



# Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit  
Klosterwall 6 (Block C), D – 20095 Hamburg

An die Vorsitzende des Innen- und  
Rechtsausschuss des  
Schleswig-Holsteinischen Landtages  
Frau Barbara Ostmeier

Innenausschuss@landtag.ltsh.de

Klosterwall 6, Block C  
D – 20095 Hamburg  
Telefon: 040 - 428 54 - 40 51 Zentrale - 40 40  
Telefax: 040 - 428 54 - 40 00  
Ansprechpartner: Herr Dr. Karg  
E-Mail\*: Moritz.Karg@datenschutz.hamburg.de

Az.: D61 / 30.09-05

Hamburg, den 09.01.2017

Schleswig-Holsteinischer Landtag  
Umdruck 18/7189

## **Stellungnahme des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit zum Entwurf eines Gesetzes zur Modernisierung der elektronischen Verwaltung – Gesetzesentwurf der Landesregierung Drs. 18/4663**

Sehr geehrte Frau Ostmeier,

vielen Dank für die Möglichkeit, zum o.g. Gesetzesentwurf der Landesregierung Schleswig-Holstein Stellung nehmen zu können. Der zu beratende Gesetzentwurf regelt zentrale Elemente einer modernen digitalen Verwaltung in Schleswig-Holstein. Die Landesregierung Schleswig-Holstein legt damit die Basis für eine rechtssichere und vor allem datenschutzkonforme Ausgestaltung des E-Governments. Diese Vorgehensweise entspricht der seit 2010 vom Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI) gestellten Forderung, Dienste und Anwendungen des E-Governments, wie die E-Akte, digitale Dokumentenmanagementsysteme etc., durch entsprechende rechtliche Grundlagen abzusichern. Denn die mit dem Einsatz dieser Dienste einhergehenden Eingriffe in das Recht auf Schutz personenbezogener Daten gemäß Art. 8 EU-GrCH und dem Recht auf informationelle Selbstbestimmung gemäß Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG sind durch eine gesetzliche Grundlage zu legitimieren.<sup>1</sup>

Zentrale Forderung des HmbBfDI im Hinblick auf ein datenschutzkonformes E-Government ist die Regelung

– der datenschutzrechtlichen Verantwortung der Behörden,

<sup>1</sup> vgl. 23. Tätigkeitsbericht Ziff. II 6; <https://www.datenschutz-hamburg.de/news/detail/article/ii-6-gesetzentwurf-zum-hamburger-informationsmanagement-him-23-taetigkeitsbericht-20102011.html>

- von Vorgaben für Such- und Auswertungsfunktionen, insbesondere die Volltextrecherche,
- eines konsistenten Zugriffskonzepts,
- der Übermittlung aus elektronischen Akten und
- der Protokollierung von Zugriffen.

Der Gesetzesentwurf der Landesregierung adressiert einen Teil der Forderungen des HmbBfDI und wird insoweit ausdrücklich begrüßt. Die folgenden Anmerkungen enthalten daran anschließend weitergehende Anregungen für eine mögliche Verbesserung des Schutzes der personenbezogenen Daten der Bürgerinnen und Bürger im Rahmen einer künftigen Digitalisierung der Verwaltungsverfahren.

### **I. Gewährleistung der technischen Sicherheit**

In Art. 1 Nr. 2 § 52a Abs. 8 sowie Nr. 3 § 52 d Abs. 3 des Entwurfs werden allgemeine Vorgaben zur technischen Sicherheit der Datenverarbeitung normiert. Zusätzlich finden sich an mehreren Stellen in der Begründung des Entwurfs Bezüge zu den Vorgaben des Landesdatenschutzgesetzes (LDSG SH) im Hinblick auf die Gewährleistung der vor allem technischen Schutzziele des Datenschutzes (vgl. S. 27, 32f., 34f.).

Der HmbBfDI schlägt aus Gründen der Normenklarheit vor, einen generellen Verweis auf die Beachtung der Vorgaben des Landesdatenschutzgesetzes in den Normtext aufzunehmen und lediglich die Maßnahmen zu regeln, die aufgrund der entstehenden spezifischen technischen und rechtlichen Risiken der Digitalisierung ergriffen werden müssen. Derzeit könnte der Eindruck entstehen, dass nur für die elektronische Kommunikation und die digitale Aktenführung technisch-organisatorische Maßnahmen ergriffen werden müssten.

Dies gilt umso mehr für den ab Mai 2018 auch für die Behörden des Landes Schleswig-Holstein gemäß Art. 32 DSGVO geltenden Maßstab für die Ergreifung der technischen und organisatorischen Maßnahmen der Datensicherheit und des Datenschutzes. Bereits jetzt ist erkennbar, dass mit dem Geltungsbeginn der DSGVO eine Anpassung bisher ergriffener Maßnahmen des Datenschutzes erforderlich wird.

#### **1) Zu Nummer 2 § 52a Abs. 8**

Der HmbBfDI empfiehlt die Formulierung des Absatzes 8, um eine Normierung des technischen Standards zu ergänzen. Absatz 8 könnte dann wie folgt lauten:

*„Die elektronische Kommunikation erfolgt unter Verwendung eines dem Stand der Technik entsprechenden und der Schutzbedürftigkeit der Kommunikation angemessenen Verschlüsselungsverfahrens.“*

Die 89. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hat 2015 die Forderung aufgestellt, dass dem Stand der Technik entsprechende kryptographische Technologien in E-Government-Verfahren standardmäßig zu implementieren sind.<sup>2</sup> Die derzeit verwendete Formulierung bleibt hinter dieser Forderung zurück.

Zudem sollte darauf hingewiesen werden, dass Absatz 8 möglicherweise den Anforderungen des § 5 Abs. 1 LDSG SH nicht entspricht, wonach technisch-organisatorische Maßnahmen dem Stand der Technik entsprechen müssen. Zwar nimmt die Begründung (S. 26) diese Vorgaben in Bezug. Dem Bestimmtheitsgebot folgend empfiehlt der HmbBfDI jedoch, den Maßstab der zu gewährleistenden technischen Sicherheit in den Normtext mit aufzunehmen.

Der HmbBfDI weist in diesem Zusammenhang auch darauf hin, dass die in der Begründung getätigte Aussage, dass der Bürger auch eine unsichere Form der Kommunikation wählen kann, nicht dazu „missbraucht“ werden darf, die Verwendung einer verschlüsselten Kommunikation derart zu erschweren, dass deren Einsatz praktisch ausgeschlossen wird.

Ausdrücklich begrüßt der HmbBfDI die ebenfalls in der Begründung getätigte Aussage, dass Behörden verpflichtet sein können, bei Verwendung des Rückkanals ausschließlich verschlüsselt zu kommunizieren. Der HmbBfDI empfiehlt diesbezüglich, das Angemessenheitserfordernis in Absatz 8 mit aufzunehmen, um die Maßnahmen dem jeweiligen Schutzbedarf in konkreten Fall anpassen zu können.

In jedem Fall sollte geprüft werden, für die Übermittlung von sensiblen Daten durch die Verwaltung deutlich die Vorgabe einer Ende-zu-Ende-Verschlüsselung zu fordern.

## **2) Zu Nummer 3 § 52 d Abs. 3**

Der HmbBfDI empfiehlt, Absatz 3 um die Gewährleistung der Schutzziele des Datenschutzes und der Datensicherheit zu ergänzen.

Die Formulierung könnte lauten:

*„Wird eine Akte elektronisch geführt, ist durch geeignete technisch-organisatorische Maßnahmen nach dem Stand der Technik sicherzustellen, dass die Grundsätze ordnungsgemäßer Aktenführung eingehalten und die Schutzziele des Datenschutzes und der Datensicherheit beachtet werden. Hierzu gehört insbesondere ein Zugriffsberechtigungskonzept, das vor unzulässigen Zugriffen auf elektronisch geführte Akten schützt.“*

---

<sup>2</sup> [https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/89\\_DSK-VerschlueselungOhneEinschraenkungenErmoeglichen.pdf](https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/89_DSK-VerschlueselungOhneEinschraenkungenErmoeglichen.pdf)

Damit würde eine normenklare Regelung geschaffen werden, die gewährleistet, dass die Verarbeitung personenbezogener Daten in der elektronischen Aktenführung den technisch-organisatorischen Anforderungen des Datenschutzes entspricht. Zudem wäre auch eine Kompatibilität mit § 5 Abs. 1 LDSG und dem zukünftig geltenden Art. 32 DSGVO gewährleistet. Außerdem können Behörden auf die spezifischen Risiken für den Schutz der personenbezogenen Daten bei der elektronischen Aktenführung reagieren und den Aufwand den tatsächlichen Bedürfnissen anpassen.

Insoweit stimmt der HmbBfDI der Aussage in der Begründung des Gesetzesentwurfes nicht zu, dass an die Umsetzung der elektronischen Aktenführung keine höheren Anforderungen als an die papierbasierte Aktenführung zu stellen seien (S. 35). Es mag zutreffen, dass im Einzelfall kein höherer Schutzbedarf bei der elektronischen Aktenführung im Verhältnis zur papierbasierten Aktenführung besteht. Die Umsetzung der zur Erreichung der Schutzziele des Datenschutzes z.B. bezüglich der Vertraulichkeit der Verarbeitung, der Umsetzung der Mandantentrennung, dem Direkterhebungsprinzip, der Protokollierung und Begrenzung von Zugriffen, der Beachtung des Zweckbindungsgrundsatzes, der Integrität und Authentizität etc., kann einen höheren Umsetzungsaufwand bezüglich der zu ergreifenden technischen und organisatorischen Maßnahmen erfordern als bei der papierbasierten Bearbeitung von Akten.

## **II. Umgehung des Direkterhebungsgrundsatzes Ziff. 2 § 52a Abs. 6 Entwurf**

Nach Ansicht des HmbBfDI sollte die Umsetzung des sogenannten „Once-Only-Principles“ in § 52 a Abs. 6 des Entwurfes und die Rechtfertigung des damit einhergehenden Verstoßes gegen das Direkterhebungsprinzips gemäß § 13 Abs, 1 Satz 1 LDSG SH normenklarer geregelt werden.

Der HmbBfDI unterstützt die Intention der Landesregierung, die Umgehung des Direkterhebungsprinzips nur mit Kenntnis und dem ausdrücklich erklärten Willen der betroffenen Person zuzulassen.<sup>3</sup> In dem Gesetz sollte allerdings zweifelsfrei geregelt werden, ob die Rechtfertigung für die Umgehung des Direkterhebungsprinzips auf der Grundlage einer gesetzlichen Ermächtigung oder einer datenschutzrechtlichen Einwilligung des Betroffenen beruht.

Die derzeit verwendete Formulierung lässt eine eindeutige Beantwortung nicht zu. Der HmbBfDI schlägt daher vor, anstelle des Begriffs „Einwilligung“ den Begriff „Zustimmung“ in § 52a Abs. 6 zu verwenden. Damit wäre deutlich, dass die direkte Erhebung von

---

<sup>3</sup> Vgl. Entschließung der 91. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder Schwerin, den 6./7. April 2016  
[https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/91D SK\\_EntschliessungServicekonten.pdf](https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/91D SK_EntschliessungServicekonten.pdf)

Nachweisen auf einer landesgesetzlichen Erlaubnis beruht. Ein gesetzliches Tatbestandsmerkmal wäre die Zustimmung der betroffenen Person als zwingendes Erfordernis für die Berechtigung der verantwortlichen Stelle, Nachweise von am Verfahren nichtbeteiligten staatlichen Stellen zu erheben. Damit wäre auch gewährleistet, dass der Zugriff jeweils nur im Einzelfall und zweckbezogen im Rahmen des jeweiligen Fachverfahrens erfolgt. Außerdem würde deutlich werden, dass die gesetzliche Grundlage für die Erhebung und Verarbeitung der personenbezogenen Daten sich aus dem jeweiligen bereichsspezifischen Recht bzw. dem Landesdatenschutzgesetz ergibt. Letztlich würde diese gesetzliche Grundlage neben der erhebenden Stelle auch die angefragte Stelle zur Übermittlung der Daten legitimieren. Beide Stellen könnten sich auf die in § 52a Abs. 6 enthaltene Rechtsgrundlage berufen.

Alternativ könnte die Rechtfertigung der Umgehung auf eine allgemeine Einwilligung gestützt werden. Abgesehen davon, dass es dafür keiner gesetzlichen Anordnung bedürfte, weil die Einwilligung bereits im LDSG SH normiert und eine Umgehungen ohne Rechtfertigung rechtlich nicht möglich wäre, könnte dies allerdings faktisch zu einem Kontrollverlust seitens der Betroffenen führen. Denn eine Wirksamkeitsvoraussetzung der Einwilligung ist die Freiwilligkeit bei der Erteilung, § 12 Abs. 2 LDSG SH. Nach Auffassung des HmbBfDI wäre die Erteilung der Einwilligung allerdings kaum freiwillig.

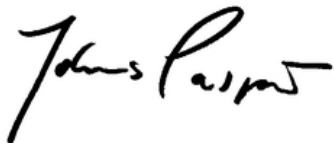
Dies ergibt sich zum einen aus dem Umstand, dass in den meisten Verwaltungsverfahren Bürgerinnen und Bürger eine Beibringungspflicht haben. Außerdem ist es erklärtes Ziel der Landesregierung, Verwaltungsverfahren medienbruchfrei und völdigitalisiert durchzuführen, (§ 52a Abs. 5 des Entwurfs). Insoweit kommt zu der regelmäßigen Beibringungspflicht die zusätzliche Anforderung an Bürgerinnen und Bürger, digitale Nachweise zu erbringen (vgl. Begründung S. 24f). Hinzukommt, dass die Landesregierung offenbar davon ausgeht, dass Nachweisen direkt von der ausstellenden Behörde eine höhere Verlässlichkeit zukommt (S. 25). Bei einer realistischen Betrachtungsweise führt dies letztlich dazu, dass die betroffene Person keine tatsächliche Wahlfreiheit mehr hat.

Außerdem kann nach Auffassung des HmbBfDI nicht ausgeschlossen werden, dass Behörden versuchen, „Vorratseinwilligungen“ von den Betroffenen zu erhalten. Denn die recht komplexen Anforderungen an die Umsetzung einer rechtswirksamen elektronischen Einwilligung und der damit verbundene Aufwand werden Bestrebungen fördern, möglichst selten das Einwilligungsverfahren durchzuführen. Das könnte die Tendenz zur Formulierung eher globalerer Zweckbestimmungen in den Einwilligungen fördern, was im Ergebnis zu einem Kontrollverlust seitens der Betroffenen führen würde. Zudem ist zu erwarten, dass mit Geltungsbeginn der DSGVO die Anforderungen an eine wirksame Einwilligung nochmals steigen werden.

Letztlich sprechen auch systematische Gründe gegen die Einwilligungslösung. Denn diese müsste von der betroffenen Person sowohl gegenüber der erhebenden als auch der übermittelnden Stelle, also zweimal erteilt werden. Auch wenn dies in einem Handlungsakt verbunden werden könnte, wären beide staatlichen Stellen gemäß § 12 Abs. 3 Nr. 4 LDSG SH verpflichtet, jeweils erteilte Einwilligungen zu protokollieren. Aus o.g. Gründen empfiehlt der HmbBfDI, daher keine Einwilligungslösung zu wählen.

Ich bitte um Ihr Verständnis, dass eine Stellungnahme zu weiteren, ebenfalls datenschutzrelevanten Themen aufgrund der beschränkten personellen Ressourcen des HmbBfDI derzeit nicht möglich ist. Gern stehe ich insoweit dem Innen- und Rechtsausschuss, soweit dies gewünscht ist, für eine mündliche Erläuterung zur Verfügung.

Mit freundlichen Grüßen

A handwritten signature in black ink, appearing to read 'Johannes Caspar'. The signature is written in a cursive, flowing style.

Prof. Dr. Johannes Caspar