Schleswig-Holsteinischer Landtag
Umdruck 18/7178

www.datenschutzzentrum.de

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

Ansprechpartner/in:
Frau Mohammadi
Durchwahl: 988-1284

Aktenzeichen:
LD2.2-01.03/16.003

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

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

Kiel, 6. Januar 2017

Gesetzentwurf der Landesregierung zur Modernisierung der elektronischen Verwaltung (LT-Drs. 18/4663)
Sachverständigenanhörung; Ihre E-Mail vom 23.11.2016

Sehr geehrteFrau Vorsitzende,
sehr geehrte Damen und Herren Abgeordnete,

ich bedanke mich für die Gelegenheit zur Stellungnahme zu dem oben genannten Gesetzentwurf im Rahmen der schriftlichen Anhörung des Innen- und Rechtsausschusses des Schleswig-Holsteinischen Landtages, die ich gern wahrnehme.

Den Gesetzentwurf der Landesregierung begrüße ich grundsätzlich. Die vorgeschlagenen Regelungen fördern in den Bereichen der elektronischen Aktenführung und elektronischen Kommunikation mit Bürgerinnen und Bürgern Rechtssicherheit und Rechtsklarheit.

Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) ist im Rahmen der Ressortabstimmung angehört worden. Viele unserer Anmerkungen wurden bereits in dem vorliegenden Entwurf umgesetzt. Aus Datenschutzsicht sollten jedoch einige weitere Änderungen vorgenommen werden.

1. Zu § 52 a Absatz 8 LVwG-E

Gemäß Absatz 8 bieten die Behörden für die elektronische Kommunikation geeignete Verschlüsselungsverfahren an. In der Begründung heißt es: „Datenschutzrechtliche Vorschriften verlangen, dass bei der elektronischen Übertragung von Dokumenten mit personenbezogenen

Daten diese nicht unbefugt gelesen und kopiert werden können. Bei einer Übertragung über das Internet kann dies nur durch eine entsprechende Transportverschlüsselung gewährleistet werden.“ (S. 26). Diese Aussage stimmt so nicht. Unter Transportverschlüsselung versteht man eine Punkt-zu-Punkt-Verschlüsselung zwischen den technischen Kommunikationseinheiten, so dass die transportierte Nachricht auf dem Übertragungsweg verschlüsselt ist, jedoch am Endpunkt entschlüsselt vorliegt. Dieser Endpunkt kann z. B. ein von einem Diensteanbieter betriebener Server sein, wo die Verschlüsselung endet. Eine durchgängige Verschlüsselung zwischen Sender und Empfänger leistet dagegen die Ende-zu-Ende-Verschlüsselung. Beim Empfänger kann es sich um einen Sachbearbeiter oder – im Behördenfall ebenfalls denkbar – um die Kopfstelle einer Behörde oder einer kleineren Organisationseinheit (z. B. Abteilung) handeln, wohin durchgehend die Verschlüsselung aufrechterhalten bliebe. Die Betonung der Transportverschlüsselung („nur“) in der Begründung geht fehl; sie ist nicht die einzige Maßnahme, um die Bedingungen der sicheren Kommunikation zu erfüllen, und wenn sie zum Einsatz kommen soll, muss geprüft werden, ob der Schutz lediglich bis zum technischen Endpunkt der Datenübertragung ausreicht oder eine Ende-zu-Ende-Verschlüsselung erforderlich ist.

Laut Begründung soll die Wahl des Verschlüsselungsverfahrens im Organisationsermessen der jeweils zuständigen Behörde liegen (S. 27). Bei der Übermittlung von besonders sensitiven Daten könne „unter Umständen“ auch eine Ende-zu-Ende-Verschlüsselung angeboten werden. Aus Sicht des ULD reicht dies nicht aus: **Zumindest für sensitive Daten genügt eine Transportverschlüsselung üblicherweise nicht den datenschutz- bzw. datensicherheitsrechtlichen Standards.** Sie gewährleistet einen Schutz der Daten vor Kenntnisnahme oder Veränderung durch Unbefugte nur auf dem Übertragungsweg, nicht aber bei den an der Übertragung beteiligten Stellen. Damit kann sie allenfalls für personenbezogene Daten ohne besonderen Schutzbedarf ausreichend sein. Im Zuge der elektronischen Kommunikation in der Verwaltung sollen jedoch auch Sozialdaten, Gesundheitsdaten und Steuerdaten übermittelt werden. Hierbei handelt es sich um eine besondere Art von Daten, die keinesfalls der Gefahr des Datenmissbrauchs oder der Manipulation ausgesetzt werden dürfen.

Gerade wenn es um die **Übermittlung sensitiver Daten** (v. a. Sozialdaten, Gesundheitsdaten und Steuerdaten) geht, sollte eine **Ende-zu-Ende-Verschlüsselung verpflichtend** sein. Unter dem Gesichtspunkt, dass § 203 StGB die Verletzung eines Privatgeheimnisses unter Strafe stellt, sollten die Risiken, die bei einer Transportverschlüsselung tatsächlich bestehen, vermieden werden.

Aus diesen Gründen sollte in dem Begründungstext auf Seite 27 der Satz „Bei besonders sensitiven Daten kann unter Umständen auch eine Ende-zu-Ende-Verschlüsselung angeboten werden.“ umformuliert werden zu

> **„Bei sensitiven Daten ist eine Ende-zu-Ende-Verschlüsselung der Kommunikation zu unterstützen.“**

2. Zu § 52 g LVwG-E (Elektronische Zahlungsverfahren)

§ 52 g Abs. 1 LVwG-E regelt die Möglichkeit der elektronischen Bezahlung in Verwaltungsverfahren. Problematisch ist die weite Verbreitung von Bezahlverfahren, die nicht den datenschutzrechtlichen Anforderungen genügen, beispielsweise weil sich die Anbieter bislang nicht an europäisches Datenschutzrecht gebunden fühlen. Daher **reicht** die Formulierung des §

52 g Abs. 1 LVwG-E, die lediglich auf **„üblich“ und „hinreichend sicher“** abstellt, **nicht aus**. Hier sollte ergänzt werden:

> „Fallen im Rahmen eines elektronisch durchgeführten Verwaltungsverfahrens Gebühren oder sonstige Forderungen an, muss die Behörde die Einzahlung dieser Gebühren oder die Begleichung dieser sonstigen Forderungen durch Teilnahme an mindestens einem im elektronischen Geschäftsverkehr üblichen **Zahlungsverfahren, das die Anforderungen des Datenschutzes und der Datensicherheit nachweislich erfüllt,** ermöglichen.“

3. Zu § 52 i LVwG-E Zentrale E-Governmentstelle

Der **Zentralen E-Governmentstelle** kommt eine **besondere Bedeutung** zu, da dort eine Einheitlichkeit der elektronischen Verfahrenshandhabung in der öffentlichen Verwaltung sichergestellt und die rechtliche und technische Kompetenz in E-Government-Angelegenheiten gebündelt werden soll (siehe S. 42). Gemäß § 52 i handelt es sich um die „für die Angelegenheiten der ressortübergreifenden IT zuständige oberste Landesbehörde“. Hier sollte geklärt und zumindest in der Begründung näher ausgeführt werden, wie das **Zusammenspiel zwischen dezentralen und zentralen Anforderungen und Komponenten** geregelt wird und wer für welche Teile die **(datenschutz-)rechtliche Verantwortung** übernimmt. Aufgrund der notwendigen Trennung von Verwaltungseinheiten ist es notwendig, dass trotz zentraler Vorgaben stets auch dezentrale Anforderungen Berücksichtigung finden müssen.

Dies zeigt sich beispielsweise bei einer **Ende-zu-Ende-Verschlüsselung**, bei der ein **Virenscan** auf dem Transportweg nicht erfolgreich wäre, sondern dies dezentral im Bereich der empfangenden Stelle geschehen muss. Eine Aktualisierung der Systeme für den Virenscan könnte wiederum zentral erfolgen.

Ein weiteres Beispiel besteht in der **Signaturprüfung**: Signaturen können dezentral geprüft werden. Dies erfordert aber die Kenntnis über die Gültigkeit der Signaturen und über möglicherweise für ungültig erklärte Signaturzertifikate (über Revocation-Listen). Eine Signaturprüfung kann so ablaufen, dass gegen dezentral vorgehaltene, ständig zu aktualisierende Revocation-Listen geprüft wird. Die zentralisierte Alternative, dass die Behörden für jede Signaturprüfung einen Online-Abgleich bei einer zentralen Signaturprüfstelle, die diese Revocation-Liste vorhält, vornehmen, birgt aus Datenschutzsicht ein Risiko, denn bei dieser zentralen Signaturprüfstelle wird sichtbar – und möglicherweise auch gespeichert – , wann welche Behörde ein Dokument von welchem Urheber (d. h. Signaturersteller) bearbeitet. So kann auch festgestellt werden, welche Urheber bei mehreren Behörden Dokumente in der Bearbeitung haben. **Selbst wenn diese Daten einer Behörde verschlüsselt zugestellt wurden, ist der Urheber bei der Signaturprüfstelle erkennbar, und selbst bei der Verwendung von pseudonymen Signaturen kann die Signaturprüfstelle eine Verkettung von verschiedenen Dokumenten vornehmen.** An diesem Beispiel zeigt sich, dass ein rein zentrales Vorhalten einer Funktion für Signaturprüfung aus Datenschutzsicht unerwünschte Effekte haben kann, die eine notwendige Mandantentrennung gefährden können. Dies liefe der **Anforderung „Datenschutz durch Technikgestaltung“** zuwider, die mit der europäischen Datenschutz-Grundverordnung (DSGVO) Pflicht wird (Art. 25 DSGVO).

Da die **Anforderungen der IT-Sicherheitsstandards** bereits in § 52 j zum Ausdruck kommen, sollte § 52 i um **Datenschutzanforderungen** und speziell das Prinzip „Datenschutz

durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“, wie es in Art. 25 DSGVO definiert ist, schon im Vorgriff auf das künftige Landesdatenschutzgesetz ergänzt werden:

> „Zentrale E-Governmentstelle ist die für die Angelegenheiten der ressortübergreifenden IT zuständige oberste Landesbehörde. Die Zentrale E-Governmentstelle wirkt auf eine einheitliche Anwendung der Vorschriften über die elektronische Verwaltung hin. **Dabei berücksichtigt sie die Anforderungen des Datenschutzes, insbesondere des Prinzips „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“.** Sie berät Behörden im Anwendungsbereich dieses Gesetzes bei der Durchführung von elektronischen Verfahren.“

Für eine Erörterung der Stellungnahme stehe ich gern zur Verfügung.

Mit freundlichen Grüßen

gez. Marit Hansen