LANDTAG MECKLENBURG-VORPOMMERN
MEDIEN-INFORMATION

Landesbeauftragter für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern:
Tätigkeitsberichte vorgestellt

Die Tätigkeitsberichte für den Berichtszeitraum 2012/2013 hat der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern, Reinhard Dankert, heute in Schwerin der Öffentlichkeit vorgestellt.

„Auch in diesem 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“, so Dankert heute in Schwerin. „Viel gesprochen worden ist in diesem Berichtszeitraum über das Grundrecht auf informationelle Selbstbestimmung“, so Dankert weiter und verweist an dieser Stelle noch einmal auf das wegweisende Urteil des Bundesverfassungsgerichtes vom 15. Dezember 1983, wo es heißt: „Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen.“

Bundespräsident Joachim Gauck fasste die Bedeutung des Datenschutzes für den Erhalt der Privatsphäre aufgrund der Ereignisse im Berichtszeitraum in seiner Rede zum Festakt am Tag der Deutschen Einheit am 3. Oktober 2013 in Stuttgart in die Worte: „So sollte der Datenschutz für den Erhalt der Privatsphäre so wichtig werden wie der Umweltschutz für den Erhalt der Lebensgrundlagen. Wir wollen und sollten die Vorteile der digitalen Welt nutzen, uns gegen ihre Nachteile aber bestmöglich schützen.“ Und wenn sogar der Bundespräsident dieses Thema aufgreift und eindrücklich auf die Bedeutung des Datenschutzes für den Erhalt der Privatsphäre hinweist, dann muss schon etwas Bedeutsames passiert sein. Und es war tatsächlich etwas passiert, das den Datenschutz in den Blickpunkt der Öffentlichkeit rückte.

Im Juni 2013 wurden erste Hinweise bekannt, dass amerikanische Geheimdienste in bisher ungeahntem Umfang die weltweite elektronische Kommunikation abhören würden, und Edward Snowden, ehemaliger Mitarbeiter des größten Auslandsgeheimdienstes der Vereinigten Staaten, der National Security Agency (NSA), hatte unzählige Dokumente, die die Spionageaktivitäten der NSA im Rahmen des Geheimprogramms PRISM dokumentieren, an die Presse weitergegeben. Die Vorwürfe beschränkten sich jedoch nicht nur auf die NSA, sondern betrafen auch den britischen Geheimdienst, das Government Communications Headquarter (GCHQ) und dessen Spionageprogramm TEMPORA. Obwohl die Gespräche des Bundesinnenministers mit Vertretern der NSA im Juli 2013 wenig Licht ins Dunkel brachten, zeigten die nach und nach von Snowden veröffentlichten Dokumente das Ausmaß der Spionage (detailliert dokumentiert unter http://www.heise.de/extras/timeline).

Angesichts dieser Bedrohungen muss vor allem die Bundesregierung handeln. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat jedoch in ihrer Entschließung vom 5. September 2013 festgestellt, dass noch immer nicht alles getan wurde, um das Ausmaß der nachrichtendienstlichen Ermittlungen mit Hilfe von Programmen wie PRISM und TEMPORA für die Bundesrepublik Deutschland aufzuklären. Nicht nur eine bessere Kontrolle der Geheimdienste und der völkerrechtlichen Abkommen sind gefordert. Nötig sind auch Gesetzesinitiativen, die das Grundrecht auf informationelle Selbstbestimmung und das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme sicherstellen ***(siehe Punkt 6.3.3)***.

„Datenschutz als Schutz von Grundrechten zu begreifen, diese Grundrechte auch zu erkennen und wahrzunehmen, erfordert eine entsprechende Kompetenz der Bürgerinnen und Bürger“, so Reinhard Dankert weiter. „Diese Kompetenz kann insbesondere durch Bildung erreicht werden. Datenschutz ist daher auch als Bildungsaufgabe zu verstehen, insbesondere schon bei Kindern und Jugendlichen. Dazu gehört auch der Erwerb von Medienkompetenz, einer Schlüsselqualifikation des 21. Jahrhunderts.“

Deshalb hat der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern ein umfangreiches Bildungspaket initiiert, das insbesondere auf die Zielgruppe der jungen Menschen in Mecklenburg-Vorpommern ausgerichtet ist ***(Punkt 2)***. Verschiedene Projekte sollen sowohl die Chancen aufzeigen, die die mediale Welt bietet, als auch die Risiken, die mit der Nutzung der modernen Technik verbunden sind. Ein Schwerpunkt ist das Projekt „Medienscouts MV“ ***(Punkt 2.2)***. Es unterstützt insbesondere Jugendliche im Alter von 14 – 16 Jahren, aber auch Lehrerinnen und Lehrer und Schulsozialarbeiterinnen und Schulsozialarbeiter dabei, ihr Wissen zum Umgang mit digitalen Medien zu erwerben und zu erweitern. Die Umsetzung des Ziels Datenschutz durch Bildung fängt im Kindesalter an und hört bei der Ausbildung, im Studium und bei der Fortbildung nicht auf. Künftig wird noch mehr die Unterstützung der staatlichen Bildungsinstitutionen und die des Parlaments erforderlich sein, damit jeder junge Mensch in Mecklenburg-Vorpommern mehrmals qualifizierte Bildungsangebote zu den Themen Medienkompetenz, Datenschutz und Urheberrecht wahrnehmen kann. Aber nicht nur die Altersgruppe der Kinder und Jugendlichen soll sensibilisiert werden für Fragen des Datenschutzes. Künftig soll auch die Altersgruppe der Seniorinnen und Senioren (im Rahmen der Projekt-Arbeit) Angebote erhalten, damit auch diese Gruppe für datenschutzrechtliche Fragen sensibilisiert wird, insbesondere wenn es um den Umgang mit dem Internet geht ***(Punkt 2.10)***.

Themenschwerpunkte im zurückliegenden Berichtszeitraum waren auch der Umgang mit persönlichen Daten bei der Nutzung sozialer Netzwerke im Internet, die Anwendung neuer E-Government-Verfahren, zahlreiche technische Entwicklungen wie De-Mail, Cloud-Computing oder der Einsatz von Smartphone und Table-PC sowie Themen aus dem Bereich der Informationsfreiheit. 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.

Soziale Netzwerke im Internet haben inzwischen weltweit bei den Nutzerzahlen die Milliardengrenze überschritten. Insbesondere das amerikanische Unternehmen Facebook liegt hier ganz vorn. Da wir die Dienste dieses Unternehmens nicht mit deutschem Datenschutzrecht vereinbar halten, haben wir insbesondere den öffentlichen Stellen in Mecklenburg-Vorpommern bereits im Oktober 2011 empfohlen, keine Facebook-Fanpages einzurichten. Inzwischen hat aber das Schleswig-Holsteinische Verwaltungsgericht auf drei Klagen von Unternehmen in Schleswig-Holstein geurteilt, dass deutsche Betreiber von Facebook-Fanpages für die bei Facebook erfolgende Datenverarbeitung datenschutzrechtlich in keiner Weise verantwortlich gemacht werden könne. Für den Datenschutz im Internet sind die Entscheidungen eine weitgehende Kapitulation. Mit aufsichtsrechtlichen Maßnahmen können deutsche Datenschutzbehörden dem Treiben von Facebook und Co. nun kaum noch Einhalt gebieten. Umso wichtiger ist es, Nutzerinnen und Nutzer über die Risiken der Nutzung zu informieren und sie für einen datenschutzgerechten Umgang mit personenbezogenen Daten zu sensibilisieren ***(Punkt 2.9, Punkt 6.9.6)***.

