KANTON AARGAU

DEPARTEMENT
FINANZEN UND RESSOURCEN

EANHÖRUNG: IHRE STELLUNGNAHME

Dieses Dokument zeigt Ihnen Ihre notierten Angaben aus dem Online-Fragebogen. Es wird automatisch generiert.

Details	
Name der eAnhörung	Gesetz über die Informationssicherheit (InfoSiG)
PDF-Dokument generiert am	08.07.2024 16:39
Stellungnahme von:	FDP.Die Liberalen Aargau

FRAGEBOGEN ZUR ANHÖRUNG

Gesetz über die Informationssicherheit (InfoSiG)

Anhörungsdauer
Die Anhörung dauert vom 8. Mai 2024 bis 16. August 2024.

Inhalt
Mit der Vorlage "Gesetz über die Informationssicherheit" wird eine gesetzliche Grundlage zum Zweck der sicheren Bearbeitung von Informationen sowie des sicheren Einsatzes der Informatikmittel durch die kantonalen Behörden geschaffen. Nebst der Festlegung der Zuständigkeiten können die zu treffenden Massnahmen als eigentlicher Kern der Gesetzgebung betrachtet werden. Sie basieren auf den branchenüblichen internationalen Standards (ISO 27001, NIST). In organisatorischer Hinsicht sollen die heutigen Strukturen gestärkt werden, namentlich soll der CISO beziehungsweise die Fachstelle für Informationssicherheit mit einem departements- und behördenübergreifenden Weisungs- und Durchgriffsrecht ausgestattet werden. Zudem soll eine kantonale Cyber-Organisation gestützt auf die Empfehlungen des Sicherheitsverbunds Schweiz geschaffen werden, welche für Vernetzung, Informationsaustausch und Sensibilisierung auch ausserhalb der Verwaltungsgrenzen (Bevölkerung, Wirtschaft, kritische Infrastrukturen, Gemeinden, andere öffentlich-rechtliche Trägerschaften) sorgen soll.

Die vollständigen Unterlagen zur Vorlage und zur Anhörung sind zu finden unter www.ag.ch/anhörungen.

Auskunftsperson
Bei inhaltlichen Fragen zur Anhörung können Sie sich an die folgende Stelle wenden:

KANTON AARGAU
Departement Finanzen und Ressourcen
Generalsekretariat
Ivano Larcher, Leiter Rechtsdienst
062 835 24 23
ivano.larcher@ag.ch

Bitte beachten Sie: Diese Anhörung wird als eAnhörung durchgeführt. Ihre Stellungnahme reichen Sie elektronisch über das "Smart Service Portal" (www.ag.ch) ein. Wenn dies aus zwingenden Gründen nicht möglich ist, stellen Sie Ihre Stellungnahme postalisch oder per E-Mail zu:

Departement Finanzen und Ressourcen
Generalsekretariat, Rechtsdienst
Tellistrasse 67
5001 Aarau
E-Mail: ivano.larcher@ag.ch

Angaben zu Ihrer Stellungnahme

Sie nehmen an dieser Anhörung im Namen einer Organisation teil.

Wenn Ihnen unten bereits Daten angezeigt werden, sind Ihre Angaben bereits hinterlegt. Sie können die Daten bei Bedarf überschreiben und so die Angaben korrigieren. Wichtig: Wenn Sie bspw. die E-Mail-Adresse ändern, wird fortan die neue von Ihnen notierte E-Mail-Adresse für den E-Mail-Versand für eine Anhörungseinladung verwendet!

Wenn Ihnen noch keine Angaben angezeigt werden, geben Sie bitte unten Ihre entsprechenden Kontaktdaten ein. Die notierten Angaben werden hinterlegt und Ihnen in weiteren Teilnahmen an eAnhörungen automatisch angezeigt.

Adressblock - Ihre Angaben

Name der Organisation	FDP.Die Liberalen Aargau
E-Mail	info@fdp-ag.ch

Zuständige Person bei inhaltlichen Rückfragen
Bitte notieren

Vorname	Bernhard
Nachname	Scholl
E-Mail	bernhard.scholl@grossrat.ag.ch

Fragen zur Anhörungsvorlage

Frage 1 – Normierung der Informationssicherheit in einem Spezialgesetz

Die Aufgaben der Informationssicherheit werden bereits heute im Rahmen der zur Verfügung stehenden Ressourcen wahrgenommen. Die entsprechenden Vorgaben finden sich jedoch weitgehend in verwaltungsinternen Dokumenten. Es handelt sich dabei vorwiegend um Regelungen, die sich an anerkannten Normen und Best Practices orientieren, aber nicht um gesetzliche Grundlagen. Eine verwaltungsinterne Regelung kommt nicht in Betracht, weil der Kanton Informationen der Bevölkerung und von Unternehmen, aber auch von anderen öffentlich-rechtlichen Trägerschaften sowie anderer Kantone und des Bundes bearbeitet, folglich eine erhebliche Aussenwirkung besteht. Aber auch aufgrund der Bedeutung, die der Informationssicherheit in der Zwischenzeit und angesichts der fortschreitenden digitalen Entwicklung in der Gesellschaft zukommt, sowie der damit verbundenen Risiken für die öffentliche Sicherheit, ist es zentral, dass die Informationssicherheit als öffentliche Aufgabe und deren Grundsätze gesetzlich normiert werden. Die Lücke in den rechtlichen Grundlagen soll mittels eines einheitlichen Gesetzes geschlossen werden.

Siehe Kapitel 5.1 des Anhörungsberichts.

Sind Sie damit einverstanden, dass für die Informationssicherheit ein Spezialgesetz geschaffen wird?

Bitte wählen Sie eine Antwort aus:

- (●) völlig einverstanden
- ( ) eher einverstanden
- ( ) eher dagegen
- ( ) völlig dagegen
- ( ) keine Angabe

Bemerkungen zur Frage 1

Frage 2 – Gemeinden und andere Träger öffentlicher Aufgaben (§ 2 Abs. 2 und 3)

Die entsprechenden Vorschriften des neuen Gesetzes sollen – in Anlehnung an die Regelung des Bundes im Verhältnis zu den Kantonen – für Gemeinden und andere Träger öffentlicher Aufgaben nur zum Tragen kommen, wenn sie klassifizierte Informationen des Kantons bearbeiten (Abs. 2 lit. a) oder auf Informatikmittel des Kantons zugreifen (Abs. 2 lit. b). In Berücksichtigung des Subsidiaritätsprinzips kommen sie aber nicht zur Anwendung, wenn die Gemeinden und anderen Träger öffentlicher Aufgaben bereits mit einer eigenen, mit derjenigen des Kantons vergleichbaren Informationssicherheit ausgestattet sind (Abs. 3). Dies ist der Fall, wenn der IKT-Minimalstandard des Bundes eingehalten wird. Dieser ist ein vom Bund als Empfehlung herausgegebener Branchenstandard, der sich zwar insbesondere an die Betreiber von kritischen Infrastrukturen richtet, aber in der Zwischenzeit auch für jedes Unternehmen und auch für die öffentliche Hand auf allen Ebenen zur eigentlichen Richtschnur und zum gemeinsamen Nenner in Bezug auf das

Sicherheitsniveau geworden ist. Aktuell ist der IKT-Minimalstandard 2023 (Version Mai 2023, mit Update NIST SP 800-53 Rev. 5 und ISO 27001:2022), der unter anderem auf die bewährten internationalen Standards NIST und ISO 27001 abstellt.

Siehe § 2 des Gesetzesentwurfs und die Ausführungen in Kapitel 7.2.2 des Anhörungsberichts.

Sind Sie damit einverstanden, dass die entsprechenden Bestimmungen des Informationssicherheitsgesetzes auf Gemeinden und andere Träger öffentlicher Aufgaben Anwendung finden, wenn sie klassifizierte Informationen des Kantons bearbeiten und auf Informatikmittel des Kantons zugreifen beziehungsweise dass die Bestimmungen keine Anwendung finden, wenn die Gemeinden und anderen Träger öffentlicher Aufgaben den IKT-Mindeststandard des Bundes gewährleisten?

Bitte wählen Sie eine Antwort aus:

- ○ völlig einverstanden
- ◉ eher einverstanden
- ○ eher dagegen
- ○ völlig dagegen
- ○ keine Angabe

Bemerkungen zur Frage 2

Die FDP ist einverstanden mit dem zu Grund gelegten Konzept, das hier angewendet werden soll. Sowohl der Geltungsbereich als auch die unter den Wirkungskreis des Gesetzes fallenden Objekte verlangen nach Klärung. Es fehlt eine Definition, was "Informationen des Kantons" sind und was nicht.
Es wird empfohlen, eine Detaillierung vorzunehmen. Das Gesetz sollte nur für Informationen/Daten anwendbar sein, bei denen der Kanton gemäss Definition der Datenschutzgesetze ein "Verantwortlicher" ist.
Zu definieren ist zudem, inwiefern das Gesetz die Träger von öffentlichen Aufgaben zutrifft, welche privatrechtlich sind. Beispielsweise erfüllen Heime einen öffentlichen Auftrag, welcher dem Kanton obliegen würde. Z. B. sind Alters- und Pflegeheime gemäss der Definition der Datenschutzgesetze als "Verantwortlicher" tätig, entsprechend handelt es sich nicht um klassifizierte Daten/Informationen des Kantons, da der Kanton nicht Verantwortlicher für die Datenbearbeitung ist.

Frage 3 – Führungsverantwortung (§ 5)

Informationssicherheit gehört zum Risikomanagement eines jeden Gemeinwesens und eines jeden Unternehmens und muss darum von den obersten Behörden verantwortet werden. Die Behörden gemäss Kapitel 5 der Kantonsverfassung (Grosser Rat, Regierungsrat, Gerichte), die für ihre Zwecke Informationen bearbeiten oder bearbeiten lassen (Abs. 1), sollen für die Informationssicherheit im Kanton verantwortlich sein. Das Gesetz hält die Aufgaben der Behörden verbindlich fest und stellt so sicher, dass diese in der Verwaltungshierarchie zuoberst angesetzt sind. Eine Delegation dieser Aufgaben ist nicht möglich. Bei einer Bearbeitung im Auftrag verbleibt die oberste Führungsverantwortung bei der beauftragenden Behörde.

Siehe § 5 des Gesetzesentwurfs und die Ausführungen in Kapitel 7.3.1.1 des Anhörungsberichts.

Sind Sie damit einverstanden, dass die oberste Führungsverantwortung für die Informationssicherheit bei den Behörden (Grosser Rat, Regierungsrat und Gerichte) festgelegt wird?

Bitte wählen Sie eine Antwort aus:

- (●) völlig einverstanden
- ( ) eher einverstanden
- ( ) eher dagegen
- ( ) völlig dagegen
- ( ) keine Angabe

Bemerkungen zur Frage 3

Frage 4 – Allgemeine Massnahmen sowie technische und organisatorische Massnahmen (Kapitel 2.2 und 3, §§ 6–24)

Die in den Kapiteln 2.2 und 3 des Gesetzesentwurfs vorgesehenen Massnahmen basieren auf den branchenüblichen internationalen Standards wie ISO 27001 und NIST). Diese haben sich in der Praxis bewährt und werden von Unternehmen der Privatwirtschaft und von kritischen Infrastrukturen angewendet.

Siehe Ausführungen zu den §§ 6–24.

Sind Sie einverstanden, die Regelung der Massnahmen an die branchenüblichen internationalen Standards anzulehnen?

Bitte wählen Sie eine Antwort aus:

- ( ) völlig einverstanden
- (●) eher einverstanden
- ( ) eher dagegen
- ( ) völlig dagegen
- ( ) keine Angabe

Bemerkungen zur Frage 4

Der grosse Aufwand und die Kosten müssen sich bei der Zertifizierung gemäss ISO 27001 in Betracht bezogen werden, und sollten nur vorgeschrieben werden, wenn die IT-Sicherheit Vorrang hat.

Frage 5 – Personensicherheitsprüfung (PSP); Personenkreis und Ausnahmen (§§ 19 Abs. 1 und 2)

Die vorgeschlagene Lösung legt den für eine PSP in Betracht kommenden Personenkreis (Abs. 1) fest:

a. *Angestellte sowie Beamtinnen und Beamten vor Abschluss des Anstellungsverhältnisses bzw. vor der Wahl oder während der Dauer des Anstellungs- bzw. des Beamtenverhältnisses,*

b. *Personen, die in ein Amt oder als Mitglied eines kantonalen Gremiums gewählt werden sollen,*

c. *Private vor Beginn oder im Rahmen der ihnen übertragenen Aufgaben oder des ihnen vergebenen öffentlichen Auftrags.*

Davon ausgenommen sollen die Mitglieder des Grossen Rats und des Regierungsrats sowie die Richterinnen und Richter sein. Auch der Bund nimmt die Legislativ- und Exekutivmitglieder sowie die Mitglieder des Bundesgerichts aus. Eine Ausnahme rechtfertigt sich, weil Politikerinnen und Politiker im Brennpunkt der Öffentlichkeit stehen. Deren Leben und Wirken wird von den Medien durchleuchtet, sodass sich die Wählerinnen und Wähler ein genaues Bild von den Kandidierenden machen können. Bei den Mitgliedern der Justiz rechtfertigt sich eine Ausnahme aufgrund deren institutioneller Stellung und folglich aus Gleichbehandlungsgründen zu den anderen Behörden. Dazu kommt, dass die überwiegende Mehrheit der Informationen, die bei den Gerichten im Rahmen ihrer Aufgabenerfüllung bearbeitet werden, schützenswerte Personendaten und folglich nicht klassifizierte Daten sind. Der Schutz dieser Informationen wird durch das Amtsgeheimnis, das Datenschutzgesetz sowie generell in den Prozessgesetzen geregelt. Das legitime öffentliche Interesse nach vertrauenswürdigen und integren Personen in der Justiz ist ausreichend durch die geltenden Bestimmungen im GOG abgedeckt.

Siehe § 19 des Gesetzesentwurfs und die Ausführungen in Kapitel 7.4.4.2.2 des Anhörungsberichts.

Sind Sie mit dem vorgeschlagenen Personenkreis bezüglich Durchführung der PSP einverstanden?

Bitte wählen Sie eine Antwort aus:

- (●) völlig einverstanden
- ( ) eher einverstanden
- ( ) eher dagegen
- ( ) völlig dagegen
- ( ) keine Angabe

Bemerkungen zur Frage 5

Frage 6 – Personensicherheitsprüfung (PSP); Zentrale Fachstelle für PSP (§ 20)

Für die Durchführung der PSP ist eine zentrale Fachstelle zu bezeichnen. Es ist wichtig, dass die Stelle, welche die PSP durchführt, das Risiko für die Informationssicherheit möglichst objektiv, mithin gestützt auf die erhobenen Daten sowie nach dem Stand der Wissenschaft und Rechtsprechung beurteilen können muss. Die Fachstelle PSP muss demzufolge in ihrer Beurteilung unabhängig, weisungsungebunden sein. Durch eine zentrale Fachstelle kann dieses Ziel viel eher erreicht werden als durch eine dezentrale Lösung. Die Kompetenzstellenlösung führt zudem auch zu einer Bündelung von Know-how und trägt zu einer einheitlichen Praxis bei. Bereits heute werden PSP zentral durch Spezialistinnen und Spezialisten der Kantonspolizei durchgeführt. Dazu kommt, dass ein Zugriff gemäss § 21 Abs. 1 lit. c und d ohnehin nur den Polizeikräften zusteht. Da auf die Möglichkeit des Zugriffs auf die entsprechenden Quellen nicht verzichtet werden sollte, kommt einzig die Kantonspolizei als zentrale Fachstelle für PSP ernsthaft in Betracht. Aus diesem Grund soll deren Zuständigkeit gesetzlich festgehalten werden (Abs. 1).

Siehe § 20 des Gesetzesentwurfs und die Ausführungen in Kapitel 7.4.4.2.3 des Anhörungsberichts.

Sind Sie einverstanden, dass die zentrale Fachstelle für PSP gesetzlich bei der Kantonspolizei verortet wird und dafür entsprechende personelle Ressourcen (aus heutiger Sicht mindestens eine Vollzeitstelle) geschaffen werden?

Bitte wählen Sie eine Antwort aus:

- ○ völlig einverstanden
- ○ eher einverstanden
- ◉ eher dagegen
- ○ völlig dagegen
- ○ keine Angabe

Bemerkungen zur Frage 6

Die FDP ist mit der Zuständigkeit der Kantonspolizei einverstanden. Die Aufgaben sollten jedoch soweit wie möglich mit den bestehenden Ressourcen erfüllt werden.

Frage 7 – Sicherheitsspezifische Eignungsprüfung von Unternehmen; Befähigungsnachweis (§ 24)

Die Gesetzesvorlage sieht neu eine gesetzliche Verpflichtung zur spezifischen Eignungsprüfung bei sicherheitsrelevanten Vergaben öffentlicher Aufträge aber auch bei der Übertragung von öffentlichen Aufgaben an Private vor. Das heisst, dass solche Vergaben nur an Unternehmen erfolgen dürfen, die sich als befähigt erweisen, die Sicherheitsinteressen des Kantons zu wahren (Abs. 1). In diesen Fällen muss die Informationssicherheit zwingend berücksichtigt werden und darf nicht dem Ermessen der Vergabestellen anheimgestellt bleiben.
Die erforderlichen Daten werden im Wesentlichen beim Betrieb selbst mit dessen Einverständnis erhoben. So sollen die Unternehmen zur Beurteilung des Risikos durch gezielte Abfrage, welche die Eigenheiten der spezifischen Vergabe beziehungsweise der Übertragung der öffentlichen Aufgabe berücksichtigt, aufgefordert werden Daten zu liefern, die für die Beurteilung ihrer Eignung in

sicherheitsbezogener Hinsicht notwendig sind (Abs. 2).

Siehe § 24 des Gesetzesentwurfs und die Ausführungen in Kapitel 7.4.5.1 des Anhörungsberichts.

Sind Sie einverstanden, dass im Rahmen von sicherheitsrelevanten Vergabeverfahren oder Auslagerungen einer öffentlichen Aufgabe eine gesetzliche Verpflichtung zur spezifischen Eignungsprüfung der potenziellen Vertragspartner statuiert wird?

Bitte wählen Sie eine Antwort aus:

- ○ völlig einverstanden
- ○ eher einverstanden
- ◉ eher dagegen
- ○ völlig dagegen
- ○ keine Angabe

Bemerkungen zur Frage 7

Frage 8 – Verwaltungsinterne Organisation; Fachstelle für Informationssicherheit (§ 25)

Die Fachstelle für Informationssicherheit soll departements- und behördenübergreifend tätig sein und über entsprechende Weisungs- und Durchsetzungsbefugnisse verfügen. Die Gefährdung der öffentlichen Interessen, die durch eine Verletzung der Informationssicherheit einher gehen kann, rechtfertigt es, dass die Fachstelle gesetzlich bestimmte Kompetenzen erhält wie beispielsweise die autonome Durchführung von Überprüfungen aber auch die Möglichkeit der Beantragung beziehungsweise des Ergreifens von Massnahmen, wenn Verletzungen der Informationssicherheitsvorgaben (Gesetz, Verordnung, Weisungen, Standards) festgestellt werden sollten. Eine Fachstelle ohne Durchsetzungsmöglichkeit ist keine wirksame Option im Hinblick auf eine möglichst risikofreie Informationssicherheit und besonders im Kampf gegen Cyberbedrohungen.

Siehe § 25 des Gesetzesentwurfs und die Ausführungen in Kapitel 7.5.1.1 des Anhörungsberichts.

Sind Sie damit einverstanden, dass die Fachstelle für Informationssicherheit departements- und behördenübergreifend tätig sein und über entsprechende Weisungs- und Durchsetzungsbefugnisse verfügen soll?

Bitte wählen Sie eine Antwort aus:

- ○ völlig einverstanden
- ◉ eher einverstanden
- ○ eher dagegen
- ○ völlig dagegen

- ○ keine Angabe

Bemerkungen zur Frage 8

Die FDP ist einverstanden, dass die Fachstelle für Informationssicherheit departements- und behördenübergreifend tätig sein und über entsprechende Weisungs- und Durchsetzungsbefugnisse verfügen kann. Davon auszunehmen sind die Gemeinden. Die Gemeinden sind autonom. Für die Gemeinden gelten die Bestimmungen gemäss § 2. Die behördenübergreifende Weisungsbefugnis ist für die Gemeinden in ein Beratungsauftrag ohne Weisungsbefugnis anzupassen.

Frage 9 – Kantonale Cyber-Organisation (§§ 26–29)

Der Gesetzesentwurf schlägt die Schaffung einer verwaltungsübergreifenden Cyber-Organisation vor, die sich im Wesentlichen auf die Empfehlungen des Schweizerischen Sicherheitsverbunds (SVS) stützt. Die Organisation soll aus einem Cyber-Ausschuss, einer Cyber-Koordinationsstelle und einer Kerngruppe Cyber bestehen. Die neue Organisation soll in erster Linie mit der Koordination und dem Informationsaustausch zwischen den staatlichen und privaten Akteuren sowie der Stärkung der Widerstandsfähigkeit in Verwaltung, Wirtschaft und Bevölkerung betraut werden (Abs. 1).

Siehe §§ 26–29 des Gesetzesentwurfs und die Ausführungen in Kapitel 7.5.2 des Anhörungsberichts.

Sind Sie mit der Schaffung einer kantonalen Cyber-Organisation zum Zwecke der Koordination und des Informationsaustausches zwischen den staatlichen und privaten Akteuren sowie der Stärkung der Widerstandsfähigkeit in Verwaltung, Wirtschaft und Bevölkerung und der damit einhergehenden Schaffung einer Stelle einverstanden?

Bitte wählen Sie eine Antwort aus:

- ○ völlig einverstanden
- ◉ eher einverstanden
- ○ eher dagegen
- ○ völlig dagegen
- ○ keine Angabe

Bemerkungen zur Frage 9

Die FDP ist mit dem Vorschlag der Schaffung einer kantonalen Cyber-Organisation einverstanden. Aus der Botschaft ist jedoch der finanzielle Aufwand nicht ersichtlich. Die Gemeinden sind einzubeziehen bei Auswirkungen auf die Gemeinden.

Frage 10 – weitere Bemerkungen

Haben Sie weitere Bemerkungen zur Anhörungsvorlage?

Die Finanzkontrolle führt Revisionen im IT-Bereich durch. Es sollte geprüft werden, ob es Bestimmungen braucht für eine Abgrenzung der Tätigkeiten der Fachstelle und der Finanzkontrolle.

Bemerkungen zur Frage 10

Auf der nachfolgenden Seite erhalten Sie Gelegenheit, Schlussbemerkungen zur vorliegenden Anhörung zu notieren.
Bitte beachten Sie: Ihre Stellungnahme wird erst eingereicht, wenn Sie anschliessend auf den Button "Antworten abschicken" klicken! Vorher wird Ihre Stellungnahme nicht übermittelt.

Schlussbemerkungen

Die FDP unterstützt den Aufbau einer kantonalen Cyberorganisation. Unklar bleiben gemäss Botschaft die finanziellen Auswirkungen insgesamt und wieviel Personal total neu eingestellt werden soll. Beim finanziellen Aufwand muss ein klar positives und effizientes Nutzen-Kosten Verhältnis eingestellt werden. Unter Nutzen sind die Sicherheit und allfällig vermiedene, vermeidbare Risiken zu verstehen. Das benötigte Personal für die Fachstelle und die Cyberorganisation soll, wo immer möglich aus dem bereits bestehenden Personal rekrutiert werden.