# LANDTAG MECKLENBURG-VORPOMMERN
# PRESSEMITTEILUNG

**Landesbeauftragter für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern: Tätigkeitsberichte vorgestellt**

Seine Tätigkeitsberichte für den Berichtszeitraum 2010/2011 hat der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern, Reinhard Dankert, heute in Schwerin der Öffentlichkeit vorgestellt.

Im vergangenen Berichtszeitraum haben sich Bürgerinnen und Bürger, Behörden, Unternehmen und andere Institutionen verstärkt an den Landesbeauftragten gewandt und um Unterstützung und Beratung zu den verschiedensten Themen aus den Bereichen Datenschutz und Informationsfreiheit gebeten.

„Das vermehrte Interesse für den Datenschutz ist zurückzuführen auf die rasante Entwicklung der Informations- und Kommunikationstechnik mit all ihren Anwendungsmöglichkeiten im Alltag, aber auch mit all ihren Gefahren für den Schutz personenbezogener Daten“, so Dankert heute in Schwerin. „Insbesondere die weltweite Vernetzung durch das Internet erfordert dabei besondere Beachtung. Hier seien als Beispiel die sozialen Netzwerke genannt, bei deren Nutzung sich dann und wann so mancher wundert, wer alles über seine persönlichen Daten Bescheid weiß, obwohl er es eigentlich gar nicht sollte“ (siehe Punkt 2.2). Der Datenschutz in sozialen Netzen stand auch im Mittelpunkt eines Projektes der Dienststelle, in dessen Rahmen für Kinder das Computerspiel „Netzwerkstar“ entwickelt wurde (siehe Punkt 2.2.4). Die Datenschutz-Fachtagung im Jahr 2011 befasste sich ebenfalls mit dem Thema der sozialen Netze und deren Folgen für die Privatsphäre der Nutzerinnen und Nutzer (siehe Punkt 2.2.3). Die zunehmende Nutzung sozialer Netze im Internet insbesondere durch Kinder und Jugendliche erfordert neue Konzepte nicht nur im Datenschutz, sondern auch in der Bildung. Datenschutz muss künftig auch als Bildungsaufgabe verstanden und praktiziert werden. Die digitale Aufklärung ist unverzichtbar als Teil einer Datenschutzkultur des 21. Jahrhunderts und wird somit ein herausragender Arbeitsschwerpunkt der Behörde sein (siehe Punkt 2.1).

„Ähnlich stark interessieren sich die Bürgerinnen und Bürger für das noch recht neue Recht auf Zugang zu Informationen aus der öffentlichen Verwaltung, das Informationsfreiheitsrecht“, so Dankert weiter. „Dieses Recht gibt es in Mecklenburg-Vorpommern seit dem Juli 2006. Es soll Verwaltungsentscheidungen transparent und damit für jedermann nachvollziehbar machen. Bei der Gewährung des Zugangs zu Informationen ist jedoch zu berücksichtigen, dass diese auch dem Datenschutz unterliegen können. In diesen Fällen ist stets eine Abwägung zwischen Informationsfreiheit und Datenschutz erforderlich. Aus diesem Grunde nennt man den Datenschutz und die Informationsfreiheit auch gern die „zwei Seiten einer Medaille“.“

Themenschwerpunkte im zurückliegenden Berichtszeitraum waren neben der Nutzung sozialer Netzwerke im Internet auch neue IT-Verfahren der Landesverwaltung, zahlreiche technische Entwicklungen wie De-Mail, Cloud-Computing oder der Einsatz von Smartphone und Table-PC. Aber auch altbekannte Themen wie Videoüberwachung, Datenschutz im Bereich der Medizin oder bei der Verarbeitung von Personal- und Sozialdaten standen wieder regelmäßig auf der Tagesordnung. Schließlich sind stark steigende Fallzahlen bei Wirtschaftsunternehmen, Vereinen und Verbänden zu verzeichnen. Unvermindert hoch sind auch die Beratungsersuchen zu verschiedensten Sachverhalten aus dem Bereich der Informationsfreiheit.