Das Artikelgesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften ist am 1. August 2013 in wesentlichen Teilen in Kraft getreten. Ziel des Gesetzes ist es, die elektronische Kommunikation mit der Verwaltung zu erleichtern. Es drängt sich der Eindruck auf, dass Erleichterung in diesem Zusammenhang vor allem ein Absenken der Sicherheitsanforderungen an die elektronische Kommunikation bedeutet. Denn offenbar hat es die Bundesregierung nun endgültig aufgegeben, das gute Konzept der qualifizierten elektronischen Signatur in die Fläche zu bringen. Stattdessen werden andere Verfahren bereitgestellt, mit denen die handschriftliche Unterschrift durch die elektronische Form ersetzt werden kann. Jedoch ist festzustellen, dass die mit dem Artikelgesetz neu zugelassenen Möglichkeiten zum Ersatz einer durch Rechtsvorschrift angeordneten Schriftform durch die elektronische Form hinsichtlich Vertrauenswürdigkeit und Sicherheit mit der qualifizierten elektronischen Signatur nicht zu verglei-

chen sind. Der Gesetzgeber spricht nämlich lediglich von *anderen Verfahren* und vermeidet offenbar bewusst den Begriff *vergleichbare Verfahren*. Mit De-Mail unternimmt die Bundesregierung den Versuch, eine vertrauenswürdige und sichere Kommunikationsinfrastruktur zu entwickeln. Aber anstatt eine dem Stand der Technik genügende Struktur mit sicherer Ende-zu-Ende-Verschlüsselung bereitzustellen, werden Sollbruchstellen eingebaut, die prinzipiell das unbefugte Mitlesen und Verändern von De-Mails ermöglichen ***(siehe Punkt 3.2)***.

Auf die Kommunen unseres Landes kommen mit den neuen E-Government-Vorhaben erhebliche technische und organisatorische Anforderungen zu. Die Kommunen sind erster Anlaufpunkt für Bürgerinnen und Bürger, wenn sie staatliche Dienstleistungen in Anspruch nehmen wollen. Dies erfordert auch dort eine funktionierende, vertrauenswürdige und vor allem sichere IT-Infrastruktur. Da verwundert es schon, dass der IT-Planungsrat mit der „Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung“ zwar für Bundes- und Landesbehörden verbindliche Sicherheitsziele für die Informationstechnik vorgibt, die Anwendung der Leitlinie den Kommunen jedoch lediglich empfiehlt ***(siehe Punkt 4.3)***. Die Mehrzahl der Mitglieder des IT-Planungsrates befürchtet offenbar, dass die Kommunen mit der Durchsetzung der Leitlinie und der Anwendung der IT-Grundschutzmethodik fachlich, personell und finanziell überfordert wären. Und diese Befürchtungen sind häufig auch berechtigt. Uns überrascht das nicht sonderlich, denn bereits im Neunten Tätigkeitsbericht hatten wir im Ergebnis einer umfangreichen Untersuchung auf zahlreiche Datenschutzprobleme in den Kommunalverwaltungen hingewiesen (siehe Neunter Tätigkeitsbericht, Punkt 6). Es ist schon bedenklich, dass offenbar nach wie vor keine angemessenen Konsequenzen gezogen wurden und die Kommunen mangels ausreichender Personal- und Finanzausstattung erhebliche Schwierigkeiten bei der Umsetzung der sicherheitstechnischen und datenschutzrechtlichen Anforderungen etwa der neuen E-Government-Verfahren haben. So stellt sich zwangsläufig die Frage, wie mit Blick auf die ständig zunehmenden Anforderungen an Datenschutz und IT-Sicherheit im kommunalen Bereich reagiert werden muss ***(Punkt 6.4.6)***. Mit dem neuen Personalausweis wurde zwar eine gute technische Infrastruktur geschaffen, die endlich eine sichere gegenseitige Identifizierung zwischen Bürgerinnen und Bürgern und Dienstleistern im staatlichen und im kommerziellen Bereich erlaubt. Doch die Bundesregierung konterkariert diese Technik, indem sie einen eher fragwürdigen Umgang mit Berechtigungen zum Auslesen der Daten aus dem Ausweis zulässt und zudem nach wie vor und wider besseren Wissens den Bürgerinnen und Bürgern die Nutzung unsicherer Kartenlesegeräte empfiehlt und somit das Vertrauen in die neue Technik untergräbt ***(siehe Punkt 6.4.5)***.

Auch Unternehmen berücksichtigen in zunehmendem Maße den Datenschutz. Sie haben erkannt, dass ihre Angebote, Produkte und Dienstleistungen nur dann für die Kundinnen und Kunden vertrauenswürdig und somit wettbewerbsfähig sind, wenn sie den Datenschutz in angemessener Weise berücksichtigen. Unternehmen erkennen immer öfter, dass Datenschutz ein Wettbewerbsvorteil sein kann und tatsächlich ist. Manchmal ist für das Finden von datenschutzfreundlichen Lösungen auch intensive Beratung durch uns nötig ***(Punkt 5.1.2)***. Unsere Beratungspraxis zeigt jedoch, dass betriebliche Interessen durchaus mit den Persönlichkeitsrechten in Übereinstimmung gebracht werden können, wenn die Prinzipien des Datenschutzes von vornherein berücksichtigt werden.

Im Bereich der Videoüberwachung ***(Punkt 5.2)*** hat sich die Idee vom Kundenvertrauen durch Datenschutz jedoch noch nicht überall durchgesetzt. Oft lassen sich Unternehmen von kostengünstigen Produkten verleiten, die inzwischen immer öfter um moderne Internettechnologien ergänzt werden. Dass durch preiswerte Technik, die zudem einfach bedienbar ist, sehr schnell neue Begehrlichkeiten entstehen, liegt auf der Hand. Und wenn dann die klassische Videoüberwachung durch Technologien zur Gesichts- und sogar Verhaltenserkennung ergänzt werden, sind Eingriffe in die Privatsphäre von Kundinnen und Kunden und Beschäftigten vorprogrammiert. Mit dieser Technik werden in zunehmendem Maße Daten unter dem Vorwand erhoben, den Service für Kundinnen und Kunden und Gäste zu verbessern. Bis zur lückenlosen Überwachung von Beschäftigten ist es dann nur noch ein kleiner Schritt, der von manchen Arbeitgebern schon einmal allzu bedenkenlos gegangen wird. Offenbar wird in vielen Fällen Rechtsbruch bewusst einkalkuliert. Sanktionen sind zunächst ja auch nicht zu erwarten, ein diesbezügliches Ordnungswidrigkeitsverfahren dauert inzwischen 3 Jahre.

Die Aufgaben, die uns der Gesetzgeber mit dem **Informationsfreiheitsgesetz** zugewiesen hat, nehmen immer mehr Zeit in Anspruch. Der ***Abschnitt 9*** dieses Berichtes gibt nur einen kleinen Einblick in die Vielfalt der Fragen, mit denen wir konfrontiert werden. Obwohl es kein Grundrecht auf Informationsfreiheit gibt, haben neben dem Bund inzwischen elf Bundesländer ein Informationsfreiheits- bzw. Transparenzgesetz verabschiedet. Es wird inzwischen in zunehmendem Maße deutlich, dass Informationen notwendig sind, damit Bürgerinnen und Bürger Entscheidungen aller Ebenen von Legislative und Exekutive verstehen und möglichst daran mitwirken – Vertrauen durch Transparenz! Mit den vielfältigen Projekten in den Bereichen Open Data und Open Government ist ein erfolgversprechender Prozess in Gang gekommen, noch verhalten, aber in die richtige Richtung.

„Die Gewährleistung von Datenschutz und Informationsfreiheit ist neben rechtlichen Vorschriften natürlich auch an bestimmte technische Voraussetzungen gebunden“, so Reinhard Dankert abschließend. „Vorrangig ist es jedoch eine Einstellungsfrage. Es geht um die Gewährleistung von Bürgerrechten, es geht um Grundrechte.“

==========

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 Elfte Tätigkeitsbericht gemäß § 33 Abs. 1 DSG M-V, der Sechste Tätigkeitsbericht gemäß § 38 Abs. 1 BDSG sowie der Vierte Tätigkeitsbericht nach dem Informationsfreiheitsgesetz umfassen den Zeitraum vom 1. Januar 2012 bis zum 31. Dezember 2013.

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 2012/2013 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/8. April 2014
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: info@datenschutz-mv.de