Schleswig-Holsteinischer Landtag
Umdruck 18/7457

www.datenschutzzentrum.de

An den
Innen- und Rechtsausschuss
des Schleswig-Holsteinischen Landtages
Düsternbrooker Weg 70
24105 Kiel

per E-Mail:
innenausschuss@landtag.ltsh.de

Holstenstraße 98
24103 Kiel
Tel.: 0431 988-1200
Fax: 0431 988-1223

Ansprechpartner/in:
Frau Hansen
Durchwahl: 988-1200

Aktenzeichen:
LD1-50.03/16.002

Kiel, 24. Februar 2017

Antrag Digitale Agenda Schleswig-Holstein: Antrag der Fraktion der FDP (Drs. 18/4850), Antrag der Fraktion der PIRATEN (Drs. 18/4883), Unterrichtung 18/256 des Ministerpräsidenten
Schriftliche Anhörung; Ihre E-Mail vom 20.01.2017

Sehr geehrte Frau Vorsitzende,
sehr geehrte Damen und Herren Abgeordnete,

ich bedanke mich für die Gelegenheit zur Stellungnahme zum Antrag Digitale Agenda für Schleswig-Holstein. Digitalisierung bietet einerseits **Chancen für unsere Gesellschaft**, andererseits sind damit **Risiken für die Menschen** verbunden. Daher ist es aus meiner Sicht wichtig, dass unser Bundesland im Rahmen der Möglichkeiten die digitalisierte Welt und die Rahmenbedingungen der Digitalisierung mitgestaltet und auf solche Lösungen hinwirkt, bei denen die Risiken eingedämmt und insbesondere die Grundrechte und Menschenrechte gestärkt werden.

In meiner **Zuständigkeit für Datenschutz und Informationsfreiheit** in Schleswig-Holstein habe ich den Entstehungsprozess der Digitalen Agenda und die Diskussion nach der Veröffentlichung der aktuellen Version mitverfolgt. Sowohl die Digitale Agenda als auch die Anträge der Fraktion der FDP und der Fraktion der PIRATEN enthalten in großen Umfang Punkte, die Datenschutz oder Informationsfreiheit berühren oder sogar ins Zentrum stellen. In den genannten Dokumenten wird an mehreren Stellen auf meine Dienststelle, das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD), verwiesen. Das ULD ist nicht nur als Aufsichtsbehörde mit den Themen befasst, sondern wird auch für Beratungen, Schulungen, Vorträge und Forschungsprojekte im Bereich der Digitalisierung und des digitalen Grundrechteschutzes angefragt. Seit vielen Jahren

bringt sich das ULD in Vorhaben zur Einführung neuer IT-Verfahren im Land und bei Kommunen intensiv ein. Damit können Aspekte des rechtlichen, technischen und organisatorischen Datenschutzes frühzeitig berücksichtigt werden. Es ist mein Bestreben, diese Praxis in Zukunft weiterzuführen. Daher begrüße ich, dass die Beteiligung des ULD in der Digitalen Agenda vorgesehen ist.

Diese Stellungnahme kann nicht vollumfänglich auf alle Themen in der Digitalen Agenda oder in den Anträgen eingehen, sondern muss sich auf Schwerpunkte beschränken. **Davon unabhängig wird das ULD bei Bedarf beratend unterstützen**, wenn es darum geht, die vorgeschlagenen Punkte konkret und praxisgerecht in **Konzepte und Implementierungen** umzusetzen. Dies betrifft auch solche aus Datenschutzsicht sehr relevanten Punkte, in denen die Digitale Agenda Datenschutz oder das ULD nicht explizit nennt, wie beispielsweise „Data Driven Government" (s. u.).

Im Folgenden werden zunächst die Digitale Agenda und anschließend die Anträge der Fraktion der FDP und der PIRATEN kommentiert:

I. Digitale Agenda

Vorbemerkung:

Die in der Digitalen Agenda genannten Einzelthemen haben großenteils einen Bezug zu Datenschutz oder Informationsfreiheit. Wie oben erläutert, werde ich nicht alle Themen im Detail kommentieren. Viele der Themen sind in der Digitalen Agenda noch sehr allgemein gehalten, und es wird vor allem in der Phase der Umsetzung darauf ankommen, die Rechte der Betroffenen zu berücksichtigen. Für die Umsetzung der Einzelmaßnahmen bietet das ULD Unterstützung in Form von Beratung an, damit **(grund-)rechtskonforme Lösungen** entwickelt werden. Zu einigen Themen hingegen werden im Text der Digitalen Agenda bereits wichtige Weichenstellungen für eine spätere Umsetzung vorgenommen. Teilweise enthält die Digitale Agenda in diesen Punkten **Formulierungen**, die **mehrdeutig oder missverständlich** sein können. Um Missverständnisse von vornherein auszuschließen, sollten die Formulierungen an diesen Stellen **präzisiert** werden, wie im Folgenden dargestellt wird.

Grundsätzliches:

Datenschutz und Informationsfreiheit – oder allgemeiner: die Grundrechte – sollten in einer Digitalen Agenda eine übergeordnete Rolle spielen. Dies betrifft insbesondere die **grundrechtskonforme Systemgestaltung** im rechtlichen, technischen und organisatorischen Bereich. Es ist Geschmackssache, ob daraus ein eigenes „strategisches Kernthema" wird oder ob dies in jedem Kernthema aufgegriffen wird. Zumindest sollte aber wegen des **übergeordneten Charakters** eine Erwähnung im vorderen Teil, beispielsweise auf Seite 8 vor der Auflistung der Kernthemen, erfolgen. Denkbar ist auch ein eigenes Kapitel, das zeigt, wie **moderner Datenschutz** im Land Schleswig-Holstein gelebt und weiterentwickelt wird. Wichtige Impulse setzen dabei die Datenschutz-Instrumente **Audit** und **Gütesiegel** sowie das **Standard-Datenschutzmodell**, das die Umsetzung der rechtlichen Anforderungen aus Land, Bund und Europa in die Praxis erleichtert. Damit können gute Lösungen aus Schleswig-Holstein über die Landesgrenzen hinweg **ausstrahlen**.

Aus den Gestaltungsanforderungen folgt eine notwendige Berücksichtigung von „Data Protection by Design and by Default" („Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen", Art. 25 DSGVO) bei Herstellern, Anbietern und Dienstleistern, beispielsweise bei **Ausschreibungen im öffentlichen Dienst**. Dies ergibt sich auch aus der EU-Datenschutz-Grundverordnung (DSGVO), die ab dem 25. Mai 2018 anwendbar sein wird (Erwägungsgrund 78 zu Art. 25 DSGVO). Zudem sollen nach § 4 Abs. 2 Landesdatenschutzgesetz Schleswig-Holstein (LDSG) Produkte, deren Vereinbarkeit mit den Vorschriften über den Datenschutz

und die Datensicherheit in einem förmlichen Verfahren festgestellt wurde (Zertifizierung), vorrangig eingesetzt werden. Das Bekenntnis der Digitalen Agenda zum **Einsatz datenschutzfreundlicher und –fördernder Informationstechnik** in der Landesverwaltung (Punkt 2.1 Nr. 7) begrüße ich. Die Berücksichtigung eines eingebauten und nachgewiesenen Datenschutzes ist leider noch keine Selbstverständlichkeit. Die jüngste Novellierung der **Landesbeschaffungsordnung Schleswig-Holstein** von Januar 2017 nimmt beispielsweise Bezug auf eine Reihe von ethischen Werten, lässt aber die Anforderungen nach eingebautem Datenschutz und eingebauter Informationssicherheit unerwähnt.

Nicht nur bei der Beschaffung, sondern auch in der **Förderpolitik** des Landes sollte „Data Protection by Design and by Default" (wie schon ähnlich erwähnt in Abschnitt 12 zum Verbraucherschutz) eine prominente Rolle spielen. Laut DSGVO sollen die **Hersteller der Produkte, Dienste und Anwendungen** ermutigt werden, das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen zu berücksichtigen (Erwägungsgrund 78 DSGVO). Informationen und Best-Practice-Beispiele zu **„Data Protection by Design and by Default"** sowohl für Implementierungen als auch bei der Entwicklung neuer Geschäftsmodelle gehören auch in die **Beratung von Unternehmen**, beispielsweise bei dem „Mittelstand 4.0-Kompetenzzentrum" oder in Wissenschaftsparks, FabLabs und Technologiezentren (Punkt 3.1 der Digitalen Agenda). Das ULD kann im Rahmen seiner Möglichkeiten unterstützend mitwirken. Im Vordergrund sollte stehen, „Data Protection by Design and by Default" **in die Förderpolitik und die Beratungskonzepte vor Ort zu integrieren.**

Zu Abschnitt 2 „E-Government und Transparenz":

Zu Punkt 2.1 Nr. 7 „Mit Datenschutz und Datensicherheit die Digitale Souveränität der Landesverwaltung sichern":

„Das Vertrauen der Bürgerinnen und Bürger in eine ordnungsgemäße Verarbeitung ihrer Daten ist die entscheidende Grundlage für alle neuen Formen der elektronischen Interaktion mit Bürgerinnen und Bürgern. Um integrierte und interaktive Dienstleistungen anbieten zu können, müssen wir mehr aus den bereits verfügbaren Daten schöpfen und gleichzeitig sicherstellen, dass die berechtigten Interessen der Bürgerinnen und Bürger auf Vertraulichkeit und nachvollziehbare Verwendung der Daten gewahrt bleiben. Wir setzen datenschutzfreundliche und -fördernde Informationstechnik ein und bauen unsere eigenen Kompetenzen im Bereich des Datenschutzes und der Datensicherheit aus. Das Recht auf informationelle Selbstbestimmung potenziell kritischer Datenverarbeitungen werden wir durch neue Konzepte, wie beispielsweise unter parlamentarischer Kontrolle stehende Datentreuhänder, zusätzlich absichern. Wir machen uns unabhängig von Monopolstellungen und stellen die Digitale Souveränität des Landes durch verstärkten Einsatz von Open Source-Software und den Eigenbetrieb bei unserem Dienstleister Dataport sicher."

Die Überschrift dieses Punktes stellt Datenschutz und Datensicherheit prominent heraus, und einige der Sätze betonen auch deren Wichtigkeit. Andere Sätze in diesem Abschnitt mögen jedoch so interpretiert werden, dass eine Datenverarbeitung **außerhalb des rechtlich Zulässigen** beworben wird, wie im Folgenden ausgeführt. Dies sollte vermieden werden.

Die Aussage, dass es für das Angebot integrierter und interaktiver Dienstleistungen notwendig sei, „mehr aus den bereits verfügbaren Daten zu schöpfen", ist in ihrer Allgemeinheit nicht korrekt und zumindest missverständlich. Es klingt an, dass alle möglichen vorhandenen Daten – möglicherweise aus verschiedenen Quellen, die zu unterschiedlichen Zwecken erhoben wurden – zu weiteren Zwecken analysiert werden sollen, um bürgerfreundliche Dienstleistungen zu erbringen. Datenschutz verhindert nicht bürgerfreundliche Dienstleistungen – hier gilt es, die Anforderungen im Einzelfall genau zu prüfen und Lösungen zu entwickeln. Eine **zweckändernde oder zweck-übergreifende Analyse aller möglichen Daten wäre aus Datenschutzsicht kritisch oder gar**

unzulässig. Der in diesem Abschnitt zum Ausdruck kommende Wunsch nach einer Big-Data-Sammlung und –Auswertung steht im Widerspruch zu den Datenschutz-Grundsätzen der Erforderlichkeit, der Zweckbindung und der Transparenz. Hier ist eine Klarstellung der Formulierung geboten.

Die Formulierung sollte außerdem klar herausstellen, dass es nicht nur um „**berechtige Interessen** der Bürgerinnen und Bürger auf Vertraulichkeit und nachvollziehbare Verwendung der Daten" geht, sondern um ihre **Rechte**. Im Unterschied zu berechtigten Interessen handelt es sich um gesetzliche Vorgaben, die erfüllt werden müssen. Die Rechte (wie auch die berechtigten Interessen) gehen zudem über Vertraulichkeit und nachvollziehbare Verwendung hinaus.

Der Hinweis auf das Recht auf informationelle Selbstbestimmung wird begrüßt; allerdings klingt die Formulierung danach, als ob **„potenziell kritische Datenverarbeitungen"** dieses Recht hätten. Das ist bestimmt nicht so gemeint. Was jedoch genau gemeint ist, erschließt sich beim Lesen des Satzes nicht: „potenziell kritische Datenverarbeitungen" sind grundsätzlich alle Verarbeitungen personenbezogener Daten durch staatliche Stellen. Einer Absicherung durch neue Konzepte steht das ULD aufgeschlossen gegenüber, jedoch wirft das genannte Beispiel von „unter parlamentarischer Kontrolle stehende[n] Datentreuhänder[n]" neue Fragen auf, falls zusätzliche Stellen zentral personenbezogene Daten speichern und vorhalten sollten oder über die Auswertung entscheiden. Hier sei auf den Grundsatz der Datensparsamkeit (§ 4 LDSG) verwiesen. Die Formulierung lässt vermuten, als ob die **gesetzliche Zuständigkeit des ULD zur Überwachung der Vorschriften des LDSG in diesem Fall ersetzt** werden soll durch eine **parlamentarische Kontrolle der Datentreuhänder**. Auch für den Fall, dass kein Ersatz, sondern eine Ergänzung durch eine solche Kontrolle gemeint ist, sollte die Motivation für diesen Vorschlag verdeutlicht und begründet werden, warum dies zu einer zusätzlichen Absicherung führen soll. In diesem Punkt wäre eine Klarstellung angeraten.

Zu Punkt 2.2 „Data Driven Government etablieren":

Während Datenschutz und Datensicherheit sowie das Recht auf informationelle Selbstbestimmung beim vorherigen Punkt 2.1 explizit behandelt wurden, könnte man aus der fehlenden Nennung dieser Konzepte beim „Data Driven Government" folgern, dass sie dabei keine Rolle spielen sollen. So ist es vermutlich nicht gemeint; vielmehr könnte der **„Ethik-Beirat ‚Daten-Analyse'"** (Punkt 2.2 Nr. 3) die notwendigen Datenschutz-Diskussionen besonders prominent herausstellen. Schließlich sollten laut Text „nicht alle Daten, die vorliegen, […] ausgewertet und genutzt werden. Der Schutz von persönlichen Rechten und unternehmerisches Handeln soll durch eine Datenanalyse nicht beeinträchtigt oder gefährdet werden."

Während eine ethische Debatte um Fragen des Data Driven Governments zu begrüßen ist, muss doch **hinterfragt** werden, welche **Konzepte der Datenanalyse und ihrer Kontrolle** zugrunde liegen. Beispielsweise legen der Begriff „data driven" und die Formulierung „welche Daten ausgewertet werden dürfen und welche nicht" nahe, dass man die vorhandenen Daten in der vorhandenen Form verwendet. Dieses Denkmodell sollte erweitert werden, denn es gibt Konzepte im technischen Datenschutz, die es ermöglichen, die **erforderlichen Informationen zu erhalten, ohne dass Daten über individuelle Bürgerinnen und Bürger verknüpft werden können**. Bei vorhandenen Datenbeständen können hier **Techniken zur Anonymisierung und Aggregation** zum Einsatz kommen. Ein wirksamerer Schutz würde **bereits bei der Erhebung der personenbezogenen Daten** dafür sorgen, dass **bestimmte Verknüpfungen und damit zusammenhängende Datenschutzrisiken technisch unterbunden werden**, aber gleichzeitig die notwendige Datenverarbeitung im Fachbereich stattfinden kann (beispielsweise durch Konzepte wie „Attribute-based Credentials"). Weiterhin könnten (technisch kontrollierbare) **Regeln zur erlaubten Verarbeitung der Daten an die Datensätze selbst gebunden** werden (beispielsweise durch Konzepte wie „Sticky Policies").

Aus Sicht des ULD ist dringend geboten, dass nicht nur die Datenanalyse des vorhandenen oder erweiterten Datenbestands, sondern **der gesamte Lebenszyklus der Verwaltungsdaten** auf den Prüfstand kommen, um zu guten und datenschutzgerechten Lösungen zu gelangen. Die Darstellung des Data Driven Governments in der Digitalen Agenda sollte daher im Sinne der obigen Darstellung überarbeitet werden. Ein Konzept, das auf einer Verwaltungsdisziplin der Datenanalysten und einem Ethik-Beirat beruht, greift unseres Erachtens zu kurz. Stattdessen wäre die **Entwicklung einer „Information Driven Government"-Strategie** unter Berücksichtigung des Stands der Technik und des Stands der Wissenschaft im Bereich des Datenschutzes angeraten. Das ULD, das auch im Fall eines eingesetzten Ethikrats weiterhin die zuständige Aufsichtsbehörde wäre, bietet hierfür seine Mitarbeit an.

Zu 2.3 „Open Data befördern":

Die Initiative für eine **Open Data-Strategie** für Schleswig-Holstein begrüße ich in meiner Zuständigkeit für Informationsfreiheit. Konkret wird es darum gehen, die Dateimanagementsysteme dahingehend einrichten, dass bei Anlage und Bearbeitung der elektronischen Akten die notwendigen Schritte zur proaktiven Veröffentlichung aller veröffentlichungsfähigen (Teil-)Akten vorgenommen werden, beispielsweise durch Trennung von Aktenteilen verschiedenen Schutzbedarfs oder durch Anonymisierungs- oder Schwärzungsfunktionalität. In der Open Data-Strategie ist der gesamte Lebenszyklus der Daten zu berücksichtigen. Für eine Beratung in diesen und verwandten auftretenden Fragen steht das ULD gerne zur Verfügung.

Weitere Einflussmöglichkeiten des Landes Schleswig-Holstein:

Das Land sollte in seiner **gesetzgeberischen Kompetenz** die Anforderungen an eine grundrechtskonforme Gestaltung der digitalisierten Welt umsetzen, wo immer dies möglich ist. Dies betrifft neben der in der Diskussion befindlichen **Novellierung des Informationszugangsgesetzes** auch die aufgrund der europäischen Datenschutzreform anzupassenden Datenschutznormen wie beispielsweise das **Landesdatenschutzgesetz**. Zudem sollte das Land Schleswig-Holstein seinen **Einfluss im Bundesrat auf die Bundesgesetzgebung** im Sinne einer grundrechtskonformen Gestaltung nutzen.

II. Antrag der Fraktion der FDP

Wie vorne erläutert, kann diese Stellungnahme nur auf Teile des Antrags der Fraktion der FDP eingehen. Generell begrüße ich, dass **Datenschutz und Informationsfreiheit eine wichtige Rolle** in dem Antrag spielen – nicht nur unmittelbar für Schleswig-Holstein, sondern auch in den Wirkungsmöglichkeiten des Landes Schleswig-Holstein auf die Entwicklungen im **Bund** und in **Europa**.

Erläuterungsbedarf besteht aus meiner Sicht in den folgenden Punkten:

Die Forderung nach einer **Einrichtung eines Cyberabwehrzentrums** (CAZ) auf Bundesebene kann sinnvoll sein. Allerdings sind die beiden formulierten Anforderungen, dass (1) dieses Cyberabwehrzentrum in das Bundesamt für Sicherheit in der Informationstechnik (BSI) integriert wird und (2) es ausdrücklich nicht dem Bundesministerium des Innern (BMI) nachgeordnet ist, vermutlich in absehbarer Zeit nicht gleichzeitig zu erfüllen. Soll dies als Arbeitsauftrag an das Land verstanden werden, sollte konkretisiert werden, welchen Bezug das CAZ zum 2011 eingerichteten Nationalen Cyber-Abwehrzentrum (keine Behörde, sondern eine Kooperationseinrichtung) hat, wie das CAZ etwa als Behörde aufgebaut werden kann und wie die Kommunikation mit anderen Bundesbehörden (insbesondere ZITIS, BKA, BfV, der Bundeswehr mit dem Forschungszentrum für

Cybersicherheit sowie der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit) und vor allem mit den Landesbehörden funktionieren soll, damit die schleswig-holsteinischen Bürgerinnen und Bürger, Wirtschaft und Verwaltung **besser vor Cyberangriffen geschützt** werden.

Unklar ist, warum es aus Sicht der Antragsteller besonders wesentlich für die Digitale Agenda des Landes Schleswig-Holstein ist, „in Zusammenarbeit mit Wirtschaft, Wissenschaft und Forschung **neue Verschlüsselungstechnologien**" zu entwickeln. Der unbefriedigende Einsatz von Verschlüsselung in Wirtschaft und Verwaltung liegt nach meiner Auffassung nicht an technologischen Fragen der Verschlüsselung, sondern an **fehlender Integration** in bestehende Systeme und Prozesse und an Defiziten in der **Benutzbarkeit**. Mängel gibt es auch in der Implementierung und in der **Qualitätskontrolle** von verbreiteten Produkten oder Systemkomponenten. Globale Bedarfe der Weiterentwicklung im Gebiet der Kryptographie bestehen insbesondere bei der **verschlüsselten Verarbeitung** in Cloud-Systemen, bei Verfahren, die **resistent** auch bei einem zukünftigen Einsatz von Quantencomputing sind, und im Gebiet der **Datenschutzforschung**. Dieser Punkt sollte erläutert werden, um festzustellen, inwieweit die aktuelle Forschungsförderung auf Bundesebene zusätzliche Schwerpunkte setzen soll und wo Anreize für die Wirtschaft verbessert werden können.

Wichtig bezüglich der „Präsenz" und dem „Angebot von Landesbehörden im Internet – insbesondere **in den sozialen Netzwerken** –" ist es, im Vorfeld auf die Datenschutzkonformität der Dienstleister hinzuwirken und die Nutzenden keinen Datenschutzrisiken auszusetzen. Dies betrifft besonders solche Dienstleister, deren Geschäftsmodell in der Auswertung der Nutzerdaten bestehen und die auf dieser Basis eine vermeintlich „kostenlose" Nutzung anbieten. Das Land Schleswig-Holstein sollte mit auszuwählenden Dienstleistern verhandeln, um Datenschutzkonformität einzufordern, bevor die Landesbehörden solche Dienstleister nutzen. Als Verhandlungsergebnis ist denkbar, dass die Präsenz der Landesbehörden in den Angeboten der Dienstleister – wie dies bei professionellen und verlässlichen Angeboten üblich ist – **gegen Bezahlung** erfolgt und selbstverständlich die Dienstleister **Datenschutzkonformität nachweisen**: Dies umfasst etwa die Transparenz über die Verarbeitung personenbezogener Daten und einen Verzicht auf eine Speicherung und Auswertung der Nutzerdaten, die bezüglich dieser Angebote anfallen. Erfolgversprechend könnte sein, wenn mehrere oder alle Bundesländer diese Verhandlungen gemeinsam führten.

Zu den medizinischen Punkten ist zu sagen, dass das ULD gerne beratend zur Verfügung steht. Dies gilt nicht nur für die Idee einer schleswig-holsteinischen **Patientenakte**, wo das ULD explizit genannt ist, sondern beispielsweise auch für **E-Health und Telemedizin**. In jedem Fall bedarf es für jedes der damit zusammenhängenden Projekte einer detaillierten Anforderungsanalyse, um die rechtlichen Rahmenbedingungen zu identifizieren und die Gestaltungsoptionen auszuloten. Das ULD steht auch für die dafür wesentlichen Fragen der **Datenschutz-Folgenabschätzung** bereit, die als neues Instrument der DSGVO eingeführt wird, um einen adäquaten Umgang mit Risiken zu gewährleisten.

III. Antrag der Fraktion der PIRATEN

Soweit die Punkte in dem Antrag der Fraktion der PIRATEN die Datenschutz oder Informationsfreiheit betreffen, stimme ich ihnen zu. Bei der Umsetzung einiger Punkte (beispielsweise bei Videokonferenzen für sensible Bereiche) muss sorgfältig geprüft werden, welche Dienstleister oder Produkte zum Einsatz kommen sollen, da vielfach eine **Marktdominanz von nicht-datenschutzkonformen Angeboten** besteht. Wie bereits am Anfang dieser Stellungnahme beschrieben, sind **künftig „Data Protection by Design and by Default" zu berücksichtigen und in öffentlichen Ausschreibungen aufzunehmen**. Das ULD unterstützt gerne dabei, die Ideen in datenschutzkonforme Lösungen für die Praxis umzusetzen.

IV. Abschließende Bemerkungen

Die Digitale Agenda und die Anträge der Fraktion der FDP und der Fraktion der PIRATEN enthalten sowohl mittelfristige Ziele als auch kurzfristig realisierbare Arbeitsaufträge. Ich rege an, für die – aufgrund der vielfältigen Diskussionsbeiträge aktualisierten – Digitale Agenda Schleswig-Holstein einen **Zeitplan** zu erarbeiten und zu veröffentlichen. Dabei sind **Priorisierungen** und **Abhängigkeiten** zu berücksichtigen. Gemäß dem Zeitplan können dann die einzelnen Vorschläge konkretisiert und **(grund-)rechtskonform** umgesetzt werden.

Für eine Erörterung meiner Stellungnahme stehe ich gern zur Verfügung.

Mit freundlichen Grüßen

gez. Marit Hansen