### 3.2.6 De-Mail: Vorsicht bei sensiblen Daten *(siehe Seite 41)*

Am 3. Mai 2011 trat das De-Mail-Gesetz in Kraft. Der De-Mail-Dienst besteht mindestens aus einem Postfach- und Versanddienst, einer Komponente für die so genannte sichere Anmeldung und einem Verzeichnisdienst. Die vorgeschriebene Transport- und Speicherverschlüsselung von De-Mails führt zu einem besseren Schutz vor unbefugtem Mitlesen als bei normalen E-Mails. Vorsicht ist dennoch geboten, wenn besonders schutzbedürftige Daten übermittelt werden, da der De-Mail-Dienst standardmäßig keine Ende-zu-Ende-Verschlüsselung bietet.

**4.1.1 Datenschutzgerechtes Cloud-Computing – geht das?** *(siehe Seite 56)*

Ein Schwerpunktthema der Computermesse CeBIT des Jahres 2011 hieß „Work and Life with the Cloud“. Wird die eigene Verarbeitung personenbezogener Daten teilweise oder vollständig in die Cloud ausgelagert, ist vor dem Beginn der Verarbeitung zu klären, wie der Datenschutz gewährleistet werden kann. Das kann zu erheblichen Schwierigkeiten führen, da renommierte Anbieter von Clouds die Daten mit hoher Wahrscheinlichkeit außerhalb des Geltungsbereichs deutschen und europäischen Datenschutzrechts speichern.

**4.1.4 Smartphone & Tablet PC im professionellen Einsatz** *(siehe Seite 64)*

Smartphones wie Blackberry oder iPhone und Tablet PC wie iPad und Co. sind inzwischen nicht mehr nur beliebtes Spielzeug von Privatanwendern. Mittlerweile haben auch Wirtschaft und Verwaltung die vielfältigen und flexiblen Möglichkeiten für sich entdeckt. Auch der Landtag Mecklenburg-Vorpommern hat seine Abgeordneten mit „lüfterlosen Lesegeräten“ – so die offizielle Gerätebezeichnung, gemeint sind iPads der Firma Apple – ausgestattet, damit sie etwa während der Landtagssitzungen auf Landtagsdokumente online zugreifen können. Mich erreichen daher immer mehr Nachfragen zum datenschutzgerechten Einsatz dieser Geräte und auch das Administrationspersonal in Wirtschaft und Verwaltung sucht nach Lösungen zur sicheren und datenschutzgerechten Einbindung der Geräte in die vorhandene IT-Landschaft.

**4.2.2 Google Analytics – Wo warst Du surfen?** *(siehe Seite 75)*

Viele Web-Seitenbetreiber analysieren zu Zwecken der Werbung und Marktforschung oder bedarfsgerechten Gestaltung ihres Internet-Angebotes das Surf-Verhalten der Nutzerinnen und Nutzer. Zur Erstellung derartiger Nutzungsprofile verwenden sie vielfach Software bzw. Dienste zur so genannten Reichweitenanalyse, die von Dritten kostenlos oder gegen Entgelt angeboten werden. Dabei müssen jedoch die Bestimmungen des Telemediengesetzes berücksichtigt werden. Weit verbreitet ist ein Produkt der amerikanischen Firma Google. Erst nach langen Verhandlungen mit deutschen Datenschützern hat Google verschiedene Änderungen an seinem Produkt Google Analytics vorgenommen, erfüllt nun aber weitgehend die Anforderungen der Datenschutzaufsichtsbehörden.

**4.2.5 Umgang mit E-Mails am Arbeitsplatz** *(siehe Seite 80)*

Die Beschäftigten einer Kommunalverwaltung waren aufgefordert worden, ihren jeweiligen Fachvorgesetzten den Zugriff auf ihr E-Mail-Postfach zu eröffnen. Die Fachvorgesetzten sollten ihrerseits dem Behördenleiter den Zugriff auf ihre E-Mail-Postfächer eröffnen. Unklar war zudem, ob Beschäftigte während ihrer Abwesenheit die eingehenden Mails an den Vertreter weiterleiten müssen oder ob die Aktivierung eines Abwesenheitsassistenten ausreiche. Es stellte sich die Frage, ob die Beschäftigten den Zugriff auf ihre E-Mail-Postfächer oder die Weiterleitung von E-Mails an Vertreter wegen der Beeinträchtigung ihres Rechts auf informationelle Selbstbestimmung verweigern können.

**4.3.1 IP-Telefonie – Organisation verbesserungswürdig** *(siehe Seite 86)*

Dem vom IT-Landesdienstleister betriebenen Verfahren IP-Telefonie konnte ich in der Vergangenheit ein hohes Datenschutzniveau bescheinigen. Während dieses Berichtszeitraumes musste ich jedoch einen schwerwiegenden Datenschutzverstoß feststellen. Die in den Verträgen mit dem Dienstleister und in den Dienstvereinbarungen der Landesverwaltung zur IP-Telefonie vereinbarten Vorgaben zum Umfang und zur Dauer der Speicherung von Verbindungsdaten der IP-Telefongespräche waren nicht eingehalten worden.

**4.3.4 Anlasslose Kontrolle der Arbeitszeit durch Vorgesetzte** *(siehe Seite 91)*

Trotz elektronischer Arbeitszeiterfassung ist es im Innenministerium nach wie vor gängige Praxis, das vom Beschäftigten auszudruckende Monatsjournal der Arbeitszeiten regelmäßig und anlasslos den Vorgesetzten vorzulegen. Was beim manuellen Aufschreiben der Arbeitszeiten durch den Beschäftigten zulässig wäre, ist jedoch anders zu bewerten, wenn die Arbeitszeitdaten auf der Grundlage einer Gleitzeitvereinbarung elektronisch erfasst und verarbeitet werden. In diesem Fall steht die Frage, zu welchem Zweck es erforderlich sein soll, dass der Vorgesetzte das Monatsjournal jedes einzelnen Beschäftigten regelmäßig zur Kenntnis nehmen soll.

**4.5.2 Anforderungen an Krankenhausinformationssysteme** *(siehe Seite 108)*

In der Prüfpraxis der Datenschutzbeauftragten hat sich in den letzten Jahren gezeigt, dass Krankenhausinformationssysteme wichtige gesetzliche Datenschutzanforderungen nicht abbilden und dass Schutzvorkehrungen nicht eingesetzt oder umgangen werden, unter anderem, weil sie schlecht bedienbar sind. In einer Orientierungshilfe der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sind grundlegende Anforderungen des Datenschutzes an Hersteller und Betreiber von Krankenhausinformationssystemen zusammengefasst, die künftig Bewertungsmaßstab für meine Beratungs- und Kontrolltätigkeit sein werden.

**4.5.3 KV SafeNet – eine Kommunikationslösung für Ärzte** *(siehe Seite 110)*

Ärzte müssen ihre Abrechnungsdaten elektronisch an die Kassenärztliche Vereinigung übermitteln. Die Kassenärztliche Bundesvereinigung (KBV) bietet mit KV-SafeNet eine Kommunikationslösung für Ärzte an, die einige Unzulänglichkeiten in technischer und in organisatorischer Hinsicht offenbart hatte. Ich übergab der KBV einen Katalog mit Forderungen, deren Umsetzung einen vollständig datenschutzkonformen Betrieb von KV-SafeNet sicherstellen sollte. Diesen Katalog hat die KBV in kürzester Zeit vollständig abgearbeitet.

**4.6 Videoüberwachung** *(siehe Seite 111)*

Videoüberwachung kommt in einem ständig steigenden Umfang zum Einsatz. Zahlreiche Petitionen zeigen, dass die datenschutzrechtlichen Rahmenbedingungen nicht immer berücksichtigt werden. Die Kontrolle der Anlagen und die Beratung der Betreiber binden einen erheblichen Anteil der personellen und zeitlichen Ressourcen meiner Dienststelle. Das betrifft sowohl die Videoüberwachung im öffentlichen Bereich als auch die Videoüberwachung bei Unternehmen oder Privaten. Im Tourismusland Mecklenburg-Vorpommern werden zudem immer öfter Webcams eingesetzt, denn Hotels möchten potenziellen Kunden gern schon vor der Reise einen Blick auf den eigenen Park mit angrenzendem Badestrand oder den benachbarten Yachthafen ermöglichen. Dass bei solchen Bildern nicht nur Strände, Häfen oder Bootsstege zu sehen sind, sondern dass auch die sich dort aufhaltenden Personen erfasst werden, wird mitunter nicht bedacht.

**5.2.1 Ahndung bei unerlaubten Datenabfragen** *(siehe Seite 123)*

Die unerlaubte Datenabfrage durch Polizeiangehörige ist bei den Datenschutzbeauftragten von Bund und Ländern immer wieder ein Thema. Auch ich hatte mich im Berichtszeitraum mit einer vermuteten unbefugten Datenabfrage zu befassen.

**5.2.3 Polizei: Uni soll Studenten erziehen** (*siehe Seite 125*)

Die Polizei bat eine Universität, gemeinsam mit einem Studenten dessen Verhalten auszuwerten, da dieser im Zusammenhang mit einer von ihm begangenen Ordnungswidrigkeit ein unrühmliches Bild auf die Uni geworfen haben soll. Die datenschutzrechtliche Bewertung ergab, dass diese Datenübermittlung rechtswidrig war. Die Polizei sicherte mir zu, dass sie derartige Datenübermittlungen nicht mehr durchführen wird.

**5.4.3 Personenbezogene Daten in einem Planfeststellungsbeschluss?** *(siehe Seite 132)*

Ein Bürger hatte mich darauf aufmerksam gemacht, dass in der Begründung zu einem Planfeststellungsbeschluss, welcher den Neubau einer Autobahnrastanlage zum Inhalt hatte, personenbezogene Daten über ihn enthalten waren. Meine Prüfung des Sachverhaltes ergab, dass die Veröffentlichung personenbezogener Daten nicht angemessen war, da das Interesse des Betroffenen auf Schutz seiner personenbezogenen Daten einem möglichen Interesse der Allgemeinheit auf Offenbarung dieser Daten überwog.

**5.4.7 Der neue Personalausweis** *(siehe Seite 138)*

Seit dem 1. Oktober 2010 erhalten Bürgerinnen und Bürger auf Antrag den neuen Personalausweis. Mit besonderem Interesse verfolge ich die Entwicklungen um die neue Funktion des elektronischen Identitätsnachweises (eID-Funktion), mit der ein sicherer Nachweis der eigenen Identität auch in E-Government-Verfahren gewährleistet werden soll. Leider fallen auch für Behörden, die Dienstleistungen unter Nutzung des neuen Personalausweises anbieten

wollen, erhebliche Kosten an. Ich habe mich nachdrücklich dafür eingesetzt, dass diese Kosten drastisch gesenkt werden, damit die auch aus datenschutzrechtlicher Sicht begrüßenswerte Infrastruktur des neuen Personalausweises vermehrt zum Einsatz kommt.

**5.5 Zensus 2011** *(siehe Seite 143)*

Im Laufe der Vorbereitung und während der Durchführung der Volkszählung 2011 erhielt ich zahlreiche Anfragen und Petitionen. Die Fragen bezogen sich sowohl auf die Gebäude- und Wohnungszählung als auch auf die Haushaltsbefragung. Um die Arbeitsweise der Erhebungsstellen datenschutzrechtlich bewerten zu können, habe ich zudem mehrere dieser Stellen kontrolliert und dabei erhebliche Mängel festgestellt.

**5.6.4 Ablösung der Lohnsteuerkarte** *(siehe Seite 151)*

Mit dem Wegfall der Papierlohnsteuerkarte werden jetzt alle Lohnsteuerdaten in der beim Bundeszentralamt für Steuern eingerichteten Datenbank gespeichert, in der bisher nur die Steuer-Identifikationsnummer abgelegt war. Die Erweiterung der zentralen Datenbank um sehr sensible personenbezogene Daten wie die zur Religionszugehörigkeit birgt aus datenschutzrechtlicher Sicht nicht unerhebliche Risiken. Unbefriedigend sind auch die Sicherheitsvorkehrungen zum Zugriff von Arbeitgebern auf diese Datenbank.

**5.8.1 Kinder- und Jugendhilfe** *(siehe Seite 157)*

Mitarbeiter eines Jugendamtes offenbarten unbefugt Sozialdaten und verletzten somit sozialdatenschutzrechtliche Bestimmungen, indem sie sich bei einem unangemeldeten Hausbesuch anderen Hausmitbewohnern zu erkennen gaben.

**5.9.1 Umgang mit Patientendaten** *(siehe Seite 163)*

Die Übermittlung von Patientendaten von Krankenhäusern, Arztpraxen oder Rehabilitationseinrichtungen stand im Mittelpunkt vieler Anfragen aus dem Gesundheitsbereich. Da die ärztliche Schweigepflicht auch unter Ärzten einzuhalten ist, dürfen Patientendaten an andere Stellen nur übermittelt werden, wenn eine Rechtsvorschrift dies vorsieht oder der Patient eingewilligt hat. Dennoch übermittelte ein Facharzt einen Befund und eine Diagnose, die weder mit der Überweisung im Zusammenhang stand noch sein Fachgebiet betraf, ohne das Einverständnis des Patienten an den überweisenden Arzt. In anderen Fällen war zu klären, welche Gesundheitsdaten vor Beginn einer Behandlung dem jeweiligen Facharzt oder vor Beginn einer Rehabilitationsmaßnahme der Klinik zur Verfügung gestellt werden dürfen.

**7.3 Open Data/Open Government** *(siehe Seite 187)*

Open Government bedeutet die weitere Öffnung des Staates gegenüber Bürgerinnen und Bürgern, Wirtschaft und Wissenschaft. Dadurch soll mehr Transparenz und Teilhabe und somit mehr direkte Demokratie ermöglicht werden. Eine Arbeitsgruppe der Konferenz der Informationsfreiheitsbeauftragten in Deutschland hat unter meiner Federführung ein Positionspapier erarbeitet und dem Bundesinnenministerium übergeben, das die Open Government Strategie der Bundesregierung untersucht und bewertet.

**7.5 Muss jede Information herausgegeben werden?** *(siehe Seite 191)*

Immer wieder informieren mich Bürgerinnen und Bürger darüber, dass der von ihnen beantragte Zugang zu Informationen nicht im erforderlichen Umfang gewährt wurde. So hatte das Ministerium für Energie, Infrastruktur und Landesentwicklung einen Antrag auf Informationszugang zu verkehrsrechtlichen Sachverhalten mit dem Hinweis auf Nichtzuständigkeit abgewiesen, obwohl es über die fraglichen Informationen verfügte.

**7.6 Wie hoch dürfen die Kosten für eine Informationsgewährung sein?** (*siehe Seiten 190 und 192)*

Einige Verwaltungen nutzten die durch das IFG M-V eingeräumte Möglichkeit der Kostenerhebung dazu, Gebühren so hoch anzusetzen, dass in der Folge Bürger auf ihr Recht auf Informationszugang verzichtet haben. Die Kostenverordnung zum IFG M-V sieht eine Gebührenerhebung nur im Fall einer umfangreichen Auskunft vor. Diese Voraussetzung war aber

nicht in jedem Fall gegeben, so dass ich in einigen Fällen Empfehlungen ausgesprochen habe, die bereits veranlassten oder vorgesehenen Gebührenerhebungen noch einmal kritisch zu überprüfen.

---

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern hat dem Landtag und der Landesregierung für jeweils zwei Kalenderjahre einen Bericht über seine Tätigkeit vorzulegen. Der Zehnte Tätigkeitsbericht gemäß § 33 Abs. 1 DSG M-V, der Fünfte Tätigkeitsbericht gemäß § 38 Abs. 1 BDSG sowie der Dritte Tätigkeitsbericht nach dem Informationsfreiheitsgesetz umfassen den Zeitraum vom 1. Januar 2010 bis zum 31. Dezember 2011. Es wurden Vorgänge ausgewählt, die einen Gesamteindruck von der Tätigkeit der Behörde vermitteln sollen. Einige Beiträge schließen an Sachverhalte aus den letzten Tätigkeitsberichten an. Insofern könnte es nützlich sein, in dem einen oder anderen Fall noch einmal auf diese Berichte zurückzugreifen.

Die Tätigkeitsberichte für den Zeitraum 2010/2011 können kostenlos als Broschüre beim Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern, Lennèstraße 1, Schloss, 19053 Schwerin, angefordert werden. Sie sind auch auf den Internetseiten des Landesbeauftragten verfügbar (www.datenschutz-mv.de).

---

verantwortlich: DL/29. Mai 2012
Landtag Mecklenburg-Vorpommern
- Pressestelle -
Lennéstraße 1, Schloss
19053 Schwerin
Fon: 0385 / 525-2149
Fax: 0385 / 525 2616
Mail : pressestelle@landtag-mv.de

Der Landesbeauftragte für Datenschutz
und Informationsfreiheit Mecklenburg-Vorpommern
Lennéstraße 1, Schloss
19053 Schwerin
Fon: 0385 / 59494-0
Fax: 0385 / 59494-58
Mail: datenschutz@mvnet.de