KANTON AARGAU

REGIERUNGSRAT

23. August 2017

BOTSCHAFT AN DEN GROSSEN RAT **17.188**

Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (IDAG); Änderung

Einführungsgesetz zur Schweizerischen Strafprozessordnung (EG StPO); Änderung

Gesetz über die Gewährleistung der öffentlichen Sicherheit (Polizeigesetz, PolG); Änderung

Einführungsgesetz zum Bundesgesetz über die obligatorische Arbeitslosenversicherung und die Insolvenzentschädigung sowie zum Bundesgesetz über die Arbeitsvermittlung und den Personalverleih (EG AVIG/AVG) Änderung

Bericht und Entwurf zur 1. Beratung

Inhaltsverzeichnis

Zusammenfassung **3**

1. Ausgangslage **4**

2. Handlungsbedarf **5**
2.1 Richtlinie (EU) 2016/680 5
2.2 Datenschutzkonvention SEV 108 6
2.3 Verordnung (EU) 2016/679 8
2.4 Aarhus-Konvention (AK) 8
2.5 Europäische Menschenrechtskonvention 9
2.6 Fazit 9

3. Umsetzung **9**
3.1 Bund 9
3.2 Kantonale Umsetzung 9

4. Verhältnis zur mittel- und langfristigen Planung **11**

5. Auswertung des Anhörungsverfahrens **11**
5.1 Bemerkungen zu den Änderungen im IDAG *(Antworten des Regierungsrats sind kursiv)* 12
5.1.1 Allgemeine Bemerkungen 12
5.1.2 Verzicht auf Schutz der juristischen Personen 13
5.1.3 Erhöhung der Transparenz von Datenbearbeitungen 14
5.1.4 Stärkung der Rechte der Betroffenen 14
5.1.5 Stärkung der Position der beauftragten Person für Öffentlichkeit und Datenschutz 15
5.2 Bemerkungen zum EG StPO und zum PolG 15
5.3 Bemerkungen zum EG AVIG/AVG 16

6. Erläuterungen zu einzelnen Gesetzesbestimmungen **17**
6.1 Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (IDAG) 17
6.1.1 Einzelne Bestimmungen 17
6.1.2 Änderungen auf Verordnungsstufe 33
6.2 Einführungsgesetz zur Schweizerischen Strafprozessordnung (EG StPO) 33
6.3 Gesetz über die Gewährleistung der öffentlichen Sicherheit (Polizeigesetz, PolG) 35
6.3.1 Vorbemerkungen 35
6.3.2 Einzelne Bestimmungen 35
6.4 Einführungsgesetz zum Bundesgesetz über die obligatorische Arbeitslosenversicherung und die Insolvenzentschädigung sowie zum Bundesgesetz über die Arbeitsvermittlung und den Personalverleih (EG AVIG/AVG) 37
6.4.1 Vorbemerkungen 37
6.4.2 Einzelne Bestimmungen 38

7. Auswirkungen **39**
7.1 Personelle und finanzielle Auswirkungen auf den Kanton 39
7.2 Auswirkungen auf die Wirtschaft 39
7.3 Auswirkungen auf die Gemeinden 39
7.4 Auswirkungen auf die Beziehungen zum Bund und zu anderen Kantonen 39

8. Weiteres Vorgehen **39**

Antrag **40**

Sehr geehrter Herr Präsident
Sehr geehrte Damen und Herren

Wir unterbreiten Ihnen den Entwurf zur Änderung des Gesetzes über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (IDAG), zur Änderung des Einführungsgesetzes zur Schweizerischen Strafprozessordnung (EG StPO); zur Änderung des Gesetzes über die Gewährleistung der öffentlichen Sicherheit (Polizeigesetz, PolG) und zur Änderung des Einführungsgesetzes zum Bundesgesetz über die obligatorische Arbeitslosenversicherung und die Insolvenzentschädigung sowie zum Bundesgesetz über die Arbeitsvermittlung und den Personalverleih (EG AVIG/AVG) für die 1. Beratung zur Beschlussfassung und erstatten Ihnen dazu folgenden Bericht.

Zusammenfassung

Am 27. April 2016 hat die Europäische Union (EU) ihre Datenschutzgesetzgebung revidiert. Diese umfasst zwei Rechtsakte. Zum einen die Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum anderen die Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten im Bereich des Strafrechts. Der Europarat wiederum sieht ein Protokoll zur Revision der Konvention SEV 108 zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten vor, dessen Verabschiedung noch aussteht.

Diese gesetzgeberischen Tätigkeiten auf europäischer Ebene wirken sich sowohl auf das Bundesrecht als auch auf kantonales Recht aus. In verschiedenen Bereichen liegt dabei die Rechtsetzungszuständigkeit beim Bund. Er nimmt die notwendigen Anpassungen in der derzeit laufenden Revision des Bundesgesetzes über den Datenschutz (DSG) vom 19. Juni 1992, das die Datenbearbeitungen durch Private und öffentliche Organe des Bundes regelt, und der bundesrechtlichen Spezialgesetzgebung vor.

Im kantonalen Datenschutzrecht, das die Bearbeitung von Personendaten durch kantonale und kommunale öffentliche Organe regelt, steht die Anpassung des formellen Datenschutzrechts im Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (IDAG) vom 24. Oktober 2006 im Vordergrund. Insbesondere durch die Einführung von neuen Begrifflichkeiten und der Erhöhung des Detaillierungsgrads der Bestimmungen im Datenschutz-Reformpaket der EU müssen Ergänzungen und Präzisierungen vorgenommen werden. Es sind aber auch Bereiche des materiellen Datenschutzrechts tangiert. Diesbezüglich anzupassen sind das Gesetz über die Gewährleistung der öffentlichen Sicherheit (Polizeigesetz, PolG) vom 6. Dezember 2005, das Einführungsgesetz zur Schweizerischen Strafprozessordnung (EG StPO) vom 16. März 2010 und das Einführungsgesetz zum Bundesgesetz über die obligatorische Arbeitslosenversicherung und die Insolvenzentschädigung sowie zum Bundesgesetz über die Arbeitsvermittlung und den Personalverleih (EG AVIG/AGV) vom 14. September 2004.

Die Vorlage beschränkt sich ausschliesslich auf die zwingend notwendigen Anpassungen. Die wesentlichen Neuerungen im IDAG betreffen:

- Verzicht auf den Schutz der Daten von juristischen Personen, wodurch auch eine Einheitlichkeit mit der vorgesehenen bundesrechtlichen Regelung geschaffen wird.
- Erhöhung der Transparenz von Datenbearbeitungen. Insbesondere wird die Informationspflicht bei der Datenbeschaffung auf alle Datenbearbeitungen durch öffentliche Organe ausgeweitet, wobei Ausnahmen vorbehalten bleiben.
- Die Rechte der betroffenen Personen werden in verschiedenen Punkten klarer definiert. Unter anderem soll ausdrücklich das Recht auf Löschung der Daten festgehalten werden, während dies im geltenden Recht nur implizit erwähnt ist.
- Die Stellung und Unabhängigkeit der beauftragten Person für Öffentlichkeit und Datenschutz wird formell gestärkt.

Die Anpassungen des kantonalen Rechts führen zu keinen personellen und finanziellen Auswirkungen auf den Kanton. Der zu erwartende Mehraufwand ist überschaubar und wird mit bestehenden Ressourcen abgedeckt.

Die vorgeschlagenen Anpassungen gewährleisten hingegen, dass die kantonalen Datenschutzbestimmungen dem europäischen Standard genügen. Dies wird für den zunehmenden elektronischen Handel und die international tätige Wirtschaft von Nutzen sein, wird dadurch doch der Marktzutritt in den EU-Raum gesichert. Dadurch profitiert auch die Aargauer Volkswirtschaft als Ganzes. Für die Polizeiarbeit wird durch die Beibehaltung des europäischen Standards der Zugriff auf das europaweite Fahndungssystem – das Schengener Informationssystem (SIS) – garantiert. Für die Prüfung eines Visumsgesuchs, die Erteilung eines Aufenthaltstitels sowie zur Überprüfung von Einreise- und Aufenthaltsverweigerungen gegenüber Drittstaatsangehörigen ist das Zugriffsrecht auf das SIS ausserdem auch für die kantonalen Migrationsbehörden relevant. Schliesslich ist das Zugriffsrecht auf das SIS auch für die Strassenverkehrsämter von Bedeutung, weil sie dadurch kontrollieren können, ob das ihnen vorgeführte Fahrzeug gestohlen oder sonst abhandengekommen ist oder ob es zur Beweissicherung in Strafverfahren gesucht wird.

Nach der Notifizierung der Richtlinie (EU) 2016/680 am 1. August 2016 beschloss der Bundesrat am 31. August 2016 deren Übernahme. Für die Schweiz gilt eine Umsetzungsfrist von zwei Jahren ab Notifikation des jeweiligen Rechtserlasses. Die EU-Datenschutzreform muss demzufolge auch von den Kantonen bis zum 1. August 2018 umgesetzt werden, das heisst, die Gesetzesänderungen müssen auf diesen Zeitpunkt in Kraft gesetzt werden.

---

1. Ausgangslage

Auf Bundesebene war der Datenschutz in den vergangenen Jahren vermehrt Gegenstand zahlreicher parlamentarischer Interventionen. Da der deutliche politische Wille besteht, die Bundesgesetzgebung in diesem Bereich zu stärken, unterzieht der Bund derzeit das Bundesgesetz über den Datenschutz (DSG) vom 19. Juni 1992 einer Totalrevision. Die Revision beruht auf einem Bundesratsbeschluss, wonach eine Vorlage mit zwei Zielsetzungen ausgearbeitet werden soll. Einerseits sollen die Schwächen des DSG behoben werden, die aufgrund der rasanten technologischen Entwicklung entstanden sind. Andererseits soll die Revision den Entwicklungen auf der Ebene des Europarats und der Europäischen Union (EU) Rechnung tragen.

Auch auf internationaler Ebene wird dem Datenschutz immer grössere Beachtung geschenkt. So hat die EU am 27. April 2016 ihre Datenschutzgesetzgebung revidiert. Diese umfasst zwei Rechtsakte. Zum einen die Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum anderen die Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten im Bereich des Strafrechts. Nur die Richtlinie (EU) 2016/680 ist Teil des Schengen-Abkommens. Der Europarat wiederum sieht ein Protokoll zur Revision der Konvention SEV 108 zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten vor, dessen Verabschiedung noch aussteht.

Die Verordnung (EU) 2016/679 und die Richtlinie (EU) 2016/680 bei der justiziellen und polizeilichen Zusammenarbeit sind beide seit 5. Mai 2016 in Kraft. Die revidierte Datenschutzkonvention des Europarats wird voraussichtlich 2017 verabschiedet werden.

Nach der Notifizierung der Richtlinie (EU) 2016/680 am 1. August 2016 beschloss der Bundesrat am 31. August 2016 deren Übernahme. Gleichzeitig beauftragte er das Eidgenössische Justiz- und Polizeidepartement (EJPD), die zur Umsetzung erforderlichen Gesetzesänderungen in die laufende Revision des DSG aufzunehmen.

Die Revision des Bundesrechts soll sicherstellen, dass die Gesetzgebung auf Bundesebene mit der revidierten Konvention SEV 108 vereinbar ist, damit die Schweiz das revidierte Übereinkommen so rasch als möglich unterzeichnen kann. Darüber hinaus soll die Vorlage die Anforderungen der Richtlinie (EU) 2016/680 übernehmen, damit die Schweiz ihren Schengen-Verpflichtungen nachkommen kann. Die Revision setzt auch die Empfehlungen um, welche die EU der Schweiz im Rahmen der Schengen-Evaluation gemacht hat. Dabei wurde insbesondere empfohlen, die Kompetenzen des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) auszubauen. Schliesslich soll die Vorlage die schweizerische Datenschutzgesetzgebung insgesamt den Anforderungen der Verordnung (EU) 2016/679 annähern. Diese Annäherung bildet zusammen mit der Ratifizierung der revidierten Konvention SEV 108 die zentrale Voraussetzung dafür, dass die Europäische Kommission der Schweiz in einem Angemessenheitsbeschluss weiterhin bestätigt, dass die schweizerische Gesetzgebung einem angemessenen Datenschutzniveau entspricht.

Die Übernahme der Richtlinie (EU) 2016/680 und die Annahme des Änderungsprotokolls zur Konvention SEV 108 durch die Schweiz ist auch für die Kantone bindend. Diese müssen ihre kantonalen Gesetzgebungen insoweit anpassen, als sie die Anforderungen dieser Instrumente nicht erfüllen.

2. Handlungsbedarf

2.1 Richtlinie (EU) 2016/680

Die Richtlinie (EU) 2016/680 ist darauf ausgerichtet, personenbezogene Daten zu schützen, die zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschliesslich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, bearbeitet werden. Sie soll ein hohes Schutzniveau für personenbezogene Daten gewährleisten und gleichzeitig den Austausch dieser Daten zwischen den zuständigen Behörden der verschiedenen Schengen-Staaten erleichtern. Sie gilt sowohl für grenzüberschreitende Datenbearbeitungen als auch für Datenbearbeitungen, die von den Polizei- und Justizbehörden ausschliesslich auf innerstaatlicher Ebene durchgeführt werden. Nachfolgend werden die wichtigsten Neuerungen aufgeführt.

- Nach den allgemeine Bestimmungen in Kapitel I führt die Richtlinie (EU) 2016/680 in Kapitel II eine Verpflichtung zur Unterscheidung verschiedener Kategorien betroffener Personen sowie Regeln zur Unterscheidung der Daten und zur Überprüfung der Qualität der Daten ein. Zudem wird die Rechtmässigkeit der Datenbearbeitung geregelt. Datenbearbeitungen müssen im Wesentlichen auf einer gesetzlichen Grundlage beruhen. Andere Rechtfertigungsgründe, wie beispielsweise die Einwilligung der betroffenen Person, gelten nicht für Datenbearbeitungen in ihrem Geltungsbereich. Weiter ist eine ausschliesslich auf einer automatischen Verarbeitung beruhende Entscheidung verboten, sofern sie nach dem Recht des betreffenden Mitgliedstaats nicht erlaubt wird, und für die betroffene Person das Recht auf ein persönliches Eingreifen seitens des Verantwortlichen gewährleistet ist.
- In Kapitel III sieht die Richtlinie (EU) 2016/680 neue Rechte für die betroffene Person vor. So ist der Verantwortliche verpflichtet, die Datenverarbeitung einzuschränken, wenn die betroffene Person die Richtigkeit der Daten bestreitet und die Richtigkeit nicht festgestellt werden kann. Ebenfalls hat die betroffene Person im Fall einer Einschränkung die Möglichkeit, ihre Rechte über die Aufsichtsbehörde auszuüben.
- Im Sinn der Pflichten des für die Datenbearbeitung Verantwortlichen und des Auftragsbearbeiters führt die Richtlinie (EU) 2016/680 in Kapitel IV den Grundsatz des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen ein. Die Verantwortlichen und Auftragsbearbeiter müssen auch ein Verzeichnis aller Kategorien von Bearbeitungstätigkeiten führen, die ihrer Zuständigkeit unterliegen. Ausserdem sind die Verantwortlichen verpflichtet, vor bestimmten Verarbeitungen eine Datenschutz-Folgenabschätzung durchzuführen und gegebenenfalls die Aufsichtsbehörde zu konsultieren. Es besteht die Pflicht, in gewissen Fällen der Aufsichtsbehörde

eine Verletzung des Datenschutzes zu melden und gegebenenfalls die betroffene Person zu benachrichtigen. Ebenfalls wird in Kapitel IV die Benennung eines Datenschutzbeauftragten vorgesehen.

- Kapitel V hält fest, dass die Europäische Kommission dafür zuständig ist, das Schutzniveau zu prüfen, das ein Drittland, ein Gebiet oder ein Verarbeitungssektor in einem Drittland bietet. Hat die Europäische Kommission die Angemessenheit des Schutzniveaus in einem Drittstaat nicht durch Beschluss festgestellt, darf die Datenübermittlung nur erfolgen, wenn geeignete Garantien bestehen oder wenn in bestimmten Fällen eine Ausnahme vorliegt.
- In Kapitel VI verpflichtet die Richtlinie (EU) 2016/680 die Schengen-Staaten, im Bereich des Datenschutzes unabhängige Aufsichtsbehörden einzusetzen. Diese Aufsichtsbehörde ist aber nicht für Datenverarbeitungen zuständig, die Gerichte im Rahmen ihrer justiziellen Tätigkeit vornehmen. Die Schengen-Staaten können auch eine Ausnahme für jene Datenverarbeitungen vorsehen, die durch andere unabhängige Justizbehörden im Rahmen ihrer justiziellen Tätigkeit erfolgen. Ausserdem wird vorgesehen, dass die Aufsichtsbehörde über wirksame Untersuchungsbefugnisse verfügt, das heisst zumindest vom Verantwortlichen und vom Auftragsbearbeiter Zugang zu den verarbeiteten Daten und allen Informationen erhält, die zur Erfüllung ihrer Aufgaben notwendig sind. Die Aufsichtsbehörde soll auch über wirksame Abhilfebefugnisse verfügen, wie beispielsweise über die Befugnis zur Verwarnung eines Verantwortlichen oder eines Auftragsbearbeiters, zur Anordnung von vorschriftsgemässen Bearbeitungen, gegebenenfalls durch Berichtigung oder Löschung der Daten, sowie zur Verhängung einer vorübergehenden oder endgültigen Beschränkung der Verarbeitung, einschliesslich eines Verbots. Die Befugnisse der Aufsichtsbehörde dürfen jedoch weder die speziellen Vorschriften für Strafverfahren, einschliesslich der Ermittlung und Verfolgung von Straftaten, noch die Unabhängigkeit der Gerichte berühren.
- Schliesslich sieht die Richtlinie (EU) 2016/680 in Kapitel VII vor, dass die betroffene Person das Recht auf Beschwerde bei der Aufsichtsbehörde hat. Die betroffene Person hat auch das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen einen sie betreffenden Entscheid der Aufsichtsbehörde.

Die Richtlinie (EU) 2016/680 entspricht einer Weiterentwicklung des Schengen-Besitzstands. Gemäss Art. 2 Abs. 3 des Schengen-Assoziierungsabkommens hat sich die Schweiz grundsätzlich verpflichtet, jede Weiterentwicklung des Schengen-Besitzstands zu akzeptieren, umzusetzen und anzuwenden.

Die Richtlinie (EU) 2016/680 ist sowohl für die EU-Mitgliedstaaten als auch für die Schweiz nicht direkt anwendbar und bedarf einer Umsetzung in das jeweilige nationale Recht. In der Schweiz braucht es zur Umsetzung der Richtlinie (EU) 2016/680 nicht nur Anpassungen des DSG und verschiedener Bundesgesetze, sondern auch der kantonalen Datenschutzbestimmungen. Es gilt eine Umsetzungsfrist von zwei Jahren ab Notifikation. Die Richtlinie (EU) 2016/680 muss demzufolge auch von den Kantonen bis zum 1. August 2018 umgesetzt werden.

2.2 Datenschutzkonvention SEV 108

Mit dem Entwurf der Revision der Konvention SEV 108 zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten (nachfolgend E-SEV 108) wird der Datenschutz auf internationaler Ebene vereinheitlicht und verbessert. Dies verstärkt auch den Schutz der Schweizer Bürgerinnen und Bürger, wenn ihre Personendaten im Ausland bearbeitet werden. Der E-SEV 108 trägt ebenfalls dazu bei, die Bekanntgabe von Daten zwischen den Vertragsparteien zu vereinfachen. Dadurch erhalten Schweizer Unternehmen einen besseren Zugang zu den Märkten dieser Länder. Die Unterzeichnung des Entwurfs für die Änderung des Übereinkommens SEV 108 dürfte zudem eine zentrale Voraussetzung sein, damit die EU der Schweiz erneut ein angemessenes Datenschutzniveau bestätigt. Nur dadurch bleibt der Zugang zum europäischen Markt weiterhin uneingeschränkt gewährleistet. Der Bundesrat hat in mehreren Antworten auf parlamentarische Vorstösse

zum Ausdruck gebracht, dass er die E-SEV 108 unterstützt. Die Ratifizierung steht noch aus, denn zusammen mit dieser müssen die erforderlichen Massnahmen zur Umsetzung der Bestimmungen gemäss E-SEV 108 in Kraft treten. Der Entwurf des revidierten DSG, zu welchem im 1. Quartal 2017 das Vernehmlassungsverfahren durchgeführt worden ist, stimmt weitgehend mit den Anforderungen des Änderungsprotokolls zum E-SEV 108 überein.

Die Vertragsparteien müssen den E-SEV 108 auf alle Datenbearbeitungen in ihrer Rechtsordnung im öffentlichen und privaten Sektor anwenden. Nicht durch diesen Entwurf geregelt werden nur Datenbearbeitungen, die eine Person im Rahmen ihrer persönlichen Aktivitäten vornimmt. Die wesentlichsten Punkte im E-SEV 108 sind:

- Die Pflichten des für die Datenverarbeitung Verantwortlichen werden ausgeweitet. Dieser ist verpflichtet, der zuständigen Aufsichtsbehörde bestimmte Verstösse gegen den Datenschutz zu melden. Die Verpflichtung, die betroffene Person zu informieren, muss überdies auf die zu liefernden Informationen und die automatisierten Einzelentscheidungen ausgedehnt werden. Zudem sind im Vorfeld bestimmter Datenverarbeitungen eine Folgenabschätzung vorzunehmen und für den Datenschutz die Grundsätze der datenschutzfreundlichen Technikgestaltung (Privacy by Design) und der datenschutzfreundlichen Voreinstellungen (Privacy by Default) anzuwenden.
- Der von der Datenbearbeitung betroffenen Person ist das Recht einzuräumen, nicht einer Entscheidung unterworfen zu sein, die ausschliesslich auf der Grundlage einer automatisierten Verarbeitung ihrer Daten ergeht, ohne dass die betroffene Person ihren Standpunkt geltend machen kann. Diese Bestimmung hat für die Umsetzung im kantonalen aargauischen Recht keine Bedeutung, weil Einzelentscheidungen der Behörden über Rechte und Pflichten in Form einer Verfügung ergehen müssen, verbunden mit den entsprechenden verfahrensrechtlichen Ansprüchen der Parteien.
- Das Auskunftsrecht der betroffenen Person und die Bedingungen für deren Einwilligung in die Datenbearbeitung werden erweitert.
- Die Vertragsparteien sind verpflichtet, ein Sanktionensystem und ein Rechtsmittelsystem festzulegen. Der Ausbau des Sanktionensystems erfolgt im Vorentwurf DSG; für das kantonale Recht wird auf die Einführung von Sanktionsmöglichkeiten gegenüber den öffentlichen Organen verzichtet.
- Personendaten dürfen nur in einen Drittstaat übermittelt werden, wenn ein angemessener Schutz gewährleistet ist. Ein angemessenes Datenschutzniveau kann durch Rechtsvorschriften des betreffenden Staats oder der empfangenden internationalen Organisation oder durch bestimmte Sicherheiten gewährleistet werden. Wenn kein angemessenes Schutzniveau garantiert ist, dürfen Daten an einen Drittstaat nur weitergegeben werden, wenn der Betroffene gültig eingewilligt hat oder wenn ein bestimmter Ausnahmefall vorliegt. Schliesslich müssen die Vertragsparteien gemäss dem E-SEV 108 vorsehen, dass die Aufsichtsbehörde von der Person, welche die Daten weitergibt, den Nachweis über die Wirksamkeit der aufgestellten Sicherheiten verlangen und die Datenweitergabe gegebenenfalls verbieten oder aussetzen kann.
- Die Vertragsparteien sind verpflichtet, eine unabhängige Aufsichtsbehörde zu schaffen. Die Aufsichtsbehörden müssen ermächtigt werden, verbindliche, anfechtbare Entscheidungen zu fällen und verwaltungsrechtliche Sanktionen zu verhängen. Von der Überwachung durch die Aufsichtsbehörde sind lediglich Datenverarbeitungen ausgenommen, die von Organen in Ausübung ihrer Rechtsprechungsbefugnisse ausgeführt werden. Der Aufsichtsbehörde muss auch der Auftrag erteilt werden, die Öffentlichkeit und die für die Verarbeitung Verantwortlichen für den Datenschutz zu sensibilisieren.

2.3 Verordnung (EU) 2016/679

Die Verordnung (EU) 2016/679 ist der grundlegende Datenschutzerlass auf Ebene der EU. Sie gehört aber nicht zum Schengen-Besitzstand. Die Richtlinie (EU) 2016/680 ist inhaltlich auf die Verordnung ausgerichtet, so dass die beiden Erlasse weitgehend übereinstimmende Regelungen vorsehen. Allerdings ist die Verordnung detaillierter, während die Bestimmungen der Richtlinie (EU) 2016/680 auf die Bedürfnisse der Strafbehörden ausgerichtet sind.

Die Verordnung (EU) 2016/679 regelt hauptsächlich den Schutz von Personen, deren Daten im Rahmen des Binnenmarkts bearbeitet werden, doch sie gilt auch für den öffentlichen Sektor. Sie enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.

Für die Schweiz sind die Bestimmungen der Verordnung (EU) 2016/679 mangels Schengenrelevanz nicht verbindlich. Dies bedeutet jedoch nicht, dass sie keine Auswirkungen in den Bereichen haben, in denen die Schweiz als Drittstaat betrachtet wird. Indem ihr Geltungsbereich sehr weit gefasst ist – sie richtet sich gleichermassen an Unionsbehörden wie Private – setzt sie verbindliche Minimal-Standards. Diese Standards beziehungsweise Vorgaben zu einem angemessenen Datenschutz sind bei der Anwendung der beiden anderen Rechtserlasse im öffentlich-rechtlichen wie auch privatrechtlichen (wirtschaftlichen) Bereich (Binnenmarkt) zu beachten und demnach auch für die Schweiz massgeblich. Gemäss Beschluss der Europäischen Kommission vom 26. Juli 2000 besteht in der Schweiz ein angemessenes Datenschutzniveau. Dieser Beschluss kann jedoch jederzeit widerrufen werden. Wenn die Schweiz erneut einen Angemessenheitsbeschluss der EU erhalten will, tut sie als Drittstaat gut daran, ihre Gesetzgebung an die europäischen Anforderungen anzupassen. Die in der Verordnung (EU) 2016/679 festgelegten Kriterien sind künftig massgebend für die Beurteilung, ob die schweizerische Gesetzgebung einen angemessenen Datenschutz gewährleistet. Das kantonale Datenschutzrecht soll daher ein angemessenes Schutzniveau im Sinn der Verordnung garantieren.

2.4 Aarhus-Konvention (AK)

Am 1. Juni 2014 trat für die Schweiz das Übereinkommen über den Zugang zu Informationen, die Öffentlichkeitsbeteiligung an Entscheidungsverfahren und den Zugang zu Gerichten in Umweltangelegenheiten (Aarhus-Konvention [AK]) in Kraft, welche – neben der Beteiligung der Öffentlichkeit an Entscheidungsverfahren und dem Zugang zu Gerichten in Umweltangelegenheiten – den Zugang zu Umweltinformationen zum Gegenstand hat und die Vertragsparteien verpflichtet, diesen sicherzustellen. Enthalten die Informationen Personendaten, ist eine Abwägung zwischen dem öffentlichen Interesse an der Bekanntgabe und dem Geheimhaltungsinteresse der betroffenen Person vorzunehmen.

Das eidgenössische Parlament hat im Rahmen der Genehmigung der AK das Bundesgesetz über den Umweltschutz (Umweltschutzgesetz, USG) vom 7. Oktober 1983 angepasst und darin in einem neuen Absatz 8 zu Art. 7 den Begriff "Umweltinformationen" definiert. Zudem erhält jede Person das Recht, in amtlichen Dokumenten enthaltene Umweltinformationen einzusehen und von den Behörden Auskünfte über den Inhalt dieser Dokumente zu erhalten.

Befinden sich die Informationen bei Behörden der Kantone, richtet sich der Anspruch nach kantonalem Recht. Soweit die Kantone noch keine Bestimmungen über den Zugang zu Dokumenten erlassen haben, sind die Bestimmungen des Bundesrechts sinngemäss anzuwenden. Eine Anpassung des aargauischen kantonalen Rechts unterblieb bei Inkrafttreten des revidierten Umweltschutzgesetzes, weil damals die Auffassung herrschte, dass das kantonale Öffentlichkeitsprinzip den Anforderungen bereits entspreche. Nachdem das Verwaltungsgericht in einem Entscheid im Juni 2016 nun Klärung darüber gebracht hat, dass nach geltender Regelung des Öffentlichkeitsprinzips auch bei überwiegenden Interessen keine Einsicht in Dokumente mit Personendaten möglich ist, ist diese Anpassung nachzuholen.

2.5 Europäische Menschenrechtskonvention

Aus dem Urteil vom 8. November 2016 in Sachen MAGYAR HELSINKI BIZOTTSÁG v. HUNGARY des Europäischen Gerichtshofs für Menschenrechte geht hervor, dass die Ablehnung der Einsicht in amtliche Dokumente alleine aufgrund der Tatsache, dass darin Personendaten enthalten sind und ohne eine Interessenabwägung durchzuführen, gegen die Meinungsäusserungs- und Informationsfreiheit gemäss Art. 10 Abs. 1 der Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK) verstösst. Die Regelung des Öffentlichkeitsprinzips im Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (IDAG) vom 24. Oktober 2006 ist entsprechend anzupassen. Damit wird auch die bei Erlass des IDAG bestehende Forderung erfüllbar gemacht, dass Beschaffungsgeschäfte der öffentlichen Hand transparent gemacht werden sollen.

2.6 Fazit

Die zuvor erwähnten gesetzgeberischen Tätigkeiten und die Rechtsprechung auf europäischer Ebene wirken sich sowohl auf das Bundesrecht als auch auf kantonales Recht aus. In verschiedenen Bereichen liegt dabei die Rechtsetzungszuständigkeit beim Bund. Er hat die notwendigen Änderungen des DSG, das die Datenbearbeitungen durch Private und öffentliche Organe des Bundes regelt, und der bundesrechtlichen Spezialgesetzgebung (zum Beispiel des Bundesgesetzes über die Ausländerinnen und Ausländer [Ausländergesetz, AuG] vom 16. Dezember 2005, des Asylgesetzes [AsylG] vom 26. Juni 1998, des Bundespersonalgesetzes [BPG] vom 24. März 2000, des Schweizerischen Zivilgesetzbuchs [ZGB] vom 10. Dezember 1907 etc.) vorzunehmen.

Bei der Bearbeitung von Personendaten durch kantonale und kommunale öffentliche Organe gelten die kantonalen Datenschutzbestimmungen. Im kantonalen Recht steht die Anpassung des formellen Datenschutzrechts IDAG im Vordergrund. Insbesondere durch die Einführung von neuen Begrifflichkeiten und der Erhöhung des Detaillierungsgrads der Bestimmungen im Datenschutz-Reformpaket der EU müssen Ergänzungen und Präzisierungen vorgenommen werden. Es sind aber auch Bereiche des materiellen Datenschutzrechts tangiert, wie nachfolgend in den Ziffern 6.2–6.4 aufgezeigt wird.

3. Umsetzung

3.1 Bund

Auf Bundesebene wird, wie erwähnt, das DSG totalrevidiert. Gleichzeitig mit der Revision wird auch die EU-Datenschutzreform umgesetzt. In Zusammenhang mit dieser Revision nimmt der Bund zudem in 58 weiteren Erlassen Anpassungen des materiellen Datenschutzrechts vor (beispielsweise Regelungen des Zivilprozessrechts, des Strafrechts, des Strafprozessrechts etc.). Der Vorentwurf DSG (VE-DSG) sieht für Kantone, die am 1. August 2018 noch keinen angemessenen Datenschutz gewährleisten, eine direkte Anwendung des Bundesrechts vor.

3.2 Kantonale Umsetzung

Der unmittelbare Handlungsbedarf wurde eruiert und gestützt darauf wurden die vorliegenden Gesetzesrevisionen ausgearbeitet. Die Vorlage konzentriert sich vornehmlich am Anpassungsbedarf, der sich aufgrund der EU-Datenschutzreform ergibt. Sie beschränkt sich dabei auf die zwingend notwendigen Anpassungen, die zum wesentlichen Teil das formelle Datenschutzrecht im IDAG betreffen. Einzelne materiell-rechtliche Bestimmungen zur bereichs- und/oder fachspezifischen Umsetzung des Datenschutzes finden sich in den verschiedenen Spezialerlassen. Diesbezüglich anzupassen sind das Gesetz über die Gewährleistung der öffentlichen Sicherheit (Polizeigesetz, PolG) vom 6. Dezember 2005, das Einführungsgesetz zur Schweizerischen Strafprozessordnung (EG StPO) vom 16. März 2010 und das Einführungsgesetz zum Bundesgesetz über die obligatorische Arbeitslo-

senversicherung und die Insolvenzentschädigung sowie zum Bundesgesetz über die Arbeitsvermittlung und den Personalverleih (EG AVIG/AGV) vom 14. September 2004.

Der Revisionsentwurf orientiert sich konsequent an den potenziellen Risiken für die betroffenen Personen, denn die Gefahren für die Privatsphäre der betroffenen Personen hängen weitgehend von den Aktivitäten der verschiedenen öffentlichen Organe und Auftragsbearbeiter ab. Dementsprechend sind beispielsweise die Pflichten von öffentlichen Organen, deren Aktivitäten mit einem erhöhten Risiko verbunden sind (zum Beispiel weil sie besonders schützenswerte Personendaten bearbeiten und austauschen oder weil sie Informationssysteme mit Zugriffsmöglichkeit durch andere Behörden oder Private betreiben) strenger als jene von öffentlichen Organen, deren Aktivitäten ein geringeres Risiko darstellen (zum Beispiel Datenbearbeitungen, die in einem Dokumentenmanagementsystem ohne besonders schützenswerte Daten erfolgen).

Im Vordergrund der Revision des IDAG stehen im Wesentlichen folgende Punkte:

- Auf den Schutz der Daten juristischer Personen soll verzichtet werden. In den datenschutzrechtlichen Bestimmungen der EU und des Europarats sowie der meisten ausländischen Rechtsordnungen ist kein solcher Schutz vorgesehen. Der Schutz von Daten juristischer Personen ist nur von geringer praktischer Bedeutung. Wenn er aufgehoben wird, sollte dies keine negativen Auswirkungen haben, insbesondere mit Blick auf den Schutz, der durch andere spezifische Gesetze gewährleistet wird (Persönlichkeitsschutz, unlauterer Wettbewerb, Urheberrecht). Durch diese Änderung soll eine Einheitlichkeit mit der bundesrechtlichen Regelung gemäss VE-DSG geschaffen werden.
- Die Transparenz von Datenbearbeitungen soll erhöht werden. So wird die Informationspflicht bei der Datenbeschaffung auf alle Datenbearbeitungen durch öffentliche Organe ausgeweitet. Sie kann auf standardisierte Weise erfüllt werden, zudem sind Ausnahmen vorgesehen. Gemäss dem Entwurf müssen der betroffenen Person auch mehr Informationen vorgelegt werden, wenn diese ihr Auskunftsrecht geltend macht.
- Die Rechte der betroffenen Personen werden in verschiedenen Punkten klarer definiert. Unter anderem ist im Entwurf ausdrücklich das Recht auf Löschung der Daten festgehalten, während dies im geltenden Recht nur implizit erwähnt ist.
- Die Stellung und Unabhängigkeit der beauftragten Person für Öffentlichkeit und Datenschutz wird formell gestärkt. Sie darf nur unter ganz bestimmten Bedingungen einer Nebenbeschäftigung nachgehen. Im Weiteren wird vorgesehen, dass die beauftragte Person – wie ihre Kolleginnen und Kollegen in den anderen europäischen Ländern – nach Abschluss einer Untersuchung, die von Amtes wegen oder auf Anzeige hin eingeleitet wurde, Verfügungen erlassen kann, die für die Verantwortlichen und die Auftragsbearbeitenden verbindlich sind. Nur das öffentliche Organ, gegen das die Untersuchung eingeleitet wurde, ist in einem Untersuchungsverfahren Partei.
- Im Weiteren wird dem technologieneutralen Charakter des IDAG Beachtung geschenkt. Dadurch bleibt das Gesetz offen für weitere technologische Entwicklungen und verhindert keine Innovationen. Weil sie dem technologieneutralen Charakter des Erlasses widerspricht, wird beispielsweise die Regelung des "Abrufverfahrens" aufgegeben.
- Schliesslich wird die Terminologie modernisiert, insbesondere, um die Vereinbarkeit mit dem europäischen Recht zu verbessern. So werden gewisse Begriffe aus dem europäischen Recht übernommen. Das Register der Datensammlungen wird aufgehoben und für den Bereich der Strafverfolgung durch ein Register der Datenbearbeitungen ersetzt. Der Begriff "Persönlichkeitsprofil", der eine schweizerische Besonderheit darstellt, wird durch den Begriff "Profiling" abgelöst. Der Begriff "besonders schützenswerte Personendaten" wird um "genetische und biometrische Daten, die eine Person eindeutig identifizieren", erweitert.

4. Verhältnis zur mittel- und langfristigen Planung

Gemäss dem Entwicklungsleitbild des Regierungsrats haben die grenzüberschreitende wirtschaftliche Zusammenarbeit und die Kriminalitätsbekämpfung einen hohen Stellenwert. Dementsprechend ist es von grosser Bedeutung, dass das kantonale Datenschutzrecht in den verschiedenen Punkten den Standards des EU-Datenschutzrechts entspricht. Für die Schweiz ist die Richtlinie (EU) 2016/680 Bestandteil des Schengen-Abkommens. Dieses Abkommen gewährleistet den Zugriff auf das europaweite Fahndungssystem, das Schengener Informationssystem (SIS). Das SIS versorgt die nationalen Sicherheitsbehörden mit aktuellsten Informationen über polizeilich Gesuchte, Vermisste oder mit einem Einreiseverbot belegte Personen sowie über gestohlene Sachen. Das SIS ist zum zentralen Fahndungssystem in Westeuropa geworden, weshalb das Schengen-Abkommen für die Schweiz und die Kantone von grosser Bedeutung ist. Will man diese für die Kriminalitätsbekämpfung wichtige Möglichkeit erhalten, muss die Richtlinie (EU) aufgrund des Schengen-Assoziierungsabkommens vom 26. Oktober 2004 von Bund und Kantonen übernommen werden. Im Rahmen der Schengen-Evaluation überprüft die EU regelmässig die Schengen-Staaten und damit auch die Schweiz darauf, ob diese ihren Verpflichtungen nachkommen. Nach 2008 und 2014 wird die Schweiz 2018 seitens der EU einer weiteren ordentlichen Evaluation unterzogen. Dabei finden in einzelnen Bereichen auch Überprüfungen vor Ort statt.

In den Bereichen, die nicht der Schengen-Zusammenarbeit unterstehen, gilt die Schweiz als Drittstaat. Zwischen einem Drittstaat und den Mitgliedstaaten der EU dürfen Daten nur ausgetauscht werden, wenn der Drittstaat ein angemessenes Schutzniveau gemäss der Richtlinie 95/46/EG vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr gewährleistet. Dieses insbesondere auch für die wirtschaftliche Zusammenarbeit mit dem Ausland relevante Schutzniveau wird durch die Europäische Kommission periodisch überprüft und in einem Angemessenheitsbeschluss festgehalten. Ein solcher Beschluss kann jederzeit widerrufen werden. Die Europäische Kommission hat in einem Angemessenheitsbeschluss vom 26. Juli 2000 bestätigt, dass die Schweiz über ein angemessenes Datenschutzniveau verfügt. Diese Entscheidung beruht jedoch auf dem in der Richtlinie 95/46/EG festgelegten Schutzniveau. Künftig wird die schweizerische Gesetzgebung anhand der in der Verordnung (EU) 2016/679 enthaltenen Anforderungen überprüft. Falls die Schweiz den Angemessenheitsbeschluss beibehalten beziehungsweise im Fall eines Widerrufs erneut eine Bestätigung über das angemessene Datenschutzniveau erhalten möchte, ist es von zentraler Bedeutung, dass die schweizerische Gesetzgebung sowie die kantonalen Gesetzgebungen den Anforderungen dieser Verordnung entsprechen. Die EU erachtet auch die Ratifizierung und somit Umsetzung der E-SEV 108 als entscheidendes Kriterium für einen Angemessenheitsbeschluss.

5. Auswertung des Anhörungsverfahrens

Die Anhörung zum Entwurf der Gesetzesänderungen fand vom 7. April 2017 bis zum 7. Juni 2017 statt. 20 Rückmeldungen von Parteien, Verbänden und Behörden (SVP, CVP, SP, FDP.Die Liberalen, BDP, EVP, GLP, Grüne, Piratenpartei, Junge GLP, Gemeindeammänner-Vereinigung des Kantons Aargau, Verband Aargauer Gemeindeschreiberinnnen und Gemeindeschreiber, Verband Steuerfachleute Aargauer Gemeinden, Finanzfachleute Aargauer Gemeinden, Verband Aargauer Einwohnerdienste, Verband Aargauer Regionalpolizeien [VAG], Aargauische Gebäudeversicherung [AGV], Aargauische Industrie- und Handelskammer [AIHK], Aargauischer Gewerbeverband und Gerichte Kanton Aargau) sind eingegangen. Die Vorlage ist weitgehend zustimmend aufgenommen worden. Die vorgebrachten Kritikpunkte betreffen vor allem eine befürchtete Zunahme der Verwaltungsaufgaben verbunden mit einem Stellenzuwachs und finanziellen Mehrausgaben. Die SVP, die AIHK und der VAG äussern sich insbesondere skeptisch gegenüber der im Sicherheitsbereich notwendigen und daher im EG StPO und im Polizeigesetz festgehaltenen Benennung einer für den Datenschutz zuständigen Person.

5.1 Bemerkungen zu den Änderungen im IDAG *(Antworten des Regierungsrats sind kursiv)*

5.1.1 Allgemeine Bemerkungen

- Die SVP ist der Ansicht, die Vorlage bausche die Bürokratie auf und könne nicht ohne eine finanzielle Mehrbelastung umgesetzt werden. Sie verlangt insbesondere die Streichung der Datenschutz-Folgenabschätzung, welche unbekannte Kostenfolgen verursache. Auch die AIHK bezweifelt, dass die Vorlage keine finanziellen Auswirkungen habe, und erachtet die Datenschutz-Folgenabschätzung als kostengenerierenden Bürokratieausbau ohne wirklichen Mehrwert. Der Verband Steuerfachleute Aargauer Gemeinden gibt ebenfalls zu bedenken, die konsequente Umsetzung der Datenschutz-Folgenabschätzung führe zu einem erhöhten Aufwand für die beauftragte Person für Öffentlichkeit und Datenschutz.

  Wie unter Ziffer 6.1.1 zu § 17a E-IDAG ausgeführt, ist aufgrund der übergeordneten Rechtsgrundlagen eine Datenschutz-Folgenabschätzung durch das verantwortliche öffentliche Organ zwingend gesetzlich zu verankern. Diese Abschätzung enthält eine allgemeine Beschreibung der geplanten Bearbeitungsvorgänge, eine Bewertung der in Bezug auf die Persönlichkeit und die Grundrechte der betroffenen Personen bestehenden Risiken sowie eine Darstellung und Bewertung der geplanten Abhilfemassnahmen, Garantien, Sicherheitsvorkehren und Verfahren, durch die der Schutz der Persönlichkeit und der Grundrechte der betroffenen Personen sichergestellt und der Nachweis erbracht werden soll, dass dieses Gesetz eingehalten wird. Durch diese Datenschutz-Folgenabschätzung kann das verantwortliche öffentliche Organ letztlich den vom übergeordneten Recht ebenfalls geforderten Nachweis für die Einhaltung der Datenschutzvorschriften (Compliance, Datenschutzmanagementsystem) erbringen.

  Dabei ist zu beachten, dass eine Datenschutz-Folgenabschätzung nur bei neuen geplanten Vorhaben für eine Personendatenbearbeitung – respektive wenn die Personendatenbearbeitungen mit neuen technischen Methoden durchgeführt werden – notwendig ist. Ausserdem ist sie nur durchzuführen, wenn die vorgesehene Datenbearbeitung voraussichtlich zu einem erhöhten Risiko für die Persönlichkeit und die Grundrechte der betroffenen Personen führt. Bereits nach geltendem Recht sind die öffentlichen Organe verpflichtet, für ihre IT-Systeme eine Risikoanalyse durchzuführen und Datensicherheitskonzepte zu erstellen (§ 4 Verordnung zum Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen [VIDAG] vom 26. September 2007). Bestehen besondere Risiken, sind die Datenbearbeitungen der beauftragten Person für Öffentlichkeit und Datenschutz vorab zur Kontrolle vorzulegen (§ 6 VIDAG). Dementsprechend ist aufgrund der Datenschutz-Folgenabschätzung bei den verantwortlichen öffentlichen Organen kein wesentlicher Mehraufwand zu erwarten, der nicht mit bestehenden Ressourcen abgedeckt werden könnte. Der Mehraufwand bei der beauftragten Person für Öffentlichkeit und Datenschutz wird weitgehend durch die Entlastungsmassnahmen kompensiert werden können (vgl. Ziffer 7.1).

- Die Grünen schlagen vor, die Datenschutz-Folgenabschätzung solle bei einer Änderung des Risikos und spätestens alle fünf Jahre neu vorgenommen werden. So könne der gesellschaftlichen und technologischen Entwicklung Rechnung getragen werden.

  Unabhängig vom Zeitablauf ist bei jeder Einführung oder wesentlichen technischen Neuerung einer datenschutzrelevanten Applikation eine Datenschutz-Folgenabschätzung durchzuführen. Hingegen ist eine Datenschutz-Folgenabschätzung, die anlassfrei in sämtlichen Verwaltungsbereichen alle fünf Jahre zwingend neu vorgenommen werden muss, aufgrund der EU-Datenschutzreform nicht erforderlich. Um unnötigen Mehraufwand zu vermeiden, ist auf eine solche Regelung zu verzichten.

- Die Piratenpartei begrüsst ausdrücklich die Stärkung des Datenschutzes, ist aber mit der Aufhebung der Pflicht zur Führung von Datenregistern nicht einverstanden. Auch die SVP spricht sich für die Beibehaltung der Registrierpflicht aus.

  Aufgehoben werden nicht die Register beziehungsweise die Datensammlungen selbst; diese bleiben weiterhin für die Verwaltungsarbeit unerlässlich. Die Behörden mussten aber bisher eine Zusammenstellung der Datensammlungen führen und diese der beauftragten Person für Öffentlichkeit und Datenschutz melden, welche ein zentrales, abgekürztes Register der Datensammlungen führte. Da sich in den letzten acht Jahren nur in einem einzigen Fall eine Person nach dem Register der Datensammlungen erkundigt hat, wird der damit verbundene Aufwand (Aufbereitung nach jährlicher Aktualisierung beziehungsweise Mitteilung) nicht mehr als gerechtfertigt erachtet. Die Behörden haben weiterhin die Pflicht, jeder Person auf Anfrage darüber Auskunft zu geben, welche Daten über sie bearbeitet werden und auf welcher Rechtsgrundlage die Bearbeitung beruht. Diese konkrete, fallbezogene Auskunft ist es, welche die Betroffenen in der Praxis interessiert. Im Weiteren ist gemäss der Richtlinie (EU) 2016/680 für den justiziellen und polizeilichen Bereich inskünftig ein Register der Datenbearbeitungstätigkeit zu führen. Die gesetzlichen Grundlagen hierfür werden im EG StPO und im Polizeigesetz verankert (vgl. Ziffern 6.2 und 6.3).

- Gemäss der Ansicht der SVP geht die Definition des Profiling zu weit.

  Das Profiling wird in Art. 3 Ziffer 4 der Richtlinie [EU] 2016/680 und Art. 3 lit. f VE-DSG definiert. Die Formulierung im vorliegenden Entwurf übernimmt den vom Bund vorgeschlagenen Wortlaut.

- Diese Vorlage schafft zwei Kompetenznormen, wonach der Regierungsrat einerseits die Löschfristen von nicht mehr benötigten Personendaten sowie die Massnahmen zur regelmässigen Überprüfung der weiteren Aufbewahrungsnotwendigkeit von Personendaten (§ 21 Abs. 3 E-IDAG) und andrerseits die Aufbewahrungsfrist von Personendaten im Polizeibereich (§ 54 Abs. 3 E-PolG) mittels Verordnung regelt (vgl. Ziffern 6.1.1 und 6.3.2 hiernach). Die SVP verlangt, dass die entsprechenden Regelungen des Regierungsrats dem Grossen Rat zum Beschluss vorgelegt werden.

  Aufbewahrungsfristen beziehungsweise Löschfristen und Massnahmen zur regelmässigen Überprüfung der weiteren Notwendigkeit der Datenaufbewahrung müssen rasch an sich verändernde Umstände angepasst werden können. Es ist daher angezeigt, die entsprechenden Bestimmungen auf Verordnungsstufe festzulegen. Gemäss § 91 Abs. 2 der Bundesverfassung (BV) obliegt die Kompetenz zum Erlass von Verordnungen alleine dem Regierungsrat. Eine Regelung auf Gesetzes- oder Dekretsebene wäre nicht stufengerecht.

5.1.2 Verzicht auf Schutz der juristischen Personen

Die SVP ist mit dem Verzicht des Schutzes für juristische Personen nicht einverstanden, ohne dabei ihre Ansicht genauer auszuführen. Gemäss den Jungen Grünliberalen erscheine es schwierig, die Folgen eines Verzichts auf den Schutz juristischer Personen abzuschätzen. Die AIHK bringt vor, dass mit dem Verzicht des Schutzes für juristische Personen im Handelsregister eingetragene Einzelunternehmen sowie Mitglieder von Personengesellschaften nach wie vor vom Schutz erfasst seien, während Gesellschaften mit beschränkter Haftung und Aktiengesellschaften den Schutz verlieren würden. Die Abgrenzung der geschützten von den nicht geschützten Personenkategorien sei nicht sachgerecht. Im Handelsregister eingetragene Einzelfirmen oder Mitglieder von Personengesellschaften müssten gleich behandelt werden wie juristische Personen, und daher von der Definition "Betroffenen Personen" gemäss § 3 Abs. 1 lit e E-IDAG ausgenommen werden.

Mit der Änderung des IDAG sollen die besonderen Datenschutzregeln dieses Gesetzes nur noch für natürliche Personen gelten. Die Daten von juristischen Personen werden nach geltendem Recht durch verschiedene Bestimmungen geschützt, zum Beispiel den strafrechtlichen Schutz des Fabrikations- und Geschäftsgeheimnisses, den Persönlichkeitsschutz nach ZGB, das Bundesgesetz gegen den unlauteren Wettbewerb (UWG) vom 19. Dezember 1986, das Urheberrecht und die Daten-

schutzgesetzgebung. Die juristischen Personen werden nach Entlassung aus dem Schutzbereich des IDAG durch die übrigen Bestimmungen genügend geschützt. Der Schutz nach E-IDAG erstreckt sich dabei nur auf die natürliche Person selbst, nicht aber auf Unternehmen von natürlichen Personen, auch wenn es sich bei diesen Unternehmen nicht um juristische Personen handelt.

Die Einschränkung des Begriffs der Personendaten auf natürliche Personen schafft zudem eine Einheitlichkeit mit der bundesrechtlichen Regelung gemäss VE-DSG. Im Übrigen haben kantonale und kommunale öffentliche Organe generell und somit auch im Umgang mit juristischen Personen ohnehin zwei Eckpfeiler des behördlichen Datenschutzrechts, nämlich die in Art. 5 BV vorgeschriebenen Prinzipien der Gesetzmässigkeit und der Verhältnismässigkeit zu beachten.

5.1.3 Erhöhung der Transparenz von Datenbearbeitungen

CVP und FDP.Die Liberalen fordern, dass der mit der Erhöhung der Transparenz von Datenbearbeitungen entstehende Aufwand verhältnismässig bleibe und zu beobachten sei. Die SVP ist mit einer Erhöhung der Transparenz von Datenbearbeitungen nicht einverstanden. Ihrer Ansicht nach stelle die Informationspflicht eine unnötige Bürokratie dar, welche die Verwaltungskosten in die Höhe treibe. Zudem würden Strafverfahren dadurch unnötig in die Länge gezogen. Für den Verband Steuerfachleute Aargauer Gemeinden führt eine konsequente Information der betroffenen Personen bei jeder Informationsbeschaffung teilweise zu einem Mehraufwand. Sämtliche Arbeitsabläufe seien daher zu überprüfen und nötigenfalls anzupassen. Allenfalls seien entsprechenden Ressourcen zu bewilligen. Die Gemeindeammänner-Vereinigung des Kantons Aargau ist mit dem Grundsatz der Transparenz einverstanden, erachtet aber die vorgeschlagenen Regelungen als zu komplex und detailliert.

Beschaffen öffentliche Organe Personendaten nicht bei der betroffenen Person selbst, hat diese keine Kenntnis von der Datenbeschaffung und kann nötigenfalls ihre Rechte nicht wahrnehmen. Heute müssen die Behörden die betroffene Person nur dann über Datenbeschaffungen bei Dritten informieren, wenn es sich um besonders sensitive Daten handelt. Nach dem Entwurf hängt die Informationspflicht nicht mehr von der besonderen Sensitivität der Personendaten ab. Wie schon bisher gibt es zum Schutz der Behörden gemäss § 13 Abs. 2 E-IDAG weitreichende Ausnahmen von der Informationspflicht, namentlich dann, wenn die betroffene Person bereits über die entsprechenden Informationen verfügt, die Beschaffung gesetzlich ausdrücklich vorgesehen ist oder die Information nicht oder nur mit unverhältnismässigem Aufwand möglich ist. In Untersuchungsverfahren der Staatsanwaltschaft richtet sich die Informationspflicht nach den Vorschriften der Strafprozessordnung. Die Bestimmungen des IDAG gelten nur subsidiär. Im Bereich der selbständigen Ermittlung durch die Polizei entfällt die Informationspflicht, wenn dadurch die Ermittlung gefährdet würde (vgl. hierzu die Ausführungen in Ziffer 6.1.1 zu § 13 E-IDAG). In Bezug auf die interinstitutionelle Arbeitsmarktintegration wird mit dieser Vorlage beispielsweise gerade eine entsprechende gesetzliche Grundlage für eine Ausnahme von der Informationspflicht geschaffen (vgl. hierzu Ziffer 6.4.2). Insgesamt ist der Anwendungsbereich somit stark beschränkt, wodurch auch der entstehende Mehraufwand klein bleibt.

5.1.4 Stärkung der Rechte der Betroffenen

Die SVP lehnt die Stärkung der Rechte der Betroffenen ab. Sie bringt vor, das Interesse der Öffentlichkeit müsse immer noch schwerer gewichtet werden als das Interesse des Einzelnen am Schutz seiner Daten. Es dürfe kein Täterschutz betrieben werden. Die AIHK befürchtet hinsichtlich der Strafverfolgung durch die Stärkung der Rechte der Betroffenen zunehmend komplizierte und länger dauernde Verfahren und damit auch einen Anstieg der Kosten.

Werden Personendaten zur Erfüllung der gesetzlichen Aufgabe sowie zu Sicherungs- und Beweiszwecken nicht mehr benötigt, müssen sie gelöscht werden. Dies ist bereits heute gesetzlich vorgeschrieben (vgl. § 21 Abs. 1 IDAG). Neu wird der Anspruch der betroffenen Person, die Löschung widerrechtlich bearbeiteter Personendaten zu verlangen, gesetzlich ausdrücklich festgehalten. Die

Vorschriften über das Archivwesen bleiben weiterhin vorbehalten. Der Löschungsanspruch kann durch Spezialgesetze aber eingeschränkt werden, beispielweise zum Schutz der öffentlichen Sicherheit oder der Nichtbehinderung einer behördlichen oder gerichtlichen Untersuchung, wobei es in diesen Fällen wohl bereits an der Widerrechtlichkeit der Bearbeitung fehlen dürfte. Die Rechte und Ansprüche der betroffenen Personen während hängigen Verfahren der Zivil-, Straf- und Verwaltungsrechtspflege richten sich nach dem anwendbaren Verfahrensrecht. Im Strafverfahren gelten daher die Vorschriften der Strafprozessordnung. Die vorgesehene Änderung wirkt sich daher nicht auf das Strafverfahren aus.

5.1.5 Stärkung der Position der beauftragten Person für Öffentlichkeit und Datenschutz

Die SVP erachtet eine Amtsdauer der beauftragten Person für Öffentlichkeit und Datenschutz von acht Jahren als viel zu lang. Auch den Jungen Grünliberalen erscheint diese Amtszeit als eher lang. Nach Ansicht der AIHK sollte die Position der beauftragten Person für Öffentlichkeit und Datenschutz nur soweit ausgebaut werden, als es die Kompatibilität mit der EU-Datenschutzreform verlange. Die AIHK lehnt eine weitere Stärkung ab und plädiert für eine restriktive Anpassung, da ansonsten personelle und dadurch finanzielle Mehraufwendungen wahrscheinlich seien. Der Verband Steuerfachleute Aargauer Gemeinden ist der Auffassung, dass eine Stärkung der beauftragten Person für Öffentlichkeit und Datenschutz unweigerlich mit neuen Aufgaben verbunden sei. Dazu brauche es aber auch zusätzliche Ressourcen, es sei denn, gewisse Aufgaben würden an die Gemeinden delegiert.

Die Amtsdauer der beauftragten Person für Öffentlichkeit und Datenschutz beträgt bereits nach geltendem Recht acht Jahre. Aufgrund der EU-Datenschutzreform ergibt sich hinsichtlich der Amtsdauer kein Anpassungsbedarf. Die lange Amtsdauer ist zur Wahrung der Unabhängigkeit erforderlich, weil die beauftragte Person durch den Regierungsrat, das heisst eine von ihr zu beaufsichtigenden Behörde, gewählt wird.

Gemäss der EU-Datenschutzreform muss die beauftragte Person für Öffentlichkeit und Datenschutz über wirksame Einwirkungsbefugnisse verfügen. Sie hat das Recht, sich im Rahmen von Vorab-Konsultationen zu Vorhaben zu äussern, Hinweise zu Datenbearbeitungen abzugeben, aber auch zu konkreten Datenbearbeitungen förmliche Empfehlungen abzugeben. Sie verfügt auch über die Kompetenz, bei Verstössen gegen das Datenschutzrecht verbindliche Anordnungen in Form einer Verfügung treffen zu können (zum Beispiel ein widerrechtliches Datenbearbeiten sei einzustellen oder auf eine widerrechtliche Datenbekanntgabe sei zu verzichten). Eine solche verbindliche Anordnung kann nach der Ablehnung einer Empfehlung erlassen werden oder direkt, wenn absehbar ist, dass das öffentliche Organ einer Empfehlung keine Folge leisten wird.

Hinsichtlich der Vorab-Konsultation ist zu erwähnen, dass diese kein wirklich neues Instrument darstellt. Bereits nach geltendem Recht haben die öffentlichen Organe der beauftragten Person für Öffentlichkeit und Datenschutz Datenbearbeitungen vorab zur Kontrolle zu unterbreiten, wenn diese geeignet sind, die Freiheitsrechte betroffener Personen zu verletzen, deren Handlungsfähigkeit und/oder Handlungsmöglichkeiten einzuschränken oder technikbedingte Fehler und/oder Missbräuche zu fördern, und wenn für die Datenbearbeitung keine gesetzliche Grundlage besteht (vgl. § 6 VIDAG). Im Weiteren ist festzuhalten, dass die Aufhebung des Schlichtungsverfahrens gemäss dem vorliegenden Entwurf auch eine Entlastung der beauftragten Person für Öffentlichkeit und Datenschutz mit sich bringt.

5.2 Bemerkungen zum EG StPO und zum PolG

Gemäss CVP darf die Funktion der Datenschutzberatung zu keinem Stellenzuwachs führen. Die FDP.Die Liberalen mahnt zur Beachtung der Verhältnismässigkeit und zum Kostenbewusstsein. Nach Ansicht der SVP ist die Funktion der Datenschutzberatung zu streichen, wenn sie nicht kostenneutral umgesetzt werden könne. Die EVP ist der Meinung, dass bei der Staatsanwaltschaft, der Jugendanwaltschaft und der Kantonspolizei keine der dort ohnehin knappen Ressourcen für die Aufgabe der Datenschutzberatung zulasten des bestehenden Aufgabenbereichs genutzt werden dürfen.

Für die AIHK ist nicht nachvollziehbar, weshalb die Datenschutz-Folgenabschätzung zu den Aufgaben der für den Datenschutz zuständigen Person gehören solle. Der VAG erachtet die Einführung einer Datenschutzberatung pro Organisationseinheit insbesondere für kleinere Organisationseinheiten als problematisch. Die entsprechende Bestimmung sei unter Berücksichtigung der unterschiedlichen Grösse der Organisationseinheiten auszulegen.

Die Funktion einer für den Datenschutz zuständigen Person ist nur im Bereich der Strafverfolgung (Staatsanwaltschaft, der Jugendanwaltschaft und den Polizeikorps) zwingend vorzusehen. Grundsätzlich liegt es im Bereich der Strafverfolgung in der Kompetenz der jeweiligen Organisationseinheit, wie viele und welche Mitarbeitenden mit dieser zusätzlichen Aufgabe betraut und entsprechend geschult werden. Bei der Kantonspolizei werden die gemäss Datenschutzreform definierten Aufgaben der Datenschutzberatung heute schon zu einem grossen Teil von den entsprechenden Fachstellen der Kantonspolizei (vor allem durch den Rechtsdienst KAPO und die Abteilung IT KAPO) wahrgenommen. Insbesondere ist dort das erforderliche Fachwissen hinsichtlich Art der durchgeführten Datenverarbeitung und des erforderlichen Schutzes für die verarbeiteten personenbezogenen Daten bereits vorhanden. Eine für den Datenschutz zuständige Person kann zudem für mehrere zuständige Behörden gemeinsam ernannt werden, wobei deren Organisationsstruktur und Grösse Rechnung getragen wird (Art. 32 Abs. 3. der Richtlinie [EU] 2016/680).

Ein gewisser Mehraufwand ist durch die neu systematisch durchzuführenden Datenschutz-Folgenabschätzungen nicht auszuschliessen, wobei noch einmal festzuhalten ist, dass eine Datenschutz-Folgenabschätzung nur bei neuen geplanten Vorhaben für eine Personendatenbearbeitung oder wenn die Personendatenbearbeitungen mit neuen technischen Methoden durchgeführt werden notwendig ist (vgl. Ziffer 5.1 hiervor). Der Mehraufwand dürfte aber überschaubar bleiben und kann durch die bereits heute damit beschäftigten Fachstellen aufgefangen werden. Es geht nun vor allem darum, den Wissensstand und die entsprechenden Abläufe aufgrund der Neuerungen zu ergänzen. Die Regionalpolizeien erhalten diesbezüglich auch den notwendigen Support durch die Kantonspolizei.

Auch und insbesondere im Bereich der Strafverfolgung ist jedes öffentliche Organ neu verpflichtet, eine Datenschutz-Folgenabschätzung durchzuführen, wenn eine vorgesehene Datenbearbeitung zu einem erhöhten Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person führt. Es erscheint sachgerecht und folgerichtig, diese Aufgabe bei der Staatsanwaltschaft, der Jugendanwaltschaft und den Polizeikorps der dort zwingend vorzusehenden Funktion der Datenschutzberatung zu übertragen. Im Übrigen gehört auch gemäss Art. 34 der Richtlinie (EU) 2016/680 die Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung zu den Aufgaben der für den Datenschutz zuständigen Person.

5.3 Bemerkungen zum EG AVIG/AVG

Die Piratenpartei ist der Ansicht, dass mit der Änderung von § 9a E-EG AVIG/AVG die Datensicherheit nicht mehr gewährleistet sei. Die Grünen erachten den geplanten Datenaustausch zwischen Arbeitslosenversicherung (ALV), Invalidenversicherung (IV) und Sozialhilfe zur Wiedereingliederung in den Arbeitsmarkt als grundsätzlich sinnvoll. Von einer Blankovollmacht zur Weitergabe sei aber abzusehen. Nicht alle schützenswerten Personendaten seien für die Arbeitsmarkintegration notwendig. Religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten sowie Daten über die Intimsphäre dürften nicht bekannt gegeben werden.

Nach wie vor dürfen nur die für die Arbeitsmarktintegration des jeweiligen Stellensuchenden tatsächlich benötigten Daten bekannt gegeben werden. Für die im Hinblick auf die Arbeitsmarktintegration zusammenarbeitenden Behörden wird durch die neue Bestimmung somit keine Blankovollmacht ausgestellt. Im Einzelfall kann es aber durchaus vorkommen, dass auch höchstpersönliche Daten für die Integration in den Arbeitsmarkt von Bedeutung sein können. Durch die vorgesehene Gesetzesbestimmung wird der Regierungsrat verpflichtet, die für die Arbeitsmarktintegration nötigen Perso-

nendaten, die im Einzelfall ausgetauscht werden dürfen, auf dem Verordnungsweg zu konkretisieren. Dadurch wird die Transparenz über die Reichweite der erlaubten Datenbearbeitung für die Betroffenen gewährleistet.

6. Erläuterungen zu einzelnen Gesetzesbestimmungen

6.1 Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (IDAG)

6.1.1 Einzelne Bestimmungen

§ 2 Geltungsbereich

§ 2 Abs. 2 und 2bis (geändert)

[2] Richterliche Behörden fallen nicht in den Bereich der Aufgaben, Befugnisse und Pflichten der beauftragten Person für Öffentlichkeit und Datenschutz gemäss den §§ 17b, 17c sowie 31–33 dieses Gesetzes. […].

[2bis] Die Rechte und Ansprüche der betroffenen Personen während hängigen Verfahren der Zivil-, Straf- und Verwaltungsrechtspflege richten sich nach dem anwendbaren Verfahrensrecht.

Für richterliche Behörden galt das IDAG bisher nur, soweit diese Verwaltungsaufgaben erfüllten. Anders als nach bisherigem Recht dürfen keine generellen Ausnahmen vom Geltungsbereich der datenschutzrechtlichen Bestimmungen mehr vorgenommen werden. Im Bereich der Aufsicht ist hingegen eine Ausnahme von der Aufsicht durch die Beauftragte Person für Öffentlichkeit und Datenschutz vorzusehen. Anders als bisher sind die richterlichen Behörden auch von der Aufsicht ausgenommen, wenn sie Verwaltungsaufgaben wahrnehmen. Dies ist im Hinblick darauf zu betrachten, dass die beauftragte Person im Entwurf neu die Kompetenz erhält, Verfügungen gegenüber öffentlichen Organen (des Kantons) zu erlassen. Dadurch bestünde gegenüber den Gerichten die Gefahr, dass deren Unabhängigkeit und die Gewaltenteilung beeinträchtigt würden. Darüber hinaus ist das Verwaltungsgericht Beschwerdeinstanz für Verfügungen der beauftragten Person. Daher könnte es aufgerufen sein, einen Beschwerdeentscheid in eigener Sache zu fällen. Aus Gründen der Unabhängigkeit ist es daher nötig, dass die Gerichte eine eigenständige Form der Datenschutzaufsicht pflegen, um den Anforderungen der Richtlinie (EU) 2016/680 und dem E-SEV 108 zu genügen.

Konsequenterweise werden die Gerichte neben der Aufsicht auch von der Vermittlungs- und Beratungstätigkeit durch die beauftragte Person ausgenommen.

Für hängige Zivil-, Straf- und verwaltungs- oder verwaltungsgerichtliche Verfahren können nach dem Gesagten keine Ausnahmen vom IDAG mehr vorgesehen werden. Das bedeutet nicht, dass die Prozessordnungen nicht mehr gelten: Sie behalten als bereichsspezifisches Datenschutzrecht (wie die anderen Fachgesetze, zum Beispiel das Polizeigesetz, das Schulgesetz vom 17. März 1981 oder das Bundesgesetz über den allgemeinen Teil des Sozialversicherungsrechts [ATSG] vom 6. Oktober 2000) weiter ihre Gültigkeit (vgl. dazu BEAT RUDIN, Überholte Ausnahmen beim Geltungsbereich, digma 2016, 122 ff.). Die Regelungen zum Beispiel der Strafprozessordnung gelten weiterhin, aber auch die Grundsätze des IDAG (zum Beispiel die Regeln zur verantwortlichen Behörde, zur Informationssicherheit usw.). Auch die unabhängigen Justizbehörden haben eine Datenschutz-Folgenabschätzung vorzunehmen, wenn eine vorgesehene Datenbearbeitung voraussichtlich zu einem hohen Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person führen wird. Ergibt die Folgenabschätzung, dass effektiv ein hohes Risiko besteht, dass nicht durch geeignete Massnahmen eingedämmt werden kann, besteht jedoch keine Pflicht zur Vorab-Konsultation der beauftragten Person für Öffentlichkeit und Datenschutz, weil die Konsultationspflicht im Zusammenhang mit deren Aufsichtstätigkeit steht.

Satz 2 von Abs. 2 des geltenden Rechts gibt der Justizleitung die Ermächtigung, die Einsichtnahme in die gerichtsintern archivierten Akten zu regeln. Davon hat die Justizleitung mit der Regelung von § 9 Abs. 1 lit. b des Reglements der Justizleitung über die Information der Öffentlichkeit und die Publikation von Entscheiden (Informationsreglement) vom 19. Februar 2016 und § 21 des Reglements der Justizleitung über die Archivierung der Akten der Gerichte und der Schlichtungsbehörden des Kantons Aargau vom 21. Dezember 2012 auch Gebrauch gemacht. Der Justizleitung fehlt demgegenüber heute eine spezifische Ermächtigung, die gerichtsinterne Archivierung zu regeln, da es sich dabei um eine dem IDAG auch heute schon unterstellte Verwaltungsaufgabe der Gerichte handelt. Diese Ermächtigungsnorm der Justizleitung im IDAG wird aufgrund des sachlichen Zusammenhangs in § 21 ergänzt (vgl. dazu Bemerkungen zu § 21 E-IDAG). Inhaltlich umfasst die neue Norm auch die Ermächtigung, welche heute in Satz 2 von Absatz 2 enthalten ist. Daher kann Absatz 2 Satz 2 gestrichen werden.

Um Kollisionen zwischen einerseits den verfahrensrechtlichen und andererseits den öffentlichkeits- und datenschutzrechtlichen Informationsansprüchen zu vermeiden, wird vorgesehen, dass sich die Rechte und Ansprüche der betroffenen Personen während hängigen Verfahren nach dem anwendbaren Verfahrensrecht richten. Enthält dieses keine oder aus datenschutzrechtlicher Sicht keine genügenden Regelungen, gelangt das IDAG zur Anwendung. "Betroffen" sind alle Personen, über die Daten bearbeitet werden, das heisst auch diejenigen, deren Daten nicht verändert, sondern zur Kenntnis genommen werden, zum Beispiel beim Beizug alter Verfