Innenministerium
des Landes
Schleswig-Holstein

**Schleswig-Holsteinischer Landtag**
**Umdruck 17/2618**

Minister

An den
Vorsitzenden des
Innen- und Rechtsausschusses
beim Schleswig-Holsteinischen Landtag
Herrn Thomas Rother, MdL
Landeshaus

24105 Kiel

Kiel, 12. Juli 2011

**33. Tätigkeitsbericht des Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein**

Sehr geehrter Herr Vorsitzender,

zu den wesentlichen Punkten des Unabhängigen Landeszentrums für Datenschutz (ULD) in seinem 33. Tätigkeitsbericht gebe ich die nachfolgende Stellungnahme ab:

Die Stellungnahmen des Ministeriums für Justiz, Gleichstellung und Integration (Ziffer 4.3.1), des Ministerium für Bildung und Kultur (Ziffern 4.7.2 bis 4.7.6), des Ministeriums für Landwirtschaft, Umwelt und ländliche Räume (Ziffer 12.1), des Finanzministeriums (Ziffern 4.1.7, 4.8.2 und 6.2), und des Ministeriums für Arbeit, Soziales und Gesundheit (Ziffer 4.6.3) wurden einbezogen.

### 4.1.1 Der neue Personalausweis – ein Erfolgsmodell?

Das ULD führt aus, dass sich echte technische Sicherheitslücken beim elektronischen Identitätsnachweis (eID) bis heute nicht aufgetan hätten.
Es stellt allerdings anhand eines Beispiels (unbefugte Neusetzung der PIN in der Personalausweisbehörde) fest, das Verfahren der PIN-Vergabe durch die Meldebehörden (richtig müsste es - zudem einheitlich - heißen: „Personalausweisbehörden“) sei noch nicht ausreichend abgesichert. Die aufgezeigten Sicherheitsrisiken bei der PIN-Vergabe sollten daher von den dafür verantwortlichen Stellen durch geeignete konzeptionelle Änderungen beseitigt werden, bevor es zu tatsächlichen Missbräuchen der eID komme.

Postfach 7125, 24171 Kiel | Telefon 0431 988-0 | Telefax 0431 988-2833 | Klaus.Schlie@im.landsh.de |
www.landesregierung.schleswig-holstein.de |

Dem Innenministerium sind Schwierigkeiten hinsichtlich der Sicherheit, insbesondere bei der PIN-Vergabe, nicht bekannt.
Sofern - wie im Beispiel beschrieben - ein Mitarbeiter einer unzuständigen Personalausweisbehörde die eID eines Personalausweises in missbräuchlicher Absicht aktiviert und eine neue PIN vergibt, handelt er rechtswidrig und begeht eine Pflichtverletzung. Die jeweiligen Vorgesetzten haben im Rahmen ihrer Dienstaufsicht auf eine ordnungsgemäße Aufgabenerfüllung hinzuwirken.
Gleichwohl könnte im Interesse einer noch umfassenderen Sicherheit erwogen werden, den Empfehlungen des ULD zu folgen. Dabei sollten die vorgeschlagenen Maßnahmen allerdings einheitlich durch das zuständige Bundesinnenministerium getroffen werden. Dies könnte z. B. in den vom Bundesinnenministerium noch herauszugebenden Personalausweisverwaltungsvorschriften erfolgen. Das ULD hat sich bereits in einem Schreiben vom 26. Oktober 2010 an das Bundesinnenministerium gewandt, worin die genannten Sicherheitsrisiken benannt sind und gebeten, durch geeignete Maßnahmen den aufgezeigten Risiken zu begegnen. Eine Äußerung des Bundesinnenministeriums hierzu ist nicht bekannt.

### 4.1.7 Versand von Besoldungs- und Beihilfebescheiden im Bereich der Schulen

Zum Versand von Besoldungs- und Beihilfebescheiden im Bereich der Schulen teilt das Finanzministerium mit, dass es sich um ein "Problem" der betreffenden Schule handelt und nicht in den Einwirkungsbereich des Finanzverwaltungsamtes (FVA) fällt.
Sofern das FVA von der/dem Beihilfeberechtigten oder der Schule von einer längeren Abwesenheit erfährt, wird der Schriftverkehr selbstverständlich an die Privatanschrift gesandt.

### 4.2.2 Das Verfahren @rtus

Im Rahmen eines Auskunftsverfahrens wurden durch das ULD zu neun Petenten umfangreiche Prüfungen zu Speicherungen in @rtus VBS (Vorgangsbearbeitungssystem) durchgeführt. Die in den Protokollen dargestellten Daten waren nicht in jedem Fall „selbstsprechend“. Eine vertiefende Betrachtung der Vorgänge durch Einsichtnahme der gespeicherten Dokumente war notwendig. In der überwiegenden Zahl der Fälle konnten Unverständlichkeiten ausgeräumt werden. Festgestellte Fehleintragungen wurden korrigiert. Die vom ULD eingeforderte Gewährleistung einer hohen Datenqualität ist auch der Polizei ein großes Anliegen. Bereits vor der Kontrolle durch das ULD wurden im konkreten Fall Hinweise an die Dienst- und Fachaufsicht gegeben. Zur generellen Verbesserung der Datenqualität wurden Qualitätszirkel auf regionaler und eine Arbeitsgruppe im Landeskriminalamt auf überregionaler Ebene eingerichtet.

### 4.2.3 Dokumentationen von Datenübermittlungen

Im Rahmen eines Strafverfahrens wegen des Verkaufes indizierter Videos und DVDs wurden Durchsuchungen durchgeführt, bei denen sich der Anfangsverdacht ergab, dass durch die Lebensgefährtin des Beschuldigten ein Sozialleistungsbetrug begangen wurde. Der zuständigen Arbeitsagentur (ARGE) wurde zur konkreten Überprüfung das Durchsuchungsprotokoll übersandt. Im Dialog zur Datenübermittlung zwischen dem ULD und dem Innenministerium wurde vom ULD eingeräumt, dass die Beurteilungsprärogative bei der

Frage, ob ein Anfangsverdacht begründet ist oder nicht, bei der Polizei liegt. Dennoch hat das ULD die Auffassung der Polizei, dass die Tatsache der Durchsuchung wegen des Verkaufes indizierter Videos für die Bewertung des Anfangsverdachtes eines Sozialleistungsbetruges von Bedeutung ist, nicht akzeptiert und eine Beanstandung ausgesprochen. Ein staatsanwaltschaftliches Verfahren wegen der Datenübermittlung an die ARGE gegen die Polizeibeamten wurde eingestellt.
Die bei der Kontrolle durch das ULD nicht vorgelegte Dokumentation der Datenübermittlung ist darauf zurückzuführen, dass die Übermittlung nicht im Aktenrückhalt auf der Dienststelle dokumentiert war. Der Aktenrückhalt auf einer Polizeidienststelle hat grundsätzlich keinen Anspruch auf Vollständigkeit. Grundlage für Überprüfungen ist der Originalvorgang der Staatsanwaltschaft. In der ausgewerteten Originalakte befand sich die Dokumentation der Datenübermittlung. Leider stellt das ULD in seinem Tätigkeitsbericht die ausführliche Stellungnahme des Innenministeriums nicht so dar, dass der Leser ein unvoreingenommenes eigenes Bild bekommen kann.

### 4.2.4 Protokollierung - ein offenbar unlösbares Problem

Der BSI Grundschutz, vom Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der ständigen Konferenz der Datenschutzbeauftragten des Bundes und der Länder anerkannt, unterscheidet zwischen der zwingenden Vollprotokollierung (bei Systemgenerierung, Einrichten von Benutzern, Verwaltung von Befugnistabellen, Einspielen und Änderung von Anwendungssoftware, Änderung der Dateiorganisation, Durchführung von Backup Restore und sonstigen Datensicherungsmaßnahmen) und der Protokollierung von Benutzeraktivitäten in Abhängigkeit von der Sensibilität der Verfahren bzw. der Daten. Hierzu gehören die Eingabe von Daten, die Datenübermittlung, die Benutzung von automatisierten Abrufverfahren, die Löschung und das Aufrufen von Programmen. Lediglich für das letzte Themenfeld wurde für @rtus VBS eine Differenzierung vorgenommen. Für alle anderen Datenverarbeitungsschritte wird eine Vollprotokollierung gewährleistet.
Lesende Zugriffe werden protokolliert, sofern nicht der zuständige Sachbearbeiter, der Verwalter und der Dienststellenleiter auf den Vorgang zugreifen. Grundlage für diese Entscheidung war das in § 5 LDSG festgeschriebene Prinzip der allgemeinen Maßnahmen zur Datensicherheit in Bezug auf die Erforderlichkeit und Angemessenheit. Die Abwägungen der Landespolizei zur Ausgestaltung der Protokollierung haben genau diese Prinzipien beachtet. Der Sachbearbeiter, der Verwalter und auch die Dienststellenleitungen werden immer unter Bezug auf die Aufgabe (Sachbearbeitung, Dienstaufsicht) einen Zugriff begründen können. Daneben sind die personenbezogenen Daten des Vorganges dem Vorgesetzten, dem Verwalter und vor allem dem Sachbearbeiter bereits bekannt.

Als Indiz für mögliche datenschutzrechtliche Verstöße kann die Feststellung der Häufigkeit der Zugriffe auf einen Vorgang nicht herangezogen werden. Bei der Verfolgung von datenschutzrechtlichen Verstößen durch Polizeibeamte/innen der Landespolizei hat die aktuelle Ausgestaltung der Protokollierung in keinem Fall zu einer Einstellung des Verfahrens geführt. Es wird zudem um Verständnis dafür gebeten, dass die Polizei im Rahmen des rechtlich Zulässigen auch Ressourcenfragen mitberücksichtig! Leider verfügt sie nicht über unbeschränktes und vermehrbares Personal. Deshalb ist Aufgabenkritik sowohl in Richtung Aufgabenbestand als auch in Richtung kritischer Beurteilung neuer Aufgaben

Dauerthema. Daher kann Wünschen und Vorstellungen von ULD nicht „auf Zuruf“ entsprochen werden. Der Entscheidung, was voll- und was nur teilprotokolliert wird, liegen sachgerechte Überlegungen zugrunde.
Die Beanstandung durch das ULD ist insofern nicht gerechtfertigt, weil das ULD auf einer pauschalen Vollprotokollierung beharrt, ohne die Differenzierungsmöglichkeiten des LDSG zu berücksichtigen.

**4.3.1: Telefonieren im Strafvollzug – noch nicht die letzte Fortsetzung**
Die Firma „Telio communications“ (Telio) erbringt auf der Grundlage eines Vertrages mit der Justizvollzugsanstalt aus dem Jahr 2005 für die Justizvollzugsanstalt Telekommunikationsdienstleistungen, durch die es den einsitzenden Gefangenen ermöglicht wird, mit Angehörigen, Bekannten und anderen zu telefonieren.
Telio stellt der Justizvollzugsanstalt die technische Anlage und die zu deren Betrieb erforderliche Software zur Verfügung und übernimmt die Abrechnung angefallener Telefonentgelte sowie die Wartung der technischen Anlage. Die Justizvollzugsanstalt ist Betreiber der Anlage und Auftraggeber der Telekommunikationsdienstleistungen. Sie trifft die Entscheidung über Art und Umfang des den Gefangenen zu gestattenden Telefonverkehrs und die im Einzelfall anzuordnenden Überwachungsmaßnahmen. Regelmäßige Telefonkontakte mit der Familie und mit Freunden dienen der Aufrechterhaltung der Kontakte zur Außenwelt und sind für die spätere Wiedereingliederung in die Gesellschaft von großer Bedeutung. Die Zusammenarbeit mit der Firma Telio ermöglicht es der Justizvollzugsanstalt, diese Kontaktmöglichkeiten ohne finanziellen und ohne großen Personal- und Verwaltungsaufwand zu fördern.
Die Justizvollzugsanstalt hat in den letzten 2 Jahren im Zusammenwirken mit dem ULD bereits einigen datenschutzrechtlichen Beanstandungen abgeholfen.

Der Tätigkeitsbericht 2011 beanstandet noch zwei datenschutzrechtliche Mängel:

a. Sämtliche personenbezogenen Daten der Gefangenen, die Daten der Inhaber der für sie freigeschalteten Rufnummern, sowie die Daten über die geführten Telefonate werden bei dem externen Dienstleister (Telio ) ohne Rechtsgrundlage gespeichert.

b. Die Datenverarbeitung durch den Dienstleister ist unzureichend vertraglich geregelt und dokumentiert. Die Justizvollzugsanstalt verfügt faktisch über keine Kontrollmöglichkeiten, so dass die Datenverarbeitung durch den Dienstleister nicht ausreichend transparent ist.

Zu a: Das zurzeit für Schleswig – Holstein als Landesgesetz gültige Strafvollzugsgesetz (StVollzG) des Bundes hat in seinen Datenschutzbestimmungen keine ausdrückliche Vorschrift, die die Datenspeicherung bei einem externen Dienstleister erlaubt. Dieser Mangel soll durch das baldige Inkrafttreten eines neuen StVollzG SH, in das eine entsprechende Vorschrift aufgenommen werden wird, behoben werden.

Zu b: Die Firma Telio ist zur Zeit im Auftrag der Justizvollzugsanstalt damit befasst, Möglichkeiten zu finden, die es der Anstalt ermöglichen, jederzeit eine umfassende Kon-

trolle über die extern gespeicherten Daten ausüben zu können, z. B. durch lückenlose Protokollierung des Datenzugriffs bei Telio und einer genauen Definition darüber, wer bei Telio zu welchem Zweck Datenzugriff nehmen darf. Ein Ergebnis wird in naher Zukunft erwartet. Danach ist eine erneute Beteiligung des ULD vorgesehen.
Sowohl für die Firma Telio als auch für die Justizvollzugsanstalt wäre eine vollständige Anonymisierung der Gefangenendaten als auch der Daten der Gesprächsteilnehmer (angewählte Nummer) zur verwaltungsmäßigen Abwicklung des Telefonverkehrs möglich. Die Anstalt hält jedoch in Verbindung mit dieser Abwicklung Serviceleistungen für die Gefangenen vor, auf die diese sehr großen Wert legen, z. B. die Einrichtung einer sog. Hotline, mit der die Gefangenen bei der Firma Telio ihre Guthaben abfragen können und bei Bedarf Auskunft über möglicherweise auftretende technische Schwierigkeiten erhalten. Weiterhin besteht für Angehörige und Bekannte die Möglichkeit, für die Gefangenen bei der Firma Telio Telefongeld auf deren Guthabenkonten einzuzahlen. Diese Serviceleistungen wären bei einer Anonymisierung der Daten nicht mehr möglich.

### 4.6.3 Keine Infos über HIV und Hepatitis für den Rettungsdienst

Das ULD setzt sich mit der Frage auseinander, ob ein Krankenhaus dem Personal des Rettungsdienstes bei der Übergabe eines Patienten Informationen zu bestehenden Infektionskrankheiten wie HIV oder Hepatitis B und C mitteilen darf. Das ULD kommt zu dem Ergebnis, dass das den Patienten entlassende ärztliche Personal entscheiden muss, ob und inwieweit der Rettungsdienst über eine Infektionskrankheit informiert wird. Der konkrete Erreger sei nur bei hochinfektiösen und gefährlichen Infektionskrankheiten zu benennen. HIV und Hepatitis rechtfertigten nicht eine derartige Mitteilung.
Hierzu vertritt das Ministerium für Arbeit, Soziales und Gesundheit eine andere Auffassung.
Der Rettungsdienst ist wie andere Einrichtungen des Gesundheitswesens auch verpflichtet, die dem Stand der Wissenschaft entsprechenden Regeln der Hygiene einzuhalten und die Übertragung von Infektionskrankheiten zu vermeiden (vgl. auch § 13 Abs. 1 Nr. 3 Rettungsdienstgesetz - RDG). Die Verpflichtung zur Einhaltung von Hygienemaßnahmen nach dem Stand der medizinischen Wissenschaft ist auch Gegenstand des Entwurfs einer Novelle des Infektionsschutzgesetzes.
Darüber hinaus sind die Arbeitgeber nach dem Arbeitsschutzrecht verpflichtet, wirksame Schutzmaßnahmen für Arbeitnehmer einzurichten und zu überwachen. Letztlich sind die Rettungsdienst betreibenden Einrichtungen verpflichtet, Dokumentationen zum Nachweis ordnungsgemäßer Einsatzausführung zu führen (§ 5 RDG).

Eine sach- und fachgerechte Versorgung und Betreuung des Patienten durch den Rettungsdienst erfordert die genaue Kenntnis aller Umstände, also auch des Infektionsstatus des Patienten. Diese Regelungen dienen dem Gesundheitsschutz von Patientinnen und Patienten sowie Arbeitnehmerinnen und Arbeitnehmern. Es ist das erklärte Ziel der Gesundheitspolitik, die Verbreitung von Infektionskrankheiten zu verhindern. Dazu ist es we-

sentliche Voraussetzung, dass den verpflichteten Einrichtungen bekannte Infektionskrankheiten und -risiken auch benannt werden.
Der Hinweis darauf, dass die Übertragung im Falle von HIV und Hepatitis B und C durch die üblichen Schutzmaßnahmen verhindert werden kann, ist zwar grundsätzlich richtig, aber für die Situation im Rettungsdienst nicht ausreichend. Im täglichen Einsatzgeschehen kann es selbst bei so genannten Entlassungsfahrten zu Situationen kommen, die invasive Maßnahmen am infizierten Patienten unverzüglich erforderlich machen. In diesen Fällen ist das Infektionsrisiko des Rettungsdienstpersonals auch bei Beachtung der Maßnahmen der Standardhygiene deutlich erhöht. Dies gilt umso mehr in der Notfallrettung. Wirksame prophylaktische Maßnahmen – wie Schutzimpfungen – sind bei Hepatitis C- und HIV-Erregern nicht möglich. Eine Infektion ist nicht reversibel.

Das Ministerium für Arbeit, Soziales und Gesundheit kann daher die Bewertung, das Interesse des Patienten auf informationelle Selbstbestimmung überwiege gegenüber dem bestehenden Restrisiko einer Infektion, nicht nachvollziehen. Eine Rechtsgüterabwägung zwischen dem Recht des Patienten sowie dem Recht der Rettungsdienstmitarbeiter und ggf. anderer Patienten auf körperliche Unversehrtheit führt aus Sicht des Ministeriums für Arbeit, Soziales und Gesundheit in den genannten Fällen zu dem Ergebnis, dass das Recht auf körperliche Unversehrtheit als höheres Rechtsgut überwiegt und daher die in Rede stehenden Maßnahmen rechtfertigt.
Die Verpflichtung zur lückenlosen Dokumentation der Einsatzausführung ist ebenso tangiert. Auf die datenschutzrechtlichen Regelungen, die die Erhebung und Weiterverarbeitung derartiger Daten zulassen (§ 5 Abs. 2 RDG) wird Bezug genommen.

Aufgrund der besonderen Bedeutung der Angelegenheit für den Gesundheitsschutz der Mitarbeiterinnen und Mitarbeiter des Rettungsdienstes ist das Ministerium für Arbeit, Soziales und Gesundheit bereits gesondert schriftlich an das ULD herangetreten.

### 4.7.2 Elektronische Lernplattformen und der Datenschutz

Die Bereitschaft des ULD, für den Einsatz in Schulen geeignete Anwendungen in datenschutzrechtlicher Hinsicht verbindlich zu prüfen, wird vom Ministerium für Bildung und Kultur begrüßt. Im Übrigen verweist das ULD selbst auf die Komplexität und die Unterschiedlichkeit der einzelnen Angebote elektronischer Lernplattformen. Es wird daher genau zu prüfen sein, ob und ggf. in welchem Umfang generelle Vorgaben für den schulischen Einsatz elektronischer Lernplattformen zielführend sein können. Das Ministerium für Bildung und Kultur wird diesbezüglich an das ULD herantreten.

### 4.7.3 LanBSH und geplanter USB-Stick erhöhen Datensicherheit

Das Ministerium für Bildung und Kultur wird sich über die Arbeitsgruppe IT-Bildung für eine Erweiterung der Ausstattungsempfehlungen für Schulen um die vom Institut für Qualitätssicherung an Schulen Schleswig-Holstein (IQSH) entwickelte Lösung zur Verschlüsselung von USB-Sticks einsetzen.

### 4.7.4 Schulleiterfortbildungen im Datenschutz weiterhin erforderlich

Das IQSH bietet seit Jahren in enger Kooperation mit dem ULD einmal pro Halbjahr eine intensiv beworbene Fortbildungsveranstaltung zum Thema „Datenschutzrecht für Schulleiterinnen und Schulleiter“ an.

### 4.7.5 Schulen brauchen ein einheitliches und nachhaltiges Datenschutzkonzept

Die Bestellung schulischer Datenschutzbeauftragter und eine durchgängige Beachtung der (schulspezifischen) datenschutzrechtlichen Vorgaben stehen nicht zwingend in einem Kausalzusammenhang. Gem. § 4 Abs. 1 Satz 1 Datenschutzverordnung Schule (DSVO-Schule) ist die Schulleiterin oder der Schulleiter für die Verarbeitung der personenbezogenen Schüler- sowie Elterndaten verantwortlich. In der Wahrnehmung dieser Verantwortung kann sich die Schulleiterin oder der Schulleiter für die Einrichtung eines schulischen Datenschutzbeauftragten entscheiden. Gleiches gilt für die schuleigene Datenschutzkonzeption. Das Ministerium für Bildung und Kultur berät die Schulen umfassend in datenschutzrechtlichen Fragestellungen.
Das IQSH entwickelt zurzeit ein Datenschutzkonzept für das Landesnetz Bildung.

### 4.7.6 Fehlende Umsetzung einer Meldevorschrift

Die Regelung des § 30 Abs. 7 Schulgesetz (SchulG) wird umgesetzt. Vorschlägen zu verfahrenstechnischen Verbesserungen wird das Ministerium für Bildung und Kultur nachgehen.

### 4.8.2 Mitgliedsdaten eines Vereins

Nach Auffassung des Finanzministeriums ist aus der Anmerkung nicht ersichtlich, dass der Betriebsprüfer zur Kontrolle der Mitgliedsbeiträge explizit auch die Telefonnummern der Mitglieder angefordert hat.
Gleichwohl wird das Finanzministerium die Anmerkung des ULD zum Anlass nehmen, die Finanzämter darauf hinzuweisen, dass private Telefonnummern im Rahmen der Prüfung der Vollständigkeit der Mitgliedsbeiträge nicht anzufordern sind.

### 6.2 Der allmächtige anonyme Administrator

Nach Mitteilung des Finanzministeriums wird die Arbeit im Tagesgeschäft der Basisinfrastrukturkomponenten standardisiert mit dedizierten personalisierten Benutzer- und Administrationskonten durchgeführt.
Für die „+1.Infrastruktur“ gilt: der "Administrator" auf dem Arbeitsplatz sollte grundsätzlich nicht genutzt werden, sondern für die jeweiligen Systeme sollten personenbezogene Administrationskonten als lokale Administratoren über Gruppenrichtlinien berechtigt werden.
Für den Notfall und für Arbeiten außerhalb der Domäne kann der „Administrator“ des lokalen Arbeitsplatzes unter der Maßgabe genutzt werden, dass die Nutzung und die mit diesem Konto durchgeführten Tätigkeiten dokumentiert werden.

### 12.1 Der schwierige Weg zu einem einheitlichen Informationszugangsrecht

Zu der Novellierung des Umweltinformationsgesetzes und der Zusammenfassung mit dem Informationsfreiheitsgesetz nehmen das Ministerium für Landwirtschaft, Umwelt und ländliche Räume und das Innenministerium wie folgt Stellung:

Der zu Beginn der Legislaturperiode von der Landesregierung in den Landtag eingebrachte Änderungsentwurf zum Umweltinformationsgesetz (UIG, Drs. 17/171) sieht zwingend notwendige, eilige und vom VG Schleswig mehrfach angemahnte Korrekturen vor. Mit dem Gesetzentwurf sollen im Wesentlichen Rechtsmängel und Unklarheiten des UIG beseitigt werden. Unabhängig von dieser kleinen vorgezogenen Novelle beabsichtigte die Landesregierung gemäß der Koalitionsvereinbarung, in der zweiten Hälfte der nunmehr verkürzten Legislaturperiode einen Gesetzentwurf vorzulegen, der das Informationsfreiheitsgesetz (IFG) und das Umweltinformationsgesetz zusammenführt. Dem sind die Fraktionen von CDU und FDP zuvorgekommen, indem sie einen vom ULD formulierten Gesetzentwurf aufgegriffen haben.
Der vom ULD vorgelegte Entwurf verstieß allerdings gegen europäisches Recht, war unnötig kompliziert und führte keineswegs zu der beabsichtigten Verwaltungsvereinfachung. Die Reduzierung der Anzahl der Paragraphen allein bedeutet nicht, dass die Rechtslage und damit die Rechtsanwendung tatsächlich vereinfacht werden.
So behielt der Gesetzentwurf die Unterscheidung zwischen Umwelt- und sonstigen Informationen bei und übernahm weitgehend alle bislang im UIG und IFG enthaltenen Ablehnungsgründe, ohne diese – wo möglich - zusammenzuführen. Daher hätte der Rechtsanwender weiterhin die im Einzelfall schwierige Unterscheidung zwischen Umwelt- und sonstigen Informationen treffen müssen. Dabei hat gerade das ULD in seinen Stellungnahmen zu dem bereits 2006 von der damaligen Landesregierung erarbeiteten Entwurf für gemeinsame IFG/UIG-Regelungen (Drs. 16/722) noch angemahnt, auf die Unterscheidung zwischen Umwelt- und sonstigen Informationen zu verzichten.
Das ULD konnte im April 2010 nicht alle Argumente des Ministeriums für Landwirtschaft, Umwelt und ländliche Räume widerlegen. Dies gilt insbesondere für die zahlreichen Verstöße gegen die EG-Umweltinformationsrichtlinie, die sich weiterhin in dem Gesetzentwurf fanden.
Das Innenministerium und das Ministerium für Landwirtschaft, Umwelt und ländliche Räume haben inzwischen gegenüber den Fraktionen der CDU und der FDP zu diesem Entwurf Stellung genommen. Die Fraktionen von CDU und FDP sind den Änderungsvorschlägen der Ministerien weitestgehend gefolgt. Die Fraktionen werden ihren Gesetzentwurf demnächst als Drucksache 17/1610 in den Landtag einbringen.

### 12.3 Keine Informationskosten für nicht rechtsfähige gemeinnützige Vereine

Die Auffassung des ULD, nicht rechtsfähige gemeinnützige Vereine sollten bei Anträgen auf Informationszugang von Gebühren befreit sein, wird vom Innenministerium nicht geteilt.
Nach § 8 Abs. 1 Nr. 6 Verwaltungskostengesetz (VwKostG) sind Körperschaften, Vereinigungen und Stiftungen, die gemeinnützigen oder mildtätigen Zwecken im Sinne des Steuerrechts dienen, von der Gebührenpflicht befreit, soweit die Angelegenheit nicht einen steuerpflichtigen wirtschaftlichen Geschäftsbetrieb betrifft. Dabei ist die Gemeinnützigkeit oder Mildtätigkeit durch einen Beleg des Finanzamtes nachzuweisen. Auf diese Weise kann sichergestellt werden, dass nur Vereinigungen, die auch tatsächlich gemeinnützige oder mildtätige Ziele verfolgen, in den Genuss der Gebührenfreiheit kommen.
Andere Vereinigungen, die keine juristische Person bilden, werden einen derartigen Nachweis, ebenso wie natürliche Personen, gar nicht oder zumindest nicht ohne weiteres

erbringen können. Um Missbrauch zu verhindern, sollte aber nicht ohne Not auf derartige Nachweise verzichtet werden.
Nicht rechtsfähige Vereine, die mildtätig oder gemeinnützig tätig sind, können aber auf andere Weise bei der Gebührenberechnung berücksichtigt werden. So ermöglicht das Verwaltungskostengesetz ein Absehen von der Gebühr aus Gründen der Billigkeit in Einzelfällen. Darüber hinaus kann das fehlende wirtschaftliche Interesse eines mildtätigen Vereins auch bei der Berechnung der Gebührenhöhe nach § 9 Abs. 1 VwKostG Berücksichtigung finden.

Mit freundlichen Grüßen

gez.
Klaus Schlie