Stellungnahme zum Entwurf eines Gesetzes zur Förderung der elektronischen Verwaltung im Saarland sowie zur Änderung weiterer Vorschriften

Christoph Sorge Ninja Marnau
CISPA
Universität des Saarlandes

Vorbemerkung

Die vorliegende Stellungnahme wurde durch zwei Forscher des CISPA – Univ.-Prof. Dr.-Ing. Christoph Sorge, Inhaber der juris-Stiftungsprofessur für Rechtsinformatik, und Ninja Marnau, Senior Researcher am CISPA – erstellt. Das CISPA (Center for IT Security, Privacy) ist eines von drei BMBF-geförderten Forschungszentren für IT-Sicherheit und befindet sich derzeit im Ausgründungsprozess. Mit Unterstützung von Landes- und Bundesregierung ist geplant, dass das CISPA als Helmholtz-Zentrum für Informationssicherheit von der Helmholtz-Gemeinschaft aufgenommen wird.

1 Einleitung

Mit dem vorliegenden Gesetzentwurf werden die Voraussetzungen für den elektronischen Zugang zur Verwaltung geschaffen. Wir begrüßen dies nicht nur als effizienzsteigernde Maßnahme, sondern sehen darin auch einen Beitrag, den Zugang zu Verwaltungsdienstleistungen zu erleichtern und damit letztlich die Attraktivität des Saarlandes als Wirtschaftsstandort und als Wohnsitzland zu erhöhen. Nicht zu vergessen ist auch die Wirkung für Menschen mit Behinderungen; so kann der elektronische Zugriff auf — entsprechend § 8 des Saarländischen Behindertengleichstellungsgesetzes sowie der Saarländischen Behindertengleichstellungsverordnung gestaltete — elektronisch angebotene Dienstleistungen eine erhebliche Erleichterung im Vergleich zu „Offline“-Angeboten

darstellen. Im Folgenden werden wir den Schwerpunkt unserer Betrachtung aber auf die Aspekte des Datenschutzes und der IT-Sicherheit legen.

2 Sichere Bereitstellung von Informationen und sicherer Zugang zur Verwaltung

Im vorliegenden Entwurf regeln §§ 2 und 3 EGovG die Bereitstellung von Informationen und den elektronischen Zugang zur Verwaltung. Zu § 2 Abs. 3 möchten wir anmerken, dass die Begriffe der „sicheren“ und „vertrauenswürdigen“ Bereitstellung auslegungsbedürftig sind. Die Begründung konkretisiert, dass die Gewährleistung der Authentizität gemeint ist. Dies kann, wie in der Begründung ebenfalls dargestellt, mit Hilfe TLS-gesicherter Übertragung erreicht werden.[1] Andererseits wäre die Absicherung mit höherem Sicherheitsniveau durch (fortgeschrittene bzw. qualifizierte) elektronische Signaturen oder Siegel möglich. Wir gehen nicht davon aus, dass die Auslegung der Norm zum Ergebnis kommt, dieses höhere Niveau sei erforderlich; eine Klarstellung könnte aber die Rechtssicherheit erhöhen. Der Begriff der „Sicherheit“ könnte zudem die Sicherstellung der Verfügbarkeit, etwa durch redundante Server, beinhalten.

Die Vorgabe der sicheren Bereitstellung sollte aus unserer Sicht ebenso für den neuen § 5a der Verordnung über die öffentlichen Bekanntmachungen der Gemeinden und Gemeindeverbände gelten. Auch wenn die Anforderung des § 2 Abs. 3 EGovG gegebenenfalls auch in diesem Fall Anwendung findet, sollte im Sinne der Rechtsklarheit und um zu verhindern, dass die auf den Webseiten[2] der Gemeinden publizierte öffentliche Bekanntmachung von Dritten während der Übertragung manipuliert werden könnten, auch hier auf eine Pflicht zur „sicheren und vertrauenswürdigen Bereitstellung“ im Rahmen eines Verweises auf § 2 Abs. 3 EGovG ergänzt werden.

Auslegungsbedürftig ist aus unserer Sicht auch § 3 Abs. 1 Satz 2 EGovG. Die Norm kann sich, wie in der Begründung wohl unterstellt, sowohl auf den Transportweg (TLS-verschlüsselte Übertragung) als auch auf die übertragenen Dokumente (z.B. verschlüsselte Zip-Archive, zu denen das Passwort telefonisch mitgeteilt wird) beziehen. Ende-zu-Ende-verschlüsselte E-Mails stellen einen weiteren Weg dar. Für den Bürger am komfortabelsten ist sicherlich die Bereitstellung eines Web-Portals, in dem die Behörde einen verschlüsselten Datei-Upload anbietet. Die Lösungen unterscheiden sich deutlich im Umsetzungsaufwand und der Praktikabilität. Angesichts der Verpflichtung aus dem Onlinezugangsgesetz wird mittelfristig jedenfalls eine Integration in die dort geforderte Portallösung anzustreben sein.

[1] Die Begründung differenziert zwischen SSL und TLS; im allgemeinen Sprachgebrauch werden beide Begriffe oft als Synonyme verwendet. In der Tat hießen die bis 2001 aktuellen Vorgängerversionen der aktuellen TLS-Standards SSL; differenziert man zwischen beiden Protokollen, ist von der Verwendung vom veralteten SSL-Standards aber jedenfalls dringend abzuraten.

[2] Der Entwurf des § 5a spricht hier von „Internetseiten“ und „Internetadressen“. Wir möchten anregen, dies durch „Webseiten“ und „Domain-Namen“ zu ersetzen.

3 IT-Sicherheit beim ersetzenden Scannen

Die Regelung des § 7 EGovG-E entspricht im Wesentlichen der bundesgesetzlichen Regelung. Wir halten sie für sachgerecht. Einerseits ist das Einscannen bei digitalisierten Geschäftsprozessen die einzige Möglichkeit, mit nach wie vor eingehenden Papierdokumenten umzugehen; andererseits muss sichergestellt werden, dass das Digitalisat mit dem Papieroriginal übereinstimmt. Der Gesetzesentwurf erwähnt lediglich die bildliche Übereinstimmung und sieht hierfür ein Vorgehen „nach dem Stand der Technik“ vor. Eine ergänzende Texterkennung (OCR), die z.B. eine Volltextsuche ermöglicht, wird nicht gefordert; selbstverständlich steht diese Möglichkeit trotzdem offen. In der Literatur wird – zutreffend – die Technische Richtlinie des BSI zum rechtssicheren Scannen (TR RESISCAN)[3] als maßgebliche Darstellung des Stands der Technik gesehen; insoweit besteht also auch keine Rechtsunsicherheit.

Es sei allerdings darauf hingewiesen, dass die TR RESISCAN Freiheitsgrade in der konkreten Umsetzung lässt. Insbesondere ist der jeweilige Schutzbedarf der gescannten Dokumente bezüglich mehrerer Schutzziele zu bewerten und die zu treffenden Schutzmaßnahmen entsprechend auszuwählen. Diese Aufgabe ist nicht zu unterschätzen. Durch ein koordiniertes Vorgehen dürften Effizienzgewinne zu erwarten sein; denkbar ist aus unserer Sicht auch eine Verordnungsermächtigung, um der Landesregierung die Möglichkeit zu geben, den zugrunde zu legenden Schutzbedarf für Verfahrens- oder Dokumentenarten landesweit festzulegen. Die Verordnungsermächtigung des § 3 Abs. 5 könnte zu diesem Zweck ausgeweitet werden.

4 Elektronische Siegel

Wir möchten außerdem anregen, die Verwendung (fortgeschrittener oder qualifizierter) elektronischer Siegel zu prüfen, die durch die eIDAS-Verordnung eingeführt worden sind. Diese haben aus technischer Sicht die gleichen Eigenschaften wie die entsprechenden elektronischen Signaturen. Sie sind jedoch juristischen Personen zugeordnet und ermöglichen daher die Sicherstellung der Authentizität und Integrität von Dokumenten, die beispielsweise von einer Behörde erstellt wurden. Daher dürften sie in vielen Anwendungsfällen praktikabler sein als elektronische Signaturen der jeweils handelnden natürlichen Personen. Der vorliegende Entwurf sieht in § 3 Abs. 1 EGovG die Entgegennahme von Dokumenten vor, die mit einem elektronischen Siegel versehen sind. Darüber hinaus wäre es aus unserer Sicht zielführend, zu prüfen, in welchen Fällen, in denen bislang die elektronische Signatur gefordert ist, auch elektronische Siegel zum Einsatz kommen könnten. Denkbar wäre dies etwa im Fall des ersetzenden Scannens, um die Übereinstimmung des Scanprodukts mit dem Papieroriginal zu bestätigen. Bedeutsamer erscheinen uns jedoch Regelungen außerhalb des E-Government-Gesetzes, etwa im SVwVfG oder im AmtsBlG. Gegebenenfalls könnte der Prüfauftrag des § 20 entsprechend erweitert werden.

[3] BSI Technische Richtlinie 03138 – Ersetzendes Scannen, aktuell vorliegend in Version 1.1 vom 02.03.2017

5 Technikneutralität und De-Mail

Angesichts der verfassungsrechtlichen Implikationen von staatlichen Technologievorgaben unterliegen diese strengen Anforderungen an Technik- und Marktneutralität. „Verbindliche staatliche Technologievorgaben können in Konflikt mit Verfassungs- und Vergaberecht geraten, soweit den verankerten IT-Standards eine spürbare marktregulierende Wirkung zukommt, etwa weil sie all jene IT-Produkte und Dienstleistungen vom Beschaffungsmarkt der Öffentlichen Hand abkoppeln, die sich als nicht „standardkonform“ erweisen“[4]. Der Entwurf des EGovG versucht hier eine Balance zu finden zwischen zentralen Diensten und Standards und der Öffnung hin zum EU-Binnenmarkt und insbesondere den Nachbarländern Frankreich und Luxemburg. Aus unserer Sicht gelingt dies gut. Bedenkenswert ist lediglich, dass die Öffnung teilweise lediglich in der Gesetzesbegründung erfolgt und nicht im Gesetzestext selbst – etwa bezüglich der elektronischen Erreichbarkeit per De-Mail.

Die Gesetzesbegründung führt hier aus: „Um die problemlose elektronische Erreichbarkeit im Bereich des EU-Binnenmarktes gem. den unionsrechtlichen Anforderungen sicherzustellen, sollen die über De-Mail erreichbaren Behörden nicht ausschließlich auf akkreditierte De-Mail-Dienste hinweisen, sondern auch auf im Sinne des § 19 des De-Mail-Gesetzes gleichgestellte ausländische Dienste. Hierzu genügt es, einen elektronischen Verweis auf die im Internet durch das BSI jeweils aktuell veröffentlichte Liste solcher Anbieter einzufügen.“

Ebenso wie in § 3 Abs. 4 EGovG für ausländische elektronischen Identitätsnachweise wäre eine explizite Öffnung im Gesetz im Hinblick auf gleichgestellte ausländische Dienste nach § 19 des De-Mail-Gesetzes wünschenswert.

6 Datenschutz

Die EU Datenschutzgrundverordnung (DSGVO) wird am 25. Mai 2018 in Kraft treten. Sie wird dann grundsätzlich auch für alle bundes-, landes- und kommunalrechtlichen Aufgabenbereiche gelten, bei denen personenbezogenen Daten verarbeitet werden. Die DSGVO enthält jedoch auch einige Öffnungsklauseln, die dem Landesgesetzgeber erlauben, spezifischere Bestimmungen zur Anpassung der Anwendung der Vorschriften der Verordnung einführen. Darunter fällt auch Artikel 6 zur Rechtmäßigkeit der Verarbeitung. Absatz 2 erlaubt den nationalen Gesetzgebern von Absatz 1 Satz e (die Rechtsgrundlage für die Rechtmäßigkeit der Verarbeitung für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt) abzuweichen, „indem sie spezifische Anforderungen für die Verarbeitung sowie sonstige Maßnahmen präziser bestimmen, um eine rechtmäßig und nach Treu und Glauben erfolgende Verarbeitung zu gewährleisten, einschließlich für andere besondere Verarbeitungssituationen“.

Daher können auch die eGovermentgesetze des Bundes und der Länder besondere datenschutz- und informationssicherheitsspezifische Regelungen umfassen. Allerdings

[4] *Heckmann/Bernhardt*: Digitale Gewaltenteilung als Marktverantwortung, Passau 2016.

müssen diese spezifischen Regelungen mit den übrigen Vorgaben der DSGVO in Übereinstimmung sein. Diese Balance gelingt dem vorliegenden Entwurf zum größten Teil. Lediglich in Bezug auf die folgenden Detailbestimmungen bestehen Zweifel an der Vereinbarkeit mit der DSGVO. Diese werden vor allem darauf zurückzuführen sein, dass hier Regelungen des Bundesgesetzes übernommen wurden, welches zeitlich vor der DSGVO entstand. Hier ist zwar grundsätzlich eine EU-rechtskonforme Auslegung möglich, im Interesse der Rechtssicherheit für die beteiligten Stellen würden wir jedoch zu einer Anpassung dieser Regelungen raten.

Die Regelung des § 15 EGovG zum gemeinsamen Verfahren entspricht der weitgehend gleichlautenden Regelung des Bundesgesetzes, die laut der Gesetzesbegründung des vorliegenden Entwurfs wiederum „auf einem Vorschlag seitens der Konferenz der Datenschutzbeauftragten des Bundes und der Länder beruht. Eine entsprechende Vorschrift wäre zudem in die jeweiligen Datenschutzgesetze der Länder aufzunehmen.“ Dennoch erscheint die Formulierung im Hinblick auf die Vereinbarkeit mit der DSGVO zumindest zweifelhaft. Es stellt sich die Frage, ob hier nicht ausschließliche der Art. 26 DSGVO zur Anwendung kommen darf. Dieser legt abschließend fest, welchen Regeln Gemeinsam für die Verarbeitung Verantwortliche unterliegen. Aus unserer Sicht gibt es keine Öffnungsklausel, die Spielraum für den § 15 EGovG erlaubt.

Die Regelungen des § 15 EGovG widerspricht auch im Detail den Anforderungen der DSGVO. Die Regelung des § 15 Abs. 4 Satz 1 Nr. 2 EGoVG gibt vor, vor der Einrichtung oder wesentlichen Änderung eines gemeinsamen Verfahrens die für die Rechtmäßigkeit der Verarbeitung verantwortliche Stelle „festzulegen“. In Bezug darauf, wer der Verantwortliche einer Datenverarbeitung (Art. 4 Nr. 7 DSGVO) ist, bzw. ob es sich bei den Beteiligten ggf. um gemeinsam Verantwortliche handelt, erscheint diese unabhängige Festlegung nach eGovG zweifelhaft.

Ebenso scheint der § 15 Abs. 6 EGovG unvereinbar mit der Art. 26 Abs. 3 DSGVO. Zwar erlaubt die Norm den Betroffenen sich an jede Stelle des gemeinsamen Verfahrens zu wenden. Diese solle das Anliegen an die jeweils zuständige Stelle weiterleiten. Art. 26 Abs. 3 DSGVO sieht eine solche Weiterleitung jedoch nicht vor. Vielmehr ist jeder der gemeinsam Verantwortlichen zuständig dafür, die Betroffenenrechte zu erfüllen und dem Anliegen abzuhelfen.

Wir plädieren in Anbetracht des Vorrangs der DSGVO und des Wiederholungsverbots dafür, die Geltung des § 15 EGovG bis zum 25.5.2018 zu befristen. Behält der nationale Gesetzgeber Normen bei, die dem vorrangigen Unionsrecht widersprechen, verstößt er damit gegen die Verpflichtung aus dem EU Primärrecht zur loyalen Zusammenarbeit (Art. 4 Abs. 3 EUV).[5]

§ 6 Abs. 3 EGovG regelt die Einwilligung von Verfahrensbeteiligten für die direkte Einholung von Nachweisen von der Stelle bei der sie vorliegen. Hier stellt sich die Frage, ob die Anforderungen an die elektronische Form der Einwilligung mit den Vorgaben des Art. 7 DSGVO entsprechen. Insbesondere schreibt Art. 7 Abs. 3 Satz 4 DSGVO vor, dass der Widerruf der Einwilligung ebenso einfach wie die Einwilligung selbst sein muss. Wir schlagen daher vor, den § 6 Abs. 3 Satz 2 Nr. 2 EGovG um die Möglichkeit des

[5] *Kühling/Martini et al.*, “Die Datenschutz-Grundverordnung und das nationale Recht”, 2016.

elektronischen Widerrufs zu ergänzen.

Ebenfalls Zweifel im Hinblick auf datenschutzrechtliche Fragen wirft die Verordnungsermächtigung in § 17 Abs. 2 EGovG zu Nutzungsbestimmungen für das Bereitstellen von Daten auf. Diese auf Open Data gerichtete Regelung orientiert sich an § 12 des Bundesgesetzes. Der Absatz 2 Satz 1 ermächtigt die Landesregierung, die Nutzungsbestimmungen, gemeint sind Lizenzen, festzulegen. Dabei sollen nach der Gesetzesbegründung ausdrücklich prinzipiell auch kommerzielle Weiternutzungen und Datenverwendungen ermöglicht werden. Die Gesetzesbegründung führt beispielhaft als Fragestellung für die Nutzungsbedingungen auf: „Darf der Nutzer die Daten verändern? Darf der Nutzer die Daten mit anderen Daten zusammenführen?“. Gerade eine solche Zusammenführung von an sich nicht personenbezogenen Daten kann jedoch ein Risiko der möglichen Re-Identifizierbarkeit von Betroffenen eröffnen. Bei der Auswahl der Nutzungsbedingungen für Open Data sollte dieses Risiko ggf. evaluiert werden und durch besondere Hinweise in den Nutzungsbedingungen abgemildert werden.

7 IT-Kooperationsrat

Der IT-Kooperationsrat erörtert die wesentlichen und grundsätzlichen IT-Themen für das Land und die Kommunen und kann hierzu Empfehlungen aussprechen. Wir möchten im Hinblick auf das in der Gründung befindliche CISPA-Helmholtzzentrum für Informationssicherheit anregen, dieses bei Bedarf beratend für Fragen der Informationssicherheit beizuziehen, da das CISPA künftig nicht mehr über das ständige Mitglied Universität des Saarlandes vertreten sein wird.

8 Fazit

Wie eingangs ausgeführt, begrüßen wir den vorliegenden Entwurf, möchten aber insbesondere auf folgende Punkte hinweisen:

- Ersetzendes Scannen nach dem „Stand der Technik“ erfordert eine Schutzbedarfsanalyse; wir schlagen vor, nach Wegen zu suchen, diese möglichst so zu koordinieren, dass nicht mehrere Behörden für gleiche Dokumentarten diesen Prüfprozess wiederholen müssen.

- Die Einführung elektronischer Siegel könnte einzelne Prozesse in der Verwaltung vereinfachen; ein entsprechender Prüfauftrag ließe sich in § 20 EGovG aufnehmen.

- Die Regelung des § 15 EGovG zum gemeinsamen Verfahren steht im Konflikt zu Art. 26 DSGVO. Wir plädieren in Anbetracht des Vorrangs der DSGVO und des Wiederholungsverbots dafür, die Geltung des § 15 EGovG bis zum 25.5.2018 zu befristen. Aus unserer Sicht ist Art. 26 DSGVO ausreichend für de im eGovG identifizierten Regulierungsbedarf für gemeinsame Verfahren.

- Ebenso wie in § 3 Abs. 4 EGovG für ausländische elektronischen Identitätsnachweise wäre eine explizite Öffnung im Gesetz im Hinblick auf gleichgestellte ausländische Dienste nach § 19 des De-Mail-Gesetzes wünschenswert.

- Für den IT-Kooperationsrat möchten wir im Hinblick auf das in der Gründung befindliche CISPA-Helmholtz-Zentrum für Informationssicherheit anregen, dieses bei Bedarf beratend für Fragen der Informationssicherheit beizuziehen.