UNABHÄNGIGES DATENSCHUTZZENTRUM SAARLAND

Erwartungen an den neuen Landtag und die neue Landesregierung im Saarland

Inhalt

Das Saarland steht in den nächsten Jahren vor großen Herausforderungen. Unter anderem die mit der zunehmenden Digitalisierung einhergehenden Veränderungen sozialer, ökonomischer, kultureller und institutioneller Art haben erhebliche Auswirkungen auf das wirtschaftliche und gesellschaftliche Leben im Saarland.

Dem Datenschutz kommt dabei durchaus eine Schlüsselrolle zu, denn unabdingbare Voraussetzung für die Akzeptanz digitaler Transformation ist Vertrauen der Nutzerinnen und Nutzer in die entsprechenden Verfahren und Prozesse. Dieses Vertrauen muss durch ausgeprägten Datenschutz, datensparsames Systemdesign, Aufklärung der Nutzer und durch wirksame IT-Sicherheitsmaßnahmen zunächst gewonnen und sodann nachhaltig gestärkt werden. Nicht die Reduzierung des Datenschutzniveaus oder gar die Absenkung datenschutzrechtlicher Anforderungen durch legislative Maßnahmen können daher als Faktoren für eine erfolgreiche Digitalisierung herangezogen werden, sondern im Gegenteil eine frühzeitige, dauerhafte und konsequente Berücksichtigung datenschutzrechtlicher Belange durch die Verantwortlichen.

Datenschutz ist somit nicht Hindernis, sondern ein wesentlicher Erfolgsfaktor für die Digitalisierung im Saarland.

In diesem Sinne sollen die nachfolgenden Punkte Vorschläge für ein legislatives wie auch administratives Tätigwerden des neuen Landtags und der neuen Landesregierung aufzeigen.

Saarbrücken, im April 2022

1. Das Saarländische Datenschutzgesetz evaluieren

Am 25. Mai 2018 ist das Saarländische Datenschutzgesetz (SDSG) in Kraft getreten. Die Neuregelung des Gesetzes war aus Anlass der ab dem gleichen Zeitpunkt anwendbaren Datenschutz-Grundverordnung (DSGVO) notwendig geworden, um die europarechtlichen obligatorischen Umsetzungspflichten auszufüllen und verbleibende fakultative Gestaltungsspielräume in Anspruch zu nehmen.

Nunmehr vier Jahre Aufsichtspraxis unter der DSGVO und dem SDSG zeigen jedoch, dass nicht nur die datenschutzrechtlichen Vorgaben des SDSG durch die verantwortlichen Stellen ernster genommen werden müssen, sondern auch, dass der regulatorische Rahmen des SDSG einer Nachschärfung und Präzisierung bedarf.

Dies gilt insbesondere für die Bestimmungen zum Anwendungsbereich des SDSG (§ 2 SDSG). Während die Vorschrift spezifische Stellen im Justizsystem entgegen europarechtlicher Vorgaben nicht erfasst, adressiert sie auf der anderen Seite privatrechtliche Unternehmen, an denen öffentliche Stellen des Saarlandes mit absoluter Mehrheit beteiligt sind, mit der Folge einer – im Verhältnis zu öffentlich-rechtlichen Unternehmen – wettbewerbsverzerrenden Überregulierung.

Dringender Reformbedarf besteht auch bezüglich des gerichtlichen Rechtsschutzes gegen Entscheidungen der Aufsichtsbehörde. Die derzeitige Regelung in § 26 SDSG bildet die unterschiedlichen Ausgangssituationen nur unzureichend ab und verkürzt so den Rechtsschutz für alle Beteiligten. Im Rahmen einer Neuregelung regen wir die Einführung einer Feststellungsklagemöglichkeit nach dem Vorbild Hessens[1] an, um eine Überprüfung der Rechtmäßigkeit aufsichtsbehördlicher Entscheidungen herbeiführen zu können.

In der Vergangenheit ist die gesetzlich vorgesehene Beteiligung der Aufsichtsbehörde bei der Einführung neuer IT-Verfahren oft zu kurz gekommen. Gerade mit Blick auf die in Umsetzung des Onlinezugangsgesetzes anstehende Digitalisierungswelle in den kommenden Jahren ist eine frühzeitige Einbindung unserer Behörde zwingend erforderlich, um bereits im Vorfeld der konkreten Ausgestaltung solcher Verfahren den Schutz personenbezogener Daten hinreichend zu gewährleisten.

Um unsere Beratungsaufgaben als Datenschutz-Aufsichtsbehörde effektiv wahrnehmen zu können, den aus datenschutzrechtlicher Sicht notwendigen konstruktiven Input bei der Einführung neuer IT-Verfahren geben zu können und die Behörden des

[1] Vgl. § 19 Abs. 5 Hessisches Datenschutz- und Informationsfreiheitsgesetz.

Saarlandes bei der Erarbeitung von Datenschutzkonzepten und bei der Erstellung von Datenschutz-Folgenabschätzungen bestmöglich unterstützen zu können, bedarf es zudem einer sachgerechten personellen Aufstockung des Unabhängigen Datenschutzzentrums Saarland. Mit der derzeit gegebenen Personalausstattung lassen sich zeitliche Vorgaben im Rahmen von Digitalisierungsprojekten nur schwerlich in Einklang bringen.

Zur Erhöhung der Rechts-, Verfahrens-, Informations- und Datensicherheit beim Betrieb von Verfahren zur Verarbeitung personenbezogener Daten sollten zudem Möglichkeiten der Zertifizierung behördlicher Verfahren in Erwägung gezogen werden. Denn durch eine gezielte Gestaltung der Systeme und Verfahren können die Ziele des Datenschutzrechts bereits durch die technischen Abläufe selbst gewährleistet werden. Gerade im Zusammenhang mit der Forderung nach einem inklusiven E-Government, das zur gleichberechtigten, umfassenden und vor allem selbstbestimmten Teilhabe aller Bürgerinnen und Bürger befähigen soll, können datenschutzrechtliche Zertifizierungen so für Transparenz und das notwendige Vertrauen in digitale Verwaltungsleistungen sorgen.

Der im Wahlprogramm der jetzigen Landesregierung angekündigte Wandel der Digitalpolitik und die avisierte Effektivierung des Digitalisierungsprozesses durch Bündelung von Knowhow und Ressourcen, sollten daher auch Überlegungen zur Schaffung einer saarländischen Zertifizierungsstelle beinhalten.

Hierzu sollten die durch den europäischen Gesetzgeber eingeräumten Möglichkeiten, im Einklang mit Art. 42 Abs. 5 DSGVO datenschutzrechtliche Zertifizierungen durch die Datenschutz-Aufsichtsbehörde zu erteilen, ausgeschöpft werden. Das Unabhängige Datenschutzzentrum Saarland könnte so in Zusammenarbeit mit anderen relevanten Stellen eine Zertifizierung von Verfahren zur Verarbeitung personenbezogener Daten anbieten. Ziel sollte es sein, die datenschutzrechtliche Zertifizierung zu einem Standard bei der Einführung neuer IT-Verfahren in der öffentlichen Verwaltung zu machen.

2. Mehr digitale Souveränität wagen

Die öffentliche Verwaltung ist in zunehmendem Maße von externen, privaten IT-Anbietern abhängig. Dies rührt vor allem daher, dass in der öffentlichen Verwaltung überwiegend Standard-Produkte von kommerziellen Software-Anbietern eingesetzt werden.[2] Bestehende Verträge und die marktbeherrschende Stellung dieser Unternehmen schränken den Handlungsspielraum bei Beschaffung, Entwicklung und Einsatz von Informations- und Kommunikationstechnologie ein. Dies kann ein Risiko für die Sicherheit, Selbstständigkeit und Selbstbestimmtheit der öffentlichen Verwaltung darstellen.

Neben unkontrollierbaren Kosten sowie eingeschränkter Flexibilität und Informationssicherheit führt vor allem die fehlende Transparenz, Kontrollierbarkeit und Intervenierbarkeit der Datenverarbeitung auch zu erheblichen rechtlichen Unsicherheiten bei der Verarbeitung personenbezogener Daten.

Um diesem Kontrollverlust entgegenzuwirken und die Abhängigkeit von externen, privaten IT-Anbietern zu reduzieren, bedarf es einer Diversifizierung der in der öffentlichen Verwaltung zum Einsatz kommenden Hard- und Software. Der konsequente Einsatz von quelloffener Software und offenen Standards sind tragende Säulen einer solchen Diversifizierungsstrategie. Seitens der Landesregierung bedarf es eines klaren Bekenntnisses zum Datenschutz sowohl für die aktuelle als auch für die künftige Gestaltung digitaler Verfahren.

Aus datenschutzrechtlicher Sicht sind hierbei insbesondere folgende Punkte zu beachten:[3]

- Der Betrieb bestehender, wie auch die Anschaffung neuer IT-Lösungen bedarf einer genauen Analyse der hiermit einhergehenden Verarbeitungsvorgänge und – daraus folgend – einer Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen sowie der Notwendigkeit und Verhältnismäßigkeit der Verarbeitung. Zertifizierungen können ein Baustein sein, um den Nachweis der Einhaltung datenschutzrechtlicher Vorgaben zu erbringen.
- Durch den Einsatz von Produkten, die auf offenen Standards basieren, wird die Verarbeitung personenbezogener Daten transparent und damit kontrollierbar. Offene Standards sind zudem geeignet, unerwünschte Lock-in-Effekte zu vermeiden und ermöglichen der öffentlichen Verwaltung so einen Wechsel, wenn der Dienstleister oder Anbieter nicht mehr in der Lage ist nachzuweisen, dass sein Produkt datenschutzrechtlichen Anforderungen genügt.

[2] Strategische Marktanalyse zur Reduzierung von Abhängigkeiten von einzelnen Software-Anbietern, PWC, 2019.
[3] Vgl. hierzu die Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) vom 22.09.2020: „Digitale Souveränität der öffentlichen Verwaltung herstellen – Personenbezogene Daten besser schützen", abrufbar unter: https://www.datenschutz.saarland.de.

- Die öffentliche Verwaltung sollte nur solche Produkte und Dienstleistungen beschaffen und nutzen, bei denen sie die Steuerungsmöglichkeiten über die Verarbeitung personenbezogener Daten behalten. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen muss elementarer Bestandteil von Dienstleistungen und Produkten sein, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen.

Vor diesem Hintergrund kritisch sehen wir die geplante oder sich schon in der Umsetzung befindliche Einführung großer Cloud-Produkte und -Dienstleistungen an der Universität des Saarlandes, an verschiedenen Schulen und mehreren Kommunen im Saarland. Derzeit ist nicht zu erkennen, wie diese Projekte mit obigen Rahmenbedingungen in Einklang gebracht werden können. Dies gilt in gleichem Maße für die in der Landesverwaltung verbreitete Nutzung verschiedener Social-Media-Plattformen für Zwecke der Öffentlichkeitsarbeit und zur externen Kommunikation mit Bürgerinnen und Bürgern. Vor allem die Speicherung von und der Zugriff auf Daten in den Geräten der Bürgerinnen und Bürger ohne wirksame Rechtsgrundlage und unzureichende Informationen machen diese Form der Datenverarbeitung datenschutzrechtlich angreifbar, was den Behörden als Nutzer dieser Angebote zuzurechnen ist.[4] Gerade zu den auch von zahlreichen öffentlichen Stellen betriebenen Facebook-Fanpages hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) jüngst mit Blick auf die in den vergangenen Jahren ergangene Rechtsprechung zu Facebook-Fanpages in einem Gutachten festgestellt, dass deren Betrieb weiterhin nicht datenschutzkonform möglich ist.[5] In der Folge hat die DSK die Vereinbarung getroffen, zunächst bei den Landes- und Bundesbehörden mit Blick auf deren Vorbildfunktion darauf hinzuwirken, dass die von ihnen betriebenen Fanpages deaktiviert werden, sofern sie als Verantwortliche die datenschutzrechtliche Konformität nicht nachweisen können.[6] Bestehende Angebote müssen daher dringend überprüft und durch datenschutzfreundliche Alternativen ersetzt werden.

Transparenzanforderungen sowie die Notwendigkeit die Kontrollierbarkeit und Intervenierbarkeit der Verarbeitung personenbezogener Daten sicherzustellen, gelten auch bei der Verarbeitung personenbezogener Daten mittels Systemen der Künstlichen Intelligenz (KI).[7] Daher begrüßen und unterstützen wir die Forderung im Wahlprogramm der jetzigen Landesregierung, sich für eine transparente und diskriminierungsfreie KI einsetzen zu wollen.

[4] Vgl. hierzu: EuGH, Urteil vom 05.06.2018, C-210/16; BVerwG, Urteil vom 11.09.2019, 6 C 15.18.
[5] Kurzgutachten der DSK zur datenschutzrechtlichen Konformität des Betriebs von Facebook-Fanpages.
[6] Vgl. den Beschluss der DSK zur Task Force Facebook-Fanpages vom 23.03.2022.
[7] Vgl. hierzu die Entschließung der DSK vom 03.04.2019: „Hambacher Erklärung zur Künstlichen Intelligenz – Sieben datenschutzrechtliche Anforderungen".

3. Die Grundlagen polizeilichen Handelns neu ordnen

Das hoheitliche Handeln der Polizei ist von rechtsstaatlichen Prinzipien geprägt. Dies umfasst, dass polizeiliches Handeln vorhersehbar und bestimmbar sein muss. Je tiefer der potenzielle Eingriff in die Grundrechte der Bürgerinnen und Bürger ist, den eine Ermächtigungsgrundlage zulässt, desto höher sind die Anforderungen an die Regelungsdichte der Vorschrift.

Dem wird das Saarländische Gesetz zur Verarbeitung personenbezogener Daten durch die Polizei (SPolDVG) nicht in vollem Umfang gerecht. Insofern teilen wir den Befund im Wahlprogramm der neuen Landesregierung, dass die derzeitige Regelung weder für die Polizeibeamtinnen und Polizeibeamten noch für betroffene Bürgerinnen und Bürger transparent und handhabbar ist.

Daher unterstützen wir die avisierte Neuordnung des Saarländischen Polizeigesetzes und des Saarländischen Gesetzes zur Verarbeitung personenbezogener Daten durch die Polizei. Dabei sollte ein besonderes Augenmerk daraufgelegt werden, dass bei heimlichen und verdeckten Ermittlungsmaßnahmen derzeit noch existierende Rechtschutzdefizite der betroffenen Personen angemessen auszugleichen sind.

Bei der Neuordnung der polizeilichen Datenverarbeitung sollten insbesondere folgende zentralen Punkte Berücksichtigung finden:

- Die Regelungen zur Datenverarbeitung von Vollzugs- und Ortspolizei sind trennscharf voneinander abzugrenzen. Vor dem Hintergrund, dass die nicht straftatenbezogene Gefahrenabwehr der Ortspolizeibehörden nicht in den Anwendungsbereich der Richtlinie (EU) 2016/280, sondern in den Anwendungsbereich der Verordnung (EU) 2016/679 fällt, gelten hier unterschiedliche europarechtliche Vorgaben.
- Die Befugnis zum Einsatz von Body-Cams in Wohnungen ist auf den Prüfstand zu stellen, da erhebliche Zweifel an der Verfassungsmäßigkeit der Regelung bestehen.
- Die Ausnahmen von der Benachrichtigungspflicht der betroffenen Personen im Falle von heimlichen und verdeckten Ermittlungsmaßnahmen sind an zwingende europarechtliche Vorgaben anzupassen.
- Die Befugnisse zum anlasslosen Datenabgleich von Störern im polizeirechtlichen Sinne sind zu streichen oder auf Fahndungsdateien zu begrenzen.
- Die Befugnisse zur Erhebung von Telekommunikationsdaten und Nutzungsdaten von Telemedien sowie zur Überwachung und Aufzeichnung der Telekommunikation bedürfen einer dringenden Anpassung an die Vorgaben des Bundesverfassungsgerichts.

Zunehmend kritisch sehen wir auch die ausufernde Praxis der Funkzellenabfragen. Während im Jahr 2020 noch 6.196 nicht-individualisierte Funkzellen-

abfragen durch die saarländische Polizei vorgenommen wurden[8], hat sich diese Zahl im Jahr 2021 auf 12.464 Abfragen mehr als verdoppelt[9]. Das entspricht zwischen einer und zwei (1,4) Funkzellenabfragen pro Stunde. Sogar verdreifacht hat sich die Anzahl der hiervon betroffenen Telekommunikationsanschlüsse. Mit 25.226.658 Anschlüssen ist statistisch jede Saarländerin und jeder Saarländer mehr als 25-mal pro Jahr Ziel einer solchen Funkzellenabfrage. Problematisch hieran ist vor allem, dass die betroffenen Bürgerinnen und Bürger bisher in keiner Weise darüber informiert werden, dass ihr Standort im Rahmen einer polizeilichen Maßnahme erfasst wurde. Folglich können sie die Maßnahme auch nicht gerichtlich überprüfen lassen. Um dieses Informations- und Rechtsschutzdefizit in Zukunft auszuräumen, regen wir an, nach dem Vorbild der Bundesländer Berlin und Baden-Württemberg die Einführung eines Funkzellen-Transparenz-Systems zu prüfen.

[8] Pressemitteilung des Ministeriums für Inneres, Bauen und Sport vom 31.12.2020.

[9] Pressemitteilung des Ministeriums für Inneres, Bauen und Sport vom 23.02.2022.

4. Datenschutz in der digitalen Bildung stärken

Ein wichtiges Vorhaben der neuen Landesregierung in der kommenden Legislaturperiode ist gerade auch die Digitalisierungsanstrengungen im Bildungsbereich voranzutreiben. Notwendige Voraussetzung für ein Gelingen der digitalen Transformation in den Schulen ist neben der erforderlichen technischen Ausstattung und deren Support zwingend aber auch die Einhaltung datenschutzrechtlicher Vorgaben.

Die seit 2018 anwendbare DSGVO bildet den regulatorischen Rahmen zum Schutz der personenbezogenen Daten der Schülerinnen und Schüler sowie der Lehrkräfte, allerdings sind die landesrechtlichen Datenschutzregelungen für den schulischen Bereich noch immer nicht an diesen europarechtlichen Rahmen angepasst worden. Einer umgehenden Anpassung aller schulrechtlich relevanten Vorschriften an die DSGVO sollte daher besondere Priorität eingeräumt werden, auch um die geplanten Digitalisierungsvorhaben im Bildungsbereich rechtssicher umsetzen zu können.

Neben dem originären Bildungs- und Erziehungsauftrag der Schulen, ergeben sich datenschutzrechtliche Bezüge aber auch im Rahmen schulinterner Verwaltungsaufgaben. Um datenschutzrechtliche Fragestellungen im Schulalltag zeitnah zu klären, die Einhaltung datenschutzrechtlicher Vorschriften in den Schulen zu überwachen und die jeweiligen Schulleitungen kompetent zu beraten, sind – ebenso wie in allen anderen Behörden – auch im schulischen Bereich behördliche Datenschutzbeauftragte zu benennen. Wenngleich nach Art. 37 Abs. 3 DSGVO mehrere öffentliche Stellen unter Beachtung ihrer Organisationsstruktur und Größe einen gemeinsamen Datenschutzbeauftragten bestellen können, ist es – wie bislang praktiziert – nicht ausreichend, für den gesamten Schulbereich des Saarlandes (Grundschulen, weiterführende Schulen, Berufsschulen) und zugleich für die Behörde des Ministeriums für Bildung und Kultur lediglich eine Person als behördliche Datenschutzbeauftragte sowie einen Stellvertreter zu benennen. Für die Schulen sind gesonderte behördliche Datenschutzbeauftragte zu bestellen, die diesen ortsnah und in ausreichendem Umfang zur Verfügung stehen, um bei datenschutzrechtlichen Fragestellungen und Projekten den Schulleitungen, den Schülerinnen und Schülern, den Lehrkräften und den Eltern beratend zur Seite stehen.

Zu begrüßen ist das Vorhaben der neuen Landesregierung, die Medienbildung als Lernbereich in der schulischen Bildung zu verankern. Die Kompetenz sich in einer mediengeprägten digitalen Welt selbstbestimmt und verantwortungsvoll als aufgeklärte und kompetente Nutzerinnen und Nutzer zu bewegen, ist essenziell für eine aktive Teilhabe an demokratischen und gesellschaftlichen Prozessen.

Dies beinhaltet als einen Baustein der Medienbildung einen datenschutzgerechten Umgang der Schülerinnen und Schüler sowohl mit ihren eigenen, als auch mit den Daten anderer. Bereits seit fast zehn Jahren führt das Unabhängige Datenschutzzentrum Saarland mit großem Erfolg Workshops zum sicheren Umgang von Schülerinnen und Schülern mit digitalen Medien an weiterführenden Schulen und seit

2017 auch an Grundschulen durch. Bisher wurden mehr als 20.000 Schülerinnen und Schüler zum datenschutzgerechten Umgang mit personenbezogenen Daten sensibilisiert. Dem großen Interesse an unserem Angebot möchten wir gerne weiterhin gerecht werden und auch dem in der Stellungnahme zu unserem 27. Tätigkeitsbericht geäußerten Wunsch des Ministeriums für Bildung und Kultur nach einer Ausweitung des Angebots auf die beruflichen Schulen nachkommen. Um weiterhin einen Beitrag zur Medienkompetenz der Schülerinnen und Schüler leisten zu können, bedarf es weiterer Unterstützung durch die neue Landesregierung.

5. Staatliches Handeln transparenter machen

Transparenz staatlichen Handelns und der Zugang zu Informationen sind essenziell für eine moderne demokratische Gesellschaft.

Daher ist das Vorhaben der Landesregierung zu unterstützen, durch ein verpflichtendes Lobbyregister bereits im Rahmen des politischen Entscheidungsprozesses Entscheidungsvorgänge transparent und nachvollziehbar zu machen.[10]

Gleichfalls zu begrüßen ist die Absicht der Landesregierung, digitale Daten als Ressource für Wissenschaft und Forschung, aber auch für die Wirtschaft zur Verfügung zu stellen. Der Zugang zu frei verfügbaren Datenbeständen der öffentlichen Hand und die Möglichkeit diese nutzen zu können, sind ein wichtiger Beitrag zur Weiterentwicklung einer Wissensgesellschaft.

Die Bereitstellung von Verwaltungsdaten sollte daher – anders als dies § 17 des saarländischen E-Government-Gesetzes (E-GovG) vorsieht – für die öffentlichen Stellen verbindlich werden. Neben der Bereitstellung von Rohdaten in standardisierten, offenen und maschinenlesbaren Formaten gebietet die Transparenz öffentlichen Handelns auch, zusammenhängende, aus sich heraus nachvollziehbare Unterlagen, wie bspw. Verträge, Studien und Pläne, zur Verfügung zu stellen.

Die proaktive Veröffentlichung von Informationen fördert nicht nur die Entwicklungen in Wissenschaft, Forschung und Wirtschaft, sie ist darüber hinaus ein wesentliches Element zur Stärkung des Vertrauens der Bürgerinnen und Bürger in staatliche Entscheidungen. Daher ist auch das seit 2006 nahezu unverändert gebliebene und den aktuellen Anforderungen an ein transparentes staatliches Handeln nicht mehr genügende saarländische Informationsfreiheitsgesetz (SIFG), das bislang nur einen individuellen Anspruch auf Informationszugang gewährt, weiterzuentwickeln.

Bei der Weiterentwicklung des Informationsfreiheitsrechts sollten insbesondere folgende zentrale Punkte Berücksichtigung finden:

- Die bestehenden Informationszugangsansprüche aus dem Saarländischen Informationsfreiheits-, dem Umweltinformationsfreiheits- und dem E-Government-Gesetz sollten in einem Transparenzgesetz kodifiziert werden, das den individuellen, antragsgebundenen Informationszugangsanspruch mit der Verpflichtung der öffentlichen Stellen, bestimmte Informationen proaktiv und

[10] Vgl. hierzu die Entschließung der Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) vom 12.06.2019: „Transparenz im Rahmen politischer Entscheidungsprozesse – Verpflichtendes Lobbyregister einführen".

antragsunabhängig auf Informationsplattformen zu veröffentlichen, verbindet.[11]

- Der oder dem Landesbeauftragten für Informationsfreiheit ist die Zuständigkeit auch für die Einhaltung und Kontrolle des Umweltinformationsrechts zu übertragen.[12]
- Es sollten landeseigene gesetzliche Regelungen geschaffen werden, in welchen die bestehenden Ausschlussgründe, die einem Informationszugang entgegenstehen können, reduziert und harmonisiert werden.
- Die oder der Landesbeauftragte sollte eine Anordnungsbefugnis bekommen, um Rechtsverstöße gegen das Informationsfreiheitsrecht beseitigen zu können.
- In das Gesetz sollte eine Regelung aufgenommen werden, nach der Informationen, die auf individuellen Antrag hin zugänglich gemacht wurden, auch im Informationsregister veröffentlicht werden können (Access for one = access for all), wenn ein öffentliches Interesse an der Veröffentlichung besteht.
- In dem Gesetz sollte der Grundsatz der „Informationsfreiheit by Design", wonach die Anforderungen an die Informationsfreiheit von Anfang an in die Gestaltung der IT-Systeme und organisatorischen Prozesse einzubeziehen sind, aufgegriffen werden.[13]
- Daneben sollte die Benennung eines behördlichen Informationsfreiheitsbeauftragten verbindlich vorgesehen werden.[14]

Das Land sollte sich mit seinem Transparenzregister am Bund-Länder-Online Portal GovData beteiligen. Ziel dieses Portals ist es, einen einheitlichen zentralen Zugang zu offenen Verwaltungsdaten aus Bund, Ländern und Kommunen an einer zentralen Stelle auffindbar und so einfacher nutzbar zu machen. Bislang sind mit Ausnahme des Saarlandes und Sachsen-Anhalts alle Bundesländer diesem Portal beigetreten.

[11] Vgl. hierzu die Entschließung der IFK vom 02.06.2021: „Forderungen für die neue Legislaturperiode des Bundes: Ein Transparenzgesetz mit Vorbildfunktion schaffen!" sowie die Grundsatzpositionen der Landesbeauftragten für die Informationsfreiheit vom 06.10.2017.
[12] Vgl. hierzu die Entschließung der IFK vom 3. November 2021: Umweltinformationen: Beratungs- und Kontrollkompetenz auch auf Landesbeauftragte für Informationsfreiheit übertragen!
[13] Vgl. hierzu das Positionspapier der IFK vom 12. Juni 2019: Informationszugang in den Behörden erleichtern durch „Informationsfreiheit by Design".
[14] Vgl. hierzu die Entschließung der IFK vom 2. Juni 2021: Mehr Transparenz durch behördliche Informationsfreiheits-beauftragte!