in Zusammenarbeit mit den Ressorts die IT in der unmittelbaren Landesverwaltung und übt zugleich die Rechtsaufsicht über Dataport aus (Ziffer 3.1.2, 3.1.4, 3.2.2 OrgErl ITSH). Vertragspartner der im Rahmen des Benutzungsverhältnisses zu Dataport zu schließenden öffentlich-rechtlichen Verträge zwischen der Landesverwaltung und Dataport ist der Beauftragte der Landesregierung für IT, vertreten durch den CIO.

2. Im Übrigen organisiert und verantwortet das für Justiz zuständige Ministerium den Einsatz der IT in den Gerichten und Staatsanwaltschaften (vgl. § 4 Absatz 1). In Teilbereichen (z.B. beim Einsatz von Fachverfahren, s. § 7) begründet es auch selbst die erforderlichen Benutzungsverhältnisse mit Dataport.

3. Dataport wurde errichtet als rechtsfähige Anstalt des öffentlichen Rechts i.S.d. §§ 41 ff. LVwG durch den Staatsvertrag über die Errichtung von Dataport als rechtsfähige Anstalt des öffentlichen Rechts zwischen dem Land Schleswig-Holstein und der Freien und Hansestadt Hamburg vom 27. August 2003 (GVOBl. Schl.-H. S. 557). Mittlerweile sind das Land Mecklenburg-Vorpommern, die Freie Hansestadt Bremen und die Länder Niedersachsen und Sachsen-Anhalt dem Vertrag als Träger beigetreten (vgl. § 1 Absatz 1 des Staatsvertrages in der Fassung des Änderungsstaatsvertrages für den Beitritt des Landes Sachsen-Anhalt vom 6. August bis 27. September 2013 (StV), Anlage zum Gesetz zum Staatsvertrag zwischen dem Land Schleswig-Holstein, der Freien und Hansestadt Hamburg, dem Land Mecklenburg-Vorpommern, der Freien Hansestadt Bremen, dem Land Niedersachsen und dem Land Sachsen-Anhalt zur rechtsfähigen Anstalt des öffentlichen Rechts „Dataport“ vom 1. Dezember 2013, GVOBl. 2013, S. 511; Bekanntmachung über das Inkrafttreten des Staatsvertrages am 24. Februar 2014 vom 11. Juni 2014, GVOBl. Schl.-H. S. 108).

   Aufgabe von Dataport ist es, die öffentlichen Verwaltungen durch Informations- und Kommunikationstechniken zu unterstützen. Dataport fungiert insbesondere

als zentraler IT-Dienstleister des Landes Schleswig-Holstein und ist befugt, sich zur Aufgabenerfüllung Dritter zu bedienen (§ 3 Absatz 1 und 2 StV). Das erforderliche Benutzungsverhältnis zwischen Dataport und den öffentlichen Stellen des Landes wird jeweils durch öffentlich-rechtlichen Vertrag begründet (§ 2 Absatz 1 der Benutzungsordnung Dataport).

Obwohl Dataport öffentlich-rechtlich organisiert ist und der Rechtsaufsicht des Landes untersteht, handelt es sich dennoch - jedenfalls aus Sicht der Justiz – nicht um eine internen, sondern um eine externen IT-Dienstleister.

Das Verhältnis von Dataport zu den öffentlichen Auftraggebern wurde bereits anlässlich der Präsentation des 26. Tätigkeitsberichtes des ULD (LT-Umdruck 15/4945) geklärt. Da § 15 Absatz 1 StV bestimmt, dass „für die Verarbeitung personenbezogener Daten durch Dataport … die Vorschriften des Schleswig-Holsteinischen Landesdatenschutzgesetzes (LDSG)….“ gelten, findet u.a. § 17 LDSG Anwendung, der Vorgaben formuliert für den Fall, dass eine datenverarbeitende öffentliche Stelle (z.B. die Polizei oder auch ein Gericht) personenbezogene Daten in ihrem Auftrag durch einen externen Dienstleister verarbeiten lässt. Über die damit einhergehende Letztverantwortlichkeit der Auftrag gebenden Stelle bestand zunächst Uneinigkeit zwischen dem ULD und dem Innenministerium. Im Rahmen einer Sitzung des Innen- und Rechtsausschusses am 29. September 2004 wurde jedoch Einigkeit über die Anwendbarkeit des § 17 LDSG erzielt mit dem Ergebnis, dass der Auftraggeber, damals die Polizei, auch dann Herr des Verfahrens und damit der Datenverarbeitung ist, wenn Dataport – damit als externer Dienstleister – mit der Datenverarbeitung beauftragt ist und dass dem Auftraggeber damit auch die gesetzlichen Kontrollpflichten obliegen (Niederschrift S. 15).

Entsprechend genießt Dataport auch im Vergleich zu anderen externen Dienstleistern keinen Sonderstatus. Aufgrund der besonderen Rechtsform kann Dataport allerdings grundsätzlich als „sorgfältig ausgewählt“ i.S.d. § 17 Absatz 3 LDSG gelten (vgl. den 27. Tätigkeitsbericht des ULD, Tz. 6.1 und 6.2). Im Übrigen wird davon ausgegangen, dass im Hinblick auf die Rechtsbeziehungen zwischen dem Land und Dataport bei dessen Beauftragung ein „vergaberechtsfreies Inhouse-Geschäft“ vorliegt und die Vorschriften des Kartellvergaberechts auf die Inanspruchnahme von Dataport durch das Land sowohl als IT-Beschaffungsstelle als auch als IT-Dienstleister nicht anwendbar sind (Gutachten Burgi vom 11.05.2006 S. 31). Die Beauftragung von Dataport kann deshalb ohne Ausschreibung erfolgen (s.a. Ziffer 11.2 OrgErl ITSH).

Absatz 2

Absatz 2 stellt klar, dass sowohl die Bestimmungen des Dataport-Staatsvertrages, die Dataport auch für die Justiz zum zentralen IT-Dienstleister des Landes bestimmen, als auch die im Umfang der jeweils geltenden rechtlichen und vertraglichen

Rahmenbedingungen bereits definierten Aufgaben unberührt bleiben und damit vorrangig sind. So baut etwa die Zuständigkeit der nach § 4 Absatz 1 Satz 2 einzurichtenden Gemeinsamen Stelle für Informations- und Kommunikationstechnik (GemIT) einerseits hierauf auf, andererseits bedient sich die Justiz und mit ihr die GemIT dabei auch der Dienste Dataports.

zu § 2

Absatz 1

Absatz 1 Satz 1 benennt die Schutzgüter des Gesetzes und nimmt vorrangig die in § 1 Absatz 1 genannten obersten Landesbehörden generalklauselartig in die Pflicht, den definierten Schutzbereich bei der Ausstattung der Gerichte und Staatsanwaltschaften mit IT und bei deren Betreuung zu wahren. Dies gilt nicht nur auf der technischen Seite, sondern auch bei der Abfassung von anderen (Verwaltungs-) Vorschriften, dem Abschluss von Dienstvereinbarungen oder bei der vertraglichen Vergabe von Dienstleistungen im IT-Bereich. Besondere Regelungen finden sich insoweit noch in den §§ 6 und 7.

Die Gewährleistung der Funktionsfähigkeit der Justiz hat sich an den aus Art. 19 Absatz 4 GG und aus der Strafprozessordnung folgenden Vorgaben auszurichten. Sie erfordert beispielsweise die Gewährleistung einer höchstmöglichen Betriebsstabilität sowie die Bereitstellung der erforderlichen (Fach-)Verfahren und fachlichen Funktionen.

Die sonstigen besonderen Belange der Justiz ergeben sich aus den allgemeinen verfassungsrechtlichen und einfachgesetzlichen Vorgaben, unter denen die verschiedenen Organe der Rechtspflege im Rahmen ihrer Zuständigkeiten tätig sind. Dabei kann der Schutzumfang durchaus unterschiedlich ausfallen, je nachdem, ob es sich um die rechtsprechende (streitentscheidende) Tätigkeit der Richterinnen und Richter, die Rechtspflege insbesondere im Sinne von Rechtsfürsorge im Bereich der freiwilligen Gerichtsbarkeit oder um die verschiedenen Tätigkeiten der Staatsanwaltschaften handelt; besonders schützenswert ist hier die vom Legalitätsprinzip getragene Ermittlungs- und Anklagetätigkeit.

Satz 2 weist darauf hin, dass insbesondere beim Abschluss von Verträgen mit externen IT-Dienstleistern darauf geachtet werden muss, dass die Einhaltung des Gesetzes sichergestellt ist (z.B. Verpflichtung des Vertragspartners zur Ermöglichung der vorgesehenen Kontrollen).

Dessen ungeachtet sind auch die externen IT-Dienstleister an das Gesetz gebunden. Die Einhaltung des Gesetzes durch Dataport unterliegt der Rechtsaufsicht durch den CIO.

Absatz 2

Des weiteren nimmt Absatz 2 Satz 1 die in § 1 Absatz 1 genannten Stellen in die grundsätzliche Pflicht, das verfassungsrechtliche Gebot der Gewaltenteilung, hier die Trennung der Judikative von der Exekutive, in einer möglichst weitgehenden, zugleich den Datenschutzbestimmungen genügenden technischen Trennung der vorhandenen Informations- und Kommunikationsstrukturen - angefangen bei einer technischen Trennung im Landesnetz - widerzuspiegeln. Aus den in der Allgemeinen Begründung genannten wirtschaftlichen Gründen erfolgt diese Trennung bei Einschaltung eines zentralen externen IT-Dienstleisters zwar nicht physisch sichtbar, aber doch durch Schaffung geschlossener, voneinander abgeschotteter Benutzergruppen, zumal auch nur so der für die Justiz gebotene „Grundschutz Hoch“ gewährleistet werden kann. Ausgenommen vom Trennungsgebot ist lediglich der Einsatz von Standard-IT und Basisdiensten nach § 6, die zum Umgang mit Dokumenten des richterlichen oder rechtspflegerischen Entscheidungsprozesses sowie der vom Legalitätsprinzip getragenen Ermittlungs- und Anklagetätigkeit und damit zu dem in Absatz 1 definierten Schutzbereich keine Berührungen haben.

Zur Absicherung dieses Modells übernimmt Absatz 2 Satz 2 die vom Hessischen Dienstgerichtshof formulierten Mindestbedingungen, unter denen eine Einbindung in die zentralen IT-Infrastrukturen der Landesverwaltung und eine zentrale Administration der in der Justiz zum Einsatz kommenden IT durch einen zentralen IT-Dienstleister verfassungsrechtlich nur zulässig ist. Zitiert wird eine Kernaussage des Hessischen Dienstgerichtshofs: Da die richterliche Unabhängigkeit eine Einflussnahme auf den sachlichen Inhalt der richterlichen Tätigkeit verbietet, muss auch jeglicher (eigenmächtige) Einblick in den richterlichen Arbeitsprozess untersagt werden. Sowohl die Kenntnisnahme als auch die Möglichkeit der Kenntnisnahme solcher Dokumente ist zu verhindern. Dies gilt bei richterlichen Dokumenten sowohl für die Dienstaufsicht und (erst recht) für andere staatliche Stellen als auch für sonstige Dritte und damit sowohl für justizeigene als auch für externe Administratorinnen und Administratoren (vgl. HessDGH, Urt. v. 20.04.2010 - DGH 4/08 - Umdr. S. 16 f., in juris Rn. 52 f.). Entsprechend wird die richterliche, rechtspflegerische und staatsanwaltliche Tätigkeit geschützt, soweit diese im Schutzbereich des Absatz 1 stattfindet.

Maßgeblich für die zur Umsetzung dieser Kernaussage erforderlichen Maßnahmen ist stets der jeweilige Stand der Technik. Die darüber hinaus enumerativ aufgeführten Einzelmaßgaben sind an die Maßgaben des Hessischen Dienstgerichtshofs angelehnt und nicht abschließend. Aus dem Umstand, dass in den Einzelmaßgaben nur die Rede von Administratorinnen und Administratoren ist, darf kein Umkehrschluss zugunsten anderer Personen oder Stellen gezogen werden; vielmehr sind die in den Nummern 1 bis 6 gemachten Vorgaben von allen beteiligten Stellen sicherzustellen. Die Aufzählung ist auch inhaltlich nicht abschließend; daneben gelten selbstredend die in den einzelnen Prozessordnungen und auf deren Grundlage erlassener Landesverordnungen (z.B. für den elektronischen Rechtsverkehr und die E-Akte) und in

den geltenden Datenschutzregelungen des Landes enthaltenen Schutzvorschriften (s. § 3 Satz 1).

Nummer 1 benennt die Bedingungen, unter denen die erforderlichen Zugänge für die Administration durch externe IT-Dienstleister geschaffen werden. Abgestellt wird auf die existierenden IT-grundschutzkonformen Regelungen, wonach die administrativen Zugänge auf allen Ebenen zu personalisieren sind.

Abweichend vom Urteil des Hessischen Dienstgerichtshofs werden nach Halbsatz 1 nicht berechtigte Inhaberinnen oder Inhaber eines Masterpassworts bestimmt, sondern zugangsberechtigte Personen (Administratorinnen und Administratoren). Da die Rolle der Administratorinnen und Administratoren auf Anwendungsebene (z.B. File-System, Fachanwendung) eine Berechtigung umfassen kann, mittels derer eine Einsichtnahme in die hier geschützten Daten und Dokumente und damit ein Verstoß gegen das die in § 2 Absatz 2 Satz 2 Nummer 2 und 3 enthaltene Verbot möglich wäre, müssen die insoweit zugangsberechtigten Administratorinnen und Administratoren durch die Justizverwaltung selbst im Rahmen des von ihr zu definierenden Berechtigungsmanagements bestimmt werden. Soweit die zugangsberechtigten Administratorinnen und Administratoren im Bereich der übrigen Rollen (Backendsysteme, Active Directory und Betriebssysteme**)** durch den externen Dienstleister selbst bestimmt werden sollen, wäre durch die Justizverwaltung – etwa durch vertragliche Regelungen – jedenfalls sicherzustellen, dass der Bestimmung eine obligatorische Sicherheitsüberprüfung vorausgeht und dass diese administrativen Tätigkeiten sowie eine Veränderung von Berechtigungen vollumfänglich und revisionssicher protokolliert und die Protokolle der Justizverwaltung als Report zur Verfügung gestellt werden, um etwaige Verstöße gegen das Gesetz umgehend registrieren zu können.

Die Bedingungen für eine etwaige Öffnung für weitere administrativ berechtigte Personen (v.a.: Erforderlichkeit) müssen nach Halbsatz 2 von der Justizverwaltung in abstrakter Form vorab festgelegt werden.

Die Benachrichtigungspflicht und das Gebot der Verfahrensänderung in Halbsatz 3 sind Folgen einer unbefugten Zugangsgewährung und des damit einhergehenden Sicherheits- und Vertrauensverlustes. Die Interessen der Richterschaft, der Rechtspflegerinnen und Rechtspfleger sowie der Bediensteten der Staatsanwaltschaften werden durch eine Unterrichtung der IT-Kontrollkommission (§ 5) gewahrt. Die Leitung der jeweils zu unterrichtenden Gerichte und Staatsanwaltschaften sollte darüber hinaus eine interne Information der örtlichen Administration sicherstellen.

Nummer 2 untersagt den Administratorinnen und Administratoren noch einmal ausdrücklich das Einsehen der besonders geschützten Dokumente und deren Weitergabe an Dritte. Beides ist zur Erfüllung rein administrativer Aufgaben nicht erforderlich.

Geschützt sind zunächst richterliche Dokumente, die den Kernbereich der richterlichen Tätigkeit betreffen - in Abgrenzung zu solchen, die allein die Ordnung oder die Art der Ausführung eines Amtsgeschäfts betreffen (§ 26 Absatz 2 DRiG). Es handelt

sich um Dokumente, die im Rahmen der rechtsprechenden Tätigkeit bis zur abschließenden Entscheidung angefertigt werden wie z.B. Verfügungen, Beschlüsse und Urteile, Notizen, Entwürfe und Voten, Ladungen und Protokolle, unabhängig davon, wo sie entstehen und wo sie dann gespeichert sind. Davon erfasst sein werden deshalb sowohl Dokumente, die später ggf. Teil der E-Akte werden als auch Annotationen in der E-Akte.

Ein entsprechender Schutz gilt für Dokumente, die von Rechtspflegerinnen und Rechtspflegern im Rahmen ihrer sachlich unabhängigen Tätigkeit (§ 9 RPflG) erstellt werden. Speziell zum Schutz des Legalitätsprinzips (§§ 152 Absatz 2, 160 StPO) und zur Gewährleistung ungestörter Ermittlungsverfahren wird die Zugriffsbeschränkung schließlich auch auf Dokumente erstreckt, die in den Staatsanwaltschaften im Zuge der Ermittlungstätigkeit von Staats- und Amtsanwältinnen und -anwälten erstellt werden.

Das Verbot der Weitergabe schließt die Möglichkeit der Kenntnisnahme durch Dritte allerdings nicht schlechthin aus. Soweit der Dienstaufsicht oder anderen staatlichen Stellen eine inhaltliche Kenntnisnahme erlaubt oder eine solche gar geboten ist, kann die Weitergabe auf der Grundlage anderer Gesetze (z.B. StPO, LDSG, Dienstrecht des Landes) zulässig sein (s. Nummer 4) oder auch unmittelbar auf Veranlassung und mit Zustimmung des Verfassers oder der Verfasserin erfolgen (Nummer 5).

Nummer 3 definiert die Begriffe „Metadaten“ und „Logdateien“ und schützt diese ausdrücklich vor einer Weitergabe an Dritte. Bei den Metadaten handelt es sich um Informationen über Merkmale oder Eigenschaften von Dokumenten wie etwa deren Entstehungsprozess, über die Person des Erstellers und die Bearbeitungsumstände, z.B. die Zeit der Erstellung oder die Dauer der Bearbeitung. Logdateien enthalten systemintern automatisch erstellte Protokolle über die Benutzung der zur Verfügung stehenden IT und vermögen damit Auskunft zu geben über das Nutzungsverhalten einzelner Personen (z.B. Zeiten der An- und Abmeldung, Lese- und Schreibvorgänge auch in Datenbanken, Dokumentation von Verfahrensabläufen - "Workflow" -). Mithilfe der Metadaten und der Logdateien ließe sich theoretisch das Arbeitsverhalten einer einzelnen Nutzerin oder eines einzelnen Nutzers in einem Umfang nachzeichnen, der selbst über das zulässige Maß der allgemeinen Dienstaufsicht nach § 26 Absatz 2 DRiG hinausgeht (vgl. HessDGH, a.a.O. Umdr. S. 23 f., in juris Rn. 69).

Die Einsicht- bzw. Kenntnisnahme dieser Daten und Dateien ist hier nicht ausdrücklich untersagt. Eine solche lässt nicht sich im Rahmen der Administration nicht immer verhindern (zu den Metadaten zählt etwa auch ein Dateiname). Insoweit gilt deshalb nur Nummer 5.

Nummer 4 formuliert eine Ausnahmemöglichkeit von den Regelungen der Nummer 2 und 3 zugunsten der Protokollierung und Kontrolle zu dienstlichen Zwecken (etwa für den Fall eines konkreten Missbrauchsverdachts zu dienstfremden Zwecken). Denn auch die Dienstaufsicht über Richterinnen und Richter umfasst die Befugnis zur Prüfung, ob die überlassenen Arbeitsmittel ausschließlich für dienstliche Zwecke ge-

braucht werden (vgl. HessDGH, a.a.O. Umdr. S. 26, in juris Rn. 75 m.w.N.). Eine entsprechende Regelung besteht derzeit in Ziffer 6. der Richtlinie zur Nutzung von Internet und E-Mail vom 17. Dezember 2009 für alle Beschäftigten der Gerichte, Staatsanwaltschaften und des Justizvollzugs im Geschäftsbereich des für Justiz zuständigen Ministeriums (Vereinbarung nach § 57 MBG Schl.-H.). Eine Einsicht im Rahmen der Rechts- bzw. Fachaufsicht bei der Staatsanwaltschaft ist durch diese Regelung im Übrigen nicht ausgeschlossen, sollte allerdings unabhängig von der externen Administration der IT sichergestellt werden.

In Bezug auf Richterinnen und Richter, Rechtspflegerinnen und Richter erscheint es im Übrigen grundsätzlich ausreichend, wenn die IT-Administration eine Einsicht zu Zwecken der allgemeinen Dienstaufsicht in Dokumente abgeschlossener Verfahren ermöglicht. Die Einsichtnahme in Dokumente laufender Verfahren muss hingegen „unerlässlich“ sein (z.B. im Rahmen von Disziplinarverfahren).

Nummer 5 stellt schließlich klar, dass auch alle anderen als die in Nummer 2 und 3 speziell behandelten Verwendungen von Dokumenten, Metadaten und Logdateien durch die Administration grundsätzlich untersagt sind. Der Begriff „Verwendung“ entspricht dem des § 2 Absatz 2 Satz 1 LDSG und umfasst jeden Umgang mit den bezeichneten Dokumenten, Daten und Dateien, mithin auch die vom Hessischen Dienstgerichtshof ausdrücklich erwähnten „inhaltlichen Zugriffe“, die Einsichtnahme oder das Speichern. Eine Ausnahme wird insoweit aber zugelassen für Verwendungen, die betriebsnotwendig und aus technischen Gründen "unerlässlich“ sind. Dies gilt zum einen für die Gewährleistung der Ordnungsmäßigkeit automatisierter (Fach-)Verfahren, die nach § 8 Absatz 2 LDSG auf zentrale Stellen übertragen werden kann (vgl. § 7 Absatz 2) und zum anderen etwa bei erforderlichen Datensicherungen, Reparaturen, Neuinstallationen usw. (vgl. Hess. DGH, Urt. v. 20.04.2010 - DGH 4/08 - Umdr. S. 16 f. und 30, in juris Rn. 52 ff., 84).

Die Pflicht zur Protokollierung in Nummer 6 umfasst in Anlehnung an die Regelungen des Datenschutzrechts jeglichen Zugriff durch Administratorinnen und Administratoren: sowohl auf Daten, Dokumente und Einträge in Justizdatenbanken als auch solche Zugriffe, mit denen Änderungen an automatisierten Verfahren und damit am System selbst bewirkt werden. Die Pflicht zur Mitteilung der protokollierten Zugriffe gilt generell, also sowohl für erlaubte als auch – und erst recht – für unerlaubte Zugriffe. Ihre Einhaltung wird durch die Protokollierung abgesichert. Die Mitteilung erfolgt im Falle eines externen Zugriffs gegenüber dem für Justiz zuständigen Ministerium (GemIT) unverzüglich und auf direktem Weg, damit dieses die ggf. erforderlichen technischen und organisatorischen Schritte veranlassen kann, u.a. die Information betroffener Verfasserinnen und Verfasser bzw. Nutzerinnen und Nutzer.

Entsprechendes gilt für den Fall, dass der Zugriff durch die im Ministerium selbst angesiedelte GemIT erfolgt.

zu § 3

Die Regelung ist deklaratorischer Art und beschränkt sich auf das Verhältnis zu anderen Landesgesetzen, weil nur insoweit eine gesetzliche Konkurrenz entstehen könnte (Art. 31 GG). Neben dem Landesdatenschutzgesetz (LDSG) unberührt bleiben ohnehin die allgemeinen und bereichsspezifischen Datenschutzregelungen (z.B. Sozialdatenschutz), die Prozessordnungen des Bundes und darauf basierende Landesverordnungen.

Die Erwähnung des LDSG hebt zugleich die gesonderte Bedeutung des Datenschutzrechts und dessen Geltung für alle beteiligten Stellen hervor. Dies gilt auch für die Datenverarbeitung durch Dataport (§ 15 Absatz 1 StV). Die bestehenden Regelungen im Bereich des Datenschutzes und der Datensicherheit sind überall dort zu beachten, wo es zugleich zur Verarbeitung personenbezogener Daten kommt. Dies wird in vielen Konstellationen der Fall sein. Diese Parallelität gesetzlicher Regelungen ist unvermeidbar, weil die Zielrichtung und die Schutzbereiche des LDSG einerseits und des vorliegenden Gesetzes andererseits nicht identisch sind. So werden etwa in den von § 2 Absatz 2 Satz 2 geschützten Dokumenten zwar häufig, aber eben nicht notwendig auch personenbezogene Daten natürlicher Personen enthalten sein. Hierauf weist auch der Hessische Dienstgerichtshof hin und führt aus, dass es bei dem in Rede stehenden Schutz vorrangig darum geht, „wie unter Berücksichtigung des Gewaltenteilungsgrundsatzes staatliche Stellen mit ihnen anvertrauten Daten einer anderen staatlichen Gewalt umzugehen haben, und zwar auch dann, wenn es sich nicht um personenbezogene Daten handelt. Dementsprechend enthält das (…) Datenschutzgesetz keine Bestimmungen und Instrumente bereit, die diesen Schutz betreffen“ (HessDGH a.a.O. Umdr. S. 27 f., in juris Rn. 80). Aus dieser Parallelität folgt u.a., dass die Vorgaben des § 17 LDSG - Auftragsdatenverarbeitung - auch im Verhältnis zu Dataport und ebenso im Verhältnis zur GemIT (§ 4) gelten und dass die Prüfungsbefugnisse des behördlichen / gerichtlichen Datenschutzbeauftragten oder des Unabhängigen Landeszentrums für Datenschutz neben die Kontrollbefugnisse der GemIT (§ 4 Absatz 3) und der IT-Kontrollkommission (§ 5 Absatz 5, 6 und 8) treten, auch wenn sich die Kontrollbereiche zum Teil überschneiden. Um doppelte Infrastrukturen und Kosten für die Organisation und Durchführung von Kontrollen zu reduzieren, sieht § 4 Absatz 4 Satz 3 (entsprechend: § 5 Absatz 5 Satz 2) eine Unterrichtungspflicht vor.

Klargestellt wird darüber hinaus, dass die gesetzlichen Aufgaben und die vorgeschriebene Beteiligung der Personalvertretungen und der Stufenvertretungen in den verschiedenen Dienststellen unberührt bleiben (§§ 36, 40 LRiG, §§ 47 - 59 MBG Schl.-H.). Die Umsetzung der im vorliegenden Gesetz enthaltenen Regelungen und die hier vorgesehenen Verfahren können zwar auch innerdienstliche mitbestimmungspflichtige Maßnahmen beinhalten oder auslösen, doch ist die Zielrichtung des IT-Justizgesetzes eine andere. Dies wird exemplarisch deutlich bei der IT-Kontrollkommission, deren Mitglieder nach § 5 Absatz 2 zwar von den Mitbestimmungsgremien benannt werden, aber keine Mitbestimmungsaufgaben wahrzunehmen hat. Ihre

Aufgabe ist es gemäß § 5 Absatz 1 vielmehr, auf den Schutz der richterlichen Unabhängigkeit, der sachlichen Unabhängigkeit der Rechtspflegerinnen und -pfleger und des Legalitätsprinzips zu achten (s. Begründung dort).

zu § 4

Absatz 1

§ 4 Absatz 1 Satz 1 stellt die grundsätzliche Ressortverantwortung des für Justiz zuständigen Ministeriums für die IT in den Gerichten und Staatsanwaltschaften klar. Diese gilt unabhängig vom Ort der konkreten Aufgabenerfüllung. Umfasst sind sowohl die sachliche als auch die politische Verantwortung, mithin auch die diesbezügliche Haushaltsplanung und Verwaltung der Mittel. Dessen ungeachtet sollen die Koordinierung der Bedarfe und der Dialog über die Notwendigkeit von Anschaffungen unter Einbindung der Gerichte und Staatsanwaltschaften weiterhin im Vordergrund stehen.

Konsequenterweise erfolgt die Einrichtung einer justizeigenen Gemeinsamen IT-Stelle (GemIT) speziell für die IT in den Gerichten und Staatsanwaltschaften gemäß Satz 2 direkt im Ministerium. Bei der Vorgabe, eine solche Stelle behördenintern einzurichten, handelt es sich um eine aus Gründen der Gewaltenteilung grundlegende Entscheidung, die der Gesetzgeber selbst trifft. Sie zielt auf die notwendige Abgrenzung der Aufgaben für die Exekutive einerseits und für die Judikative andererseits und dient der Schaffung klar ersichtlicher Strukturen und Verantwortlichkeiten. Nur so lässt sich etwa die in § 5 Absatz 5 vorgesehene Überwachung der Einhaltung geltender Regelungen aufseiten der GemIT durch die IT-Kontrollkommission realisieren (im Übrigen unterliegt die IT-Organisation des Ministeriums und der sonstigen, ihm nachgeordneten Stellen weiterhin dem zentralen Management durch die für die Angelegenheiten der ressortübergreifenden IT zuständige oberste Landesbehörde, den Vorgaben des Organisationserlasses ITSH und der exekutiven Aufsicht). Für die Einrichtung der GemIT genügt ein behördeninterner Akt, der zugleich die Geschäftsabläufe regelt. Gemäß 1.4 des Umsetzungsplans zur Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung des IT-Planungsrates (dazu Vertrag zur Ausführung von Artikel 91c GG [IT-Staatsvertrag] zwischen dem Bund und den Ländern nebst Zustimmungsgesetz vom 19.03.2010, GVOBl 2010, S. 384) ist zugleich ein unabhängiger Sicherheitsbeauftragter vorzusehen.

Geregelt werden muss nach Satz 3 weiterhin die Zusammenarbeit mit den einzelnen im Organisationserlass ITSH aufgeführten Einrichtungen des IT-Managements der Landesverwaltung (CIO, Zentrales und Dezentrales IT-Management, IT-Beauftragtenkonferenz, Landes-IT-Rat), da die Aufgaben der GemIT nicht unter die Regelungen des Organisationserlasses ITSH fallen. Die in diesem Zusammenhang erforderlich werdenden Vorgaben können nur im Einvernehmen mit der für die Angelegenheiten der ressortübergreifenden IT zuständigen obersten Landesbehörde erfolgen.

Absatz 2

Satz 1 stellt klar, dass die Anwenderbetreuung in den Gerichten und Staatsanwaltschaften durch dezentrale und jeweils eigene IT-Stellen und damit auch durch eigenes Personal erfolgt, so dass sich insgesamt für die Justiz ein mehrstufiger Aufbau der justizeigenen IT-Stellen ergibt und diesen gesetzlich sichert.

Die konkrete Aufgabenteilung zwischen GemIT und den dezentralen IT-Stellen hängt im Übrigen von einzelfall- und verfahrensbezogenen Faktoren ab und bleibt deshalb gemäß Satz 2 einer gesonderten Regelung durch das für Justiz zuständige Ministerium vorbehalten. Aufgrund der Bedeutung dieser Regelung für die Austarierung zwischen Exekutive und Judikative wird die Form der Rechtsverordnung gewählt und eine Anhörung der IT-Kontrollkommission (§ 5) vorgeschrieben, der insoweit eine planerische Mitsprache eingeräumt wird.

Die Aufgabenübertragung auf in den Gerichten und Staatsanwaltschaften vorhandenen (oder neu zu schaffenden) IT-Stellen hat den Vorteil, dass die Personalverantwortlichkeit einschließlich Dienst- und Fachaufsicht vor Ort verbleibt (bzw. entsteht), der Verordnungsgeber jedoch nicht gehindert ist, der GemIT die Befugnis einzuräumen, inhaltliche Vorgaben zu machen.

Satz 3 gibt für die Rechtsverordnung inhaltlich vor, dass die Aufgabenverantwortung in grundlegenden Angelegenheiten der IT in den Gerichten und Staatsanwaltschaften der GemIT zugewiesen wird. Zu den grundlegenden Angelegenheiten gehören etwa die Einordnung der schleswig-holsteinischen Strategie in den länderübergreifenden Entwicklungsprozess, die Zusammenarbeit in den bundesweiten Entwicklungsverbünden (auch wenn sie in Kooperation mit den zuständigen Gerichten und Staatsanwaltschaften umgesetzt wird), der Abschluss kostenwirksamer Vereinbarungen in den Verbünden und die operative Auftraggeberrolle gegenüber externen IT-Dienstleistern. Der damit verbundene Bedarf an Organisation und Koordination kann nur von zentraler Stelle aus abgedeckt werden, zumal hier auch die politische Verantwortung liegt. Im Übrigen werden auch die strategische Entwicklung, Einführung und Pflege eigener IT-Basisinfrastrukturen und Fachverfahren und damit zum Beispiel die Weiterentwicklung der rechtlichen und technischen Rahmenbedingungen des IT-Einsatzes sowie schließlich Fragen der Ausstattung der Dienststellen und der Organisation der Anwenderbetreuung zu den grundlegenden Angelegenheiten gezählt werden können. Die Vor-Ort-Betreuung soll hingegen auch künftig im notwendigen Umfang in den dezentralen IT-Stellen durch eigene Bedienstete der Gerichte und Staatsanwaltschaften wahrgenommen werden.

Satz 4 ermöglicht es dem Ministerium allerdings auch, die als grundlegend zu definierenden Angelegenheiten auf die dezentralen IT-Stellen in den Gerichten und Staatsanwaltschaften zu übertragen, soweit dies erforderlich oder jedenfalls zweckdienlich erscheint – z.B. für einzelne Sondervorhaben oder für die Pflege spezieller Fachverfahren einzelner Gerichtsbarkeiten. Insoweit kann nach Satz 5 schließlich

auch die Einrichtung von Verfahrenspflegestellen und eine Zusammenarbeit verschiedener Gerichtsbarkeiten vorgesehen werden.

Absatz 3

Aufgrund ihrer zentralen Zuständigkeit und der bestehenden Sachnähe erhält die GemIT über die aus den Benutzungsverhältnissen / Verträgen folgenden Rechte hinaus mit Satz 1 zugleich eine eigene gesetzliche Kontrollbefugnis gegenüber den externen IT-Dienstleistern der Justiz. Diese Befugnis versetzt sie in die Lage, im Rahmen der in Satz 2 beschriebenen Bereiche dafür Sorge zu tragen, dass es in den IT-Strukturen der Gerichte und Staatsanwaltschaften im Rahmen der administrativen Praxis der externen IT-Dienstleister nicht zu unbefugten Zugriffen kommt bzw. kommen kann. Als unbefugter Zugriff durch eine Mitarbeiterin oder einen Mitarbeiter externer IT-Dienstleister ist auch die missbräuchliche oder nicht den geltenden Regelungen entsprechende Eröffnung von Zugriffsmöglichkeiten für Dritte innerhalb oder außerhalb der Justiz anzusehen. Kontrolliert werden kann damit auch die Einhaltung von Gesetzen, Verträgen und sonstigen im Gesetz näher umschriebenen Bestimmungen.

Die Befugnisse in Satz 3 und 4 begründen die zur Aufgabenerfüllung erforderlichen Zutritts-, Auskunfts- und Akteneinsichtsrechte und die Befugnis zur Erhebung personenbezogener Daten, soweit dies zur Ausübung der Kontrolle erforderlich ist, vergleichbar der Regelung des § 41 Absatz 1 LDSG. Soweit allerdings (zugleich) Dokumente, Dateien und Daten i.S.d. § 2 Absatz 2 Satz 2 Nummer 2 und 3 betroffen sind, dürfen diese nach Satz 5 im Rahmen von Kontrollen nur eingesehen oder sonst verwendet werden, soweit dies zur Aufgabenerfüllung unerlässlich ist. Dieses Schutzniveau entspricht dem des § 2 Absatz 2 Satz 2 Nummer 4 und 5.

Soweit die GemIT im Falle festgestellter Mängel bei den externen IT-Dienstleistern aus kompetenzrechtlichen Gründen selbst keine Abhilfe schaffen kann, kann die gleichzeitig gemäß § 5 Absatz 5 zu unterrichtende IT-Kontrollkommission gemäß § 5 Absatz 8 verfahren.

Absatz 4

Die rechtzeitige Unterrichtung der GemIT über geplante Kontrollen anderer öffentlicher Stellen bei Dataport oder anderen externen IT-Dienstleistern und die zeitnahe Unterrichtung über deren Ergebnisse schafft die Möglichkeit von Synergien und dient zugleich der informierten Aufgabenerfüllung durch die GemIT. Je nach Kontrollgegenstand und Ergebnis kann sie an den Kontrollen teilnehmen bzw. auch von eigenen Kontrollen absehen. Dies trägt zur Vermeidung doppelter Infrastrukturen und Kosten für Organisation und Durchführung von Kontrollen bei. Zur weiteren Vereinfachung des Verfahrens könnte die Unterrichtung im Rahmen einer hierfür eingerichteten Arbeitsgruppe sämtlicher beteiligter Stellen einschließlich der IT-Kontrollkommission erfolgen, um zugleich die Unterrichtungs- und Beteiligungspflichten nach § 5 Absatz 5 Satz 2 zu erfüllen.

Um die unabhängige Aufgabenwahrnehmung durch das Unabhängige Landeszentrum für Datenschutz nicht zu beeinträchtigen, beschränkt sich dessen Pflicht aus Satz 3 auf eine nachgängige zeitnahe Unterrichtung über durchgeführte Kontrollen der Auftragnehmerinnen und Auftragnehmer der Daten verarbeitenden Stelle, d.h. zum frühest möglichen Zeitpunkt.

Absatz 5

Auch die Pflicht zur nachträglichen, aber unverzüglichen Unterrichtung über Sicherheitsvorfälle, die (auch) die Justiz betreffen, soll die GemIT in die Lage versetzen, ihre Aufgaben zum Schutze der Funktionsfähigkeit und der besonderen Belange der Justiz jederzeit sachgerecht und zielorientiert wahrnehmen zu können. Der Begriff „Sicherheitsvorfälle“ umfasst Störungen der informationstechnischen Systeme, Komponenten oder Prozesse oder auch andere Vorfälle, die zu Gefahren für Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit sowohl von Daten im Allgemeinen als auch von den mit diesem Gesetz geschützten Dokumenten im Besonderen führen. Er umfasst damit auch den Schutz der besonderen Belange der Justiz i.S.v. § 2. Die Unterrichtungspflicht trifft diejenigen Stellen, die mit der praktischen Betreuung befasst sind, mithin die für die Angelegenheiten der ressortübergreifenden IT zuständige oberste Landesbehörde und die Administration der eingeschalteten IT-Dienstleister.

zu § 5

Absatz 1

Die Einrichtung einer unabhängigen IT-Kontrollkommission gemäß Satz 1 ist Konsequenz der zitierten Entscheidung des Hessischen Dienstgerichtshofs. Die IT-Kontrollkommission repräsentiert die Judikative gegenüber der Exekutive im organisatorischen Umfeld des von der Exekutive verantworteten IT-Betriebes und vertritt die Belange und Interessen der Judikative. Sie nimmt damit neben der bestehenden Mitbestimmung ein ganz eigenes „Wächteramt“ wahr. Ohne die hier geschaffene Kontrollmöglichkeit würde der Betrieb der justizeigenen IT durch die Exekutive die richterliche Unabhängigkeit beeinträchtigen (vgl. HessDGH, Urteil vom 20.04.2010, Umdr. S. 25, 27, in juris Rn. 73, 76 f.). Die sich aus der Entscheidung des Hessischen Dienstgerichtshofs ergebenden Anforderungen werden auf den Schutz der sachlichen Unabhängigkeit der Rechtspflegerinnen und Rechtspfleger und des Legalitätsprinzips im Bereich der Aufgaben von Staatsanwältinnen und Staatsanwälten erstreckt. Die konkreten Aufgaben und Befugnisse der IT-Kontrollkommission ergeben sich aus den einzelnen Vorschriften des Gesetzes. Neben der Kontrollbefugnis sind dort auch Anhörungsrechte in Hinblick auf planerische und gestalterische Entscheidung vorgesehen. Art und Umfang der Aufgabenwahrnehmung regelt die IT-Kontrollkommission im Übrigen durch eine Geschäftsordnung (Absatz 9).

Die Einrichtung der IT-Kontrollkommission beim Ministerium dient allein organisatorischen Zwecken und berührt nicht die gebotene Unabhängigkeit der IT-Kontrollkommission insbesondere vom Ministerium selbst.

Satz 2 bestimmt, dass das Ministerium eine Geschäftsstelle vorzuhalten hat, die Versorgung mit den erforderlichen Sach- und Fachmitteln sicherstellt und auch alle weiteren durch die Tätigkeit der IT-Kontrollkommission entstehenden Kosten trägt. Nähere Einzelheiten können der entsprechend anzuwendenden Vorschrift des § 34 MBG Schl.-H. entnommen werden. Umfasst sind damit insbesondere auch Kosten für notwendige Reisen der Mitglieder.

Absatz 2

Die Zusammensetzung der IT-Kontrollkommission stellt sicher, dass jede Berufsgruppe und jede Gerichtsbarkeit mit ihren spezifischen fachlichen Anforderungen vertreten sein kann. Dabei kommt es nicht auf die Größe der Gerichtsbarkeit an.

Die Mitbestimmungsgremien sollten aus dem Kreis derjenigen Bediensteten in den Gerichten und Staatsanwaltschaften eine Person benennen, deren Interessen sie jeweils vertreten. Diese Person sollte neben einem gewissen technischen Grundverständnis insbesondere auch die fachlichen Besonderheiten ihrer Gerichtsbarkeit bzw. ihrer Gruppe mitbringen oder jedenfalls bereit sein, diese zu erwerben. Satz 1 und 2 schließen nicht aus, dass ein Mitglied zugleich mehrere (kleine) Gerichtsbarkeiten vertritt, sofern sich zuständigen Mitbestimmungsgremien darauf einigen.

Satz 2 verpflichtet jeden Personal- bzw. Richterrat neu, unverzüglich zu Beginn seiner Amtsperiode ein Mitglied der Kontrollkommission zu benennen. Dies gewährleistet, dass die Mitglieder bis zur (Neu-) Benennung im Amt bleiben und schließt die Möglichkeit einer vorzeitigen Abberufung aus. Ihre Unabhängigkeit auch gegenüber den Mitbestimmungsgremien ist damit gesichert. Das Verfahren erübrigt darüber hinaus die Etablierung eines eigenen Wahlverfahrens.

Je nach personellen Kapazitäten können nach Satz 3 mit der Benennung der einzelnen Mitglieder jeweils eine Vertreterin oder ein Vertreter benannt werden, die im Falle der zeitweiligen Verhinderung eines Mitglieds tätig werden. Im Falle des endgültigen Ausscheidens (etwa wegen Niederlegung des Amtes oder Beendigung des Dienstverhältnisses) erfolgt nach Satz 4 eine Nachbenennung.

Absatz 3

Entsprechend § 37 MBG Schl.-H. steht auch den Mitgliedern der IT-Kontrollkommission ein Fortbildungsanspruch zu.

Absatz 4

Entsprechend § 36 MBG Schl.-H. sind die Mitglieder im Interesse einer ordnungsgemäßen Wahrnehmung ihrer Aufgaben im erforderlichen Umfang von ihrer dienstli-

chen Tätigkeit freizustellen. Die Freistellung ist unabhängig von der Wahrnehmung sonstiger Ämter und damit verbundener Freistellungen zu gewähren.

Absatz 5

Die in Satz 1 beschriebene Kontrollbefugnis der IT-Kontrollkommission besteht unabhängig von und gleichberechtigt neben der Kontrollbefugnis der GemIT nach § 4 Absatz 3 und geht noch darüber hinaus, weil sie sich nicht auf die externen IT-Dienstleister beschränkt, sondern alle in § 1 Absatz 1 genannten Stellen einschließlich der GemIT selbst erfasst. Sie muss deshalb auch die Möglichkeit beinhalten, eine Kontrolle eigeninitiativ anzustoßen.

Nach Satz 2 gelten gegenüber der IT-Kontrollkommission die gleichen Unterrichtungs- und Beteiligungsverpflichtungen anlässlich von Kontrollen durch andere öffentliche Stellen wie gegenüber der GemIT nach § 4 Absatz 4 und 5. Zusätzlich wird die GemIT selbst gegenüber der IT-Kontrollkommission verpflichtet, da sie dem für Justiz zuständigen Ministerium angehört und damit einer der in § 1 Absatz 1 genannten Stellen. Die bereits von der GemIT festgestellten und mitzuteilenden Verstöße können bei Bedarf von der IT-Kontrollkommission gemäß Absatz 8 behandelt werden.

Absatz 6

Satz 1 und 2 begründen die zur umfassenden Aufgabenerfüllung erforderlichen Zutritts-, Auskunfts- und Akteneinsichtsrechte gegenüber den in § 1 Absatz 1 genannten Stellen. Satz 3 schafft eine umfassende Rechtsgrundlage zur Datenerhebung und -einsicht zu Kontrollzwecken. Ein über die Einsichtnahme hinausgehender Verwendungsbedarf besteht insoweit nicht. Als Repräsentanten der Judikative werden der IT-Kontrollkommission im Vergleich zur GemIT (in § 4 Absatz 3 Satz 5), die der Exekutive zugehört und ihrerseits den Bestimmungen des § 2 unterliegt, bewusst weitergehende Befugnisse eingeräumt.

Absatz 7

Eine notwendig werdende Beratung und Hinzuziehung externen Sachverstandes soll nach Möglichkeit kostenneutral verlaufen. Sachkundige Beschäftigte sind z.B. behördliche Datenschutzbeauftragte oder IT-Sicherheitsbeauftragte (z.B. nach § 4 Absatz 1 Satz 2). Die Beratungspflicht durch das Unabhängige Landeszentrum für Datenschutz geht zwar über den Anwendungsbereich des Landesdatenschutzgesetzes hinaus, erscheint in Anbetracht der dort vertretenen fachlichen Kompetenz allerdings sinnvoll und deshalb geboten. Sie ist für öffentliche Stellen kostenfrei.

Absatz 8

Im Falle der Feststellung von Verstößen hat die IT-Kontrollkommission die Befugnis, von den Stellen i.S.d. § 1 Absatz 1 unter Setzung einer im Einzelfall angemessenen Frist Abhilfe zu fordern und / oder gegebenenfalls eine Beanstandung auszuspre-

chen. Die Instrumente der Aufforderung zur Mängelbeseitigung und Beanstandung bei gleichzeitiger Unterrichtung der Aufsichtsbehörde entsprechen denen des Unabhängigen Landeszentrums für Datenschutz (§ 42 LDSG). Da die IT-Kontrollkommission gegenüber den Stellen i.S.d. § 1 Absatz 1 und insbesondere gegenüber den externen IT-Dienstleistern weder über Aufsichtsbefugnisse verfügt noch Auftraggeberin bzw. Vertragspartnerin ist, bleibt nur der Weg über die Beanstandung und Unterrichtung der zuständigen Aufsichtsstelle bzw. des jeweiligen Auftraggebers / Vertragspartners mit dem Ziel, dass diese per Weisung bzw. im Rahmen des öffentlich-rechtlichen Benutzungsverhältnisses / Vertragsverhältnisses für Abhilfe sorgen.

Absatz 9

Art und Umfang der Aufgabenwahrnehmung sowie die innerorganisatorischen Abläufe regelt die IT-Kontrollkommission im Übrigen durch eine eigene Geschäftsordnung.

zu § 6

Die in der öffentlichen Verwaltung des Landes zur Aufgabenerfüllung erforderliche und zu diesem Zweck eingesetzte Standard-IT wird durch die für die Angelegenheiten der ressortübergreifenden IT zuständige oberste Landesbehörde bestimmt und in Zusammenarbeit mit Dataport bereitgestellt. Nach Ziffer 10.1 OrgErl ITSH wird diese Standard-IT (Standard Arbeitsplatz, Standard Funktionalitäten und Standard Infrastruktur) durch die IT-Gesamtstrategie des Landes definiert und ist zu nutzen. Ähnlich verhält es sich mit den sogenannten zentralen Diensten des Landes (Basisdiensten) i.S.d. § 8 Absatz 1 und 2 EGovG, deren nähere Ausgestaltung durch Regelung in einer Verordnung ebenfalls der für die Angelegenheiten der ressortübergreifenden IT zuständigen obersten Landesbehörde obliegt (§ 8 Absatz 3 EGovG).

Als Organe der Rechtspflege werden die Gerichte und Staatsanwaltschaften von den Regelungen des Landes-E-Government-Gesetzes (§ 1 Satz 4 EGovG) nicht erfasst. Entsprechendes gilt gemäß Ziffer 2.4 OrgErl ITSH. Hier ist zudem ausdrücklich klargestellt, dass in diesen Fällen das für Justiz zuständige Ressort entscheidet. Dies ändert aber nichts an dem Umstand, dass die Gerichte und Staatsanwaltschaften in der Praxis keine eigene IT-Infrastruktur unterhalten, sondern dass sie hinsichtlich der Standard-IT und auch hinsichtlich der Basisdienste in die ressortübergreifenden IT-Strukturen eingebunden sind.

Absatz 1

Die für die Angelegenheiten der ressortübergreifenden IT zuständige oberste Landesbehörde wird verpflichtet dafür Sorge zu tragen, dass auch die Justiz mit der vorhandenen Standard-IT und den erforderlichen Basisdiensten des Landes ausgestattet werden kann und die dazugehörige Betreuung durch Dataport erfährt. Soweit erforderlich, müssen zu diesem Zweck entsprechende vertragliche Regelungen mit Dataport getroffen werden. Die nach § 2 Absatz 2 Satz 1 vorgeschriebene techni-

sche Trennung gilt insoweit nicht. Sie bezweckt den Schutz der besonderen Belange der Justiz im Sinne des § 2 Absatz 1 Satz 1 und gilt deshalb nur für solche Verfahren und Anwendungen, die den Umgang mit Dokumenten des richterlichen oder rechtspflegerischen Entscheidungsprozesses sowie der vom Legalitätsprinzip getragenen Ermittlungs- und Anklagetätigkeit berühren. Unbedenklich ist deshalb z.B. die Nutzung der zentralen Standard-IT Funktionalitäten im Bereich des Personalmanagements oder des Haushaltswesens.

Absatz 2

Die Entscheidung über den Einsatz der in der Landesverwaltung genutzten Standard-IT und deren einzelne Funktionen sowie über die etwaige Nutzung von Basisdiensten des Landes in den Gerichten und Staatsanwaltschaften wird nicht zentral durch die für die Angelegenheiten der ressortübergreifenden IT zuständige oberste Landesbehörde getroffen, sondern dem für die Organisation der IT in den Gerichten und Staatsanwaltschaften verantwortlichen Ministerium zugewiesen nach Anhörung der IT-Kontrollkommission (§ 5), der auch insoweit eine planerische Mitsprache eingeräumt wird.

Soweit dies erforderlich erscheint, kann zusätzlich die Einrichtung justizeigener IT-Standards vorgesehen werden. Die Entscheidung hierüber bleibt jedoch im Ermessen des Ministeriums, das insoweit im Interesse des Landes auch wirtschaftliche Fragen berücksichtigen muss.

Absatz 3

Satz 1 bestimmt, dass die nach Absatz 2 in der Justiz eingesetzte Standard-IT und die verwendeten Basisdienste prinzipiell in entsprechender Anwendung des Landes-E-Government-Gesetzes und der auf dieser Grundlage getroffenen Bestimmungen erfolgen kann, um insoweit den Gleichlauf der Systeme zu gewährleisten. Vorrangig sind allerdings die spezielleren Regelungen dieses Gesetzes, insbesondere die aus § 2 abzuleitenden Vorgaben zu beachten.

Da die Justiz insoweit kein eigenes Benutzungsverhältnis zu Dataport begründet, sondern grundsätzlich gemeinsam mit der übrigen Landesverwaltung zentral mit der Standard-IT und den Basisdiensten versorgt wird, stellen die Sätze 2 und 3 sicher, dass die für die Angelegenheiten der ressortübergreifenden IT- zuständige oberste Landesbehörde die von ihr durch öffentlich-rechtlichen Vertrag zentral begründeten Benutzungsverhältnisse zu Dataport so ausgestaltet und praktiziert, dass die Funktionsfähigkeit der Justiz nicht beeinträchtigt und die besonderen Belange der Justiz gewahrt werden.

Absatz 4

Die Unterrichtungspflicht dient insbesondere dem Erhalt der Funktionsfähigkeit der Justiz; sie wirkt präventiv und hilft, etwaigen Störungen vorzubeugen. Die Beschränkung auf „wesentliche“ Änderungen entspricht den Formulierungen im Landesdaten-

schutzgesetz (vgl. § 5 Absatz 2, § 7 Absatz 3 und § 9 Absatz 1 LDSG) und stellt sicher, dass einfache Änderungen und Updates die Unterrichtungspflicht noch nicht auslösen.

zu § 7

Absatz 1

„Fachverfahren“ sind nach der Definition des § 2 Nummer 4 EGovG solche Verfahren, bei denen die thematisch als zusammengehörig empfundene Verarbeitung von Informationen zu einem dienstlichen Zweck erfolgt. In der Praxis der Justiz sind dies einerseits fachspezifische Anwendungen wie z.B. forumSTAR in der ordentlichen Gerichtsbarkeit oder das in der Sozial-, Finanz- und Verwaltungsgerichtsbarkeit eingesetzte Verfahren EUREKA-Fach, andererseits aber auch solche Verfahren, die ohne fachlichen Bezug einem bestimmten Zweck dienen, z.B. der Anbindung und Betreuung des elektronischen Rechtsverkehrs via Elektronisches Gerichts- und Verwaltungspostfach - EGVP- oder der Führung elektronischer Akten als etablierte Standards. Sämtlichen Fachverfahren ist gemeinsam, dass sie jeweils auf die vorhandene Standard-IT oder auf spezielle IT-Basisinfrastrukturen aufsatteln.

Diese justizeigenen, in den einzelnen Gerichtsbarkeiten und in den Staatsanwaltschaften benötigten Fachverfahren werden auf der Grundlage gesonderter Verträge zwischen dem für Justiz zuständige Ministerium und Dataport von Dataport bereitgestellt und betrieben. Im Einzelfall kann das Ministerium die Befugnis zur Beauftragung Dataports auf eine ihm nachgeordnete Stelle delegieren (vgl. § 4 Absatz 2 Satz 4). Soweit die Justiz selbst außenstehende Dritte einschaltet, hat auch sie die Vorgaben dieses Gesetzes zu beachten.

Absatz 2

Absatz 2 berücksichtigt eine weitere Parallelität zum Landesdatenschutzrecht. Sofern ein in der Justiz eingesetztes automatisiertes Fachverfahren von mehreren datenverarbeitenden Stellen, d.h. von mehreren Gerichten oder Staatsanwaltschaften eingesetzt wird (z.B. forumSTAR in der ordentlichen Gerichtsbarkeit), handelt es sich datenschutzrechtlich um ein gemeinsames Verfahren i.S.d. § 8 Absatz 1 LDSG.
§ 8 Absatz 2 LDSG erlaubt in diesen Fällen, die bei der einzelnen datenverarbeitenden Stelle liegende Verantwortung für die Gewährleistung der Ordnungsmäßigkeit des automatisierten Verfahrens durch eine Verordnung der für das Verfahren zuständigen obersten Landesbehörde von der Verantwortung für die gespeicherten Daten abzutrennen und auf eine zentrale Stelle zu übertragen. Hiervon Gebrauch zu machen, bietet sich etwa an für die nach § 5 Absatz 2 LDSG durchzuführenden Tests und Freigaben automatisierter Verfahren vor ihrem erstmaligen Einsatz und nach wesentlichen Änderungen. Um die einzelnen Gerichte oder Staatsanwaltschaften von dieser Pflicht zu befreien, könnte das für Justiz zuständige Ministerium für

diese Aufgabe eine zentrale Stelle bestimmen und zugleich die Einzelheiten über die Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung regeln. Während sich aus § 13 Absatz 6 LDSG ergibt, dass diese zentrale Stelle im Rahmen der ihr übertragenen Aufgaben zweckgebunden auch personenbezogene Daten verwenden darf, bietet das Landesdatenschutzgesetz keine hinreichende Ermächtigungsgrundlage für Regelungen in Bezug auf die sich aus dem IT-Justizgesetz ergebenden Besonderheiten. Insofern wird die Verordnungsermächtigung aus § 8 Absatz 2 LDSG erweitert, indem die justizintern für automatisierte Fachverfahren zuständige zentrale Stelle zugleich zu verpflichten ist, die Vorgaben des § 2 Absatz 2 Satz 2 zu beachten. Darüber hinaus ist auch insoweit eine Mitwirkung und Mitgestaltung durch die Justiz sicherzustellen. Das Gesetz stellt dem Verordnungsgeber dafür zwei Alternativen zur Verfügung.

Absatz 3

Inhaber der Rechtsaufsicht über Dataport sind die Trägerländer, Aufsichtsbehörde ist „das für ressortübergreifende IT-Angelegenheiten zuständige Ministerium des Landes Schleswig-Holstein“ (§ 10 StV) - nach der hier im Gesetz verwendeten Formulierung „die für die Angelegenheiten der ressortübergreifenden IT zuständige oberste Landesbehörde“. Wahrgenommen wird diese Aufgabe von dem in der Staatskanzlei angesiedelten Chief Information Officer (CIO), Ziffer 3.1.4 OrgErl ITSH.

Diese durch Staatsvertrag zugewiesene Rechtsaufsicht unterliegt nicht der Disposition eines einzelnen Landesgesetzgebers. Deshalb kann an dieser Stelle nur sichergestellt werden, dass das für Justiz zuständige Ministerium an der Ausübung der Rechtsaufsicht möglichst einvernehmlich zu beteiligen ist. Der Letztentscheid muss im Zweifel aber bei der Aufsichtsbehörde, mithin bei der für die Angelegenheiten der ressortübergreifenden IT zuständigen obersten Landesbehörde bleiben.

zu § 8

Die in § 2 Absatz 1 beschriebenen Belange der Justiz müssen nicht nur gegenüber den in § 1 Absatz 1 genannten Stellen der Exekutive, sondern auch gegenüber der Justizverwaltung in den Gerichten und Staatsanwaltschaften geschützt werden.

§ 8 sieht deshalb vor, dass die vom Hessischen Dienstgerichtshof zum Schutz der richterlichen Unabhängigkeit formulierte Forderung nach einem Regelwerk, das Zugriffsrechte auf die in § 2 Absatz 2 Satz 2 genannten Dokumente und Informationen festlegt und Vorkehrungen sowohl zur Sicherung der Zweckbindung als auch zum Schutz vor unbefugter Einsichtnahme trifft (vgl. HessDGH, Umdr. S. 16 f. und S. 23 ff., in juris Rn. 52-54, 68-70, 74 und Vorschlag des hessischen Datenschutzbeauftragten im Schreiben vom 18.10.2011 an den Hessischen Landtag zur vollständigen Umsetzung dieser Entscheidung), auch insoweit umgesetzt wird. In Betracht kommen Regelungen etwa in Bezug auf die GemIT, die Dienstaufsicht führenden oder sonstige, in-

nerhalb der Justiz tätigen Personen. Dabei ist anhand der jeweiligen Aufgabenbeschreibung zu definieren, wer zum Beispiel welche administrativen Zugriffsrechte erhält und wer im Rahmen der Dienstaufsicht welche Informationen zu welchen Zwecken benötigt und erhält und insoweit auch eigene Zugriffsrechte eingeräumt bekommen kann (z.B. zur Ermittlung des Nutzungsverhaltens, der Erledigungsquote oder über sonstige Leistungskontrollen, vgl. HessDGH, Umdr. S. 23 f., in juris Rn. 69).

Der Schutzumfang fällt auch hier unterschiedlich aus, je nach dem, ob es sich um die streitentscheidende, rechtsprechende Tätigkeit der Richterinnen und Richter, die Rechtspflege oder um die Ermittlungs- und Anklagetätigkeit der Staatsanwaltschaften handelt, weil auch die Aufsicht unterschiedlich weit reicht.

Bei der Aufstellung dieser Regelungen ist nach Möglichkeit eine Einigung mit der IT-Kontrollkommission herzustellen, der Letztentscheid muss im Zweifel aber bei der zuständigen Verwaltung bleiben, die ihr Handeln gegenüber dem Parlament zu verantworten hat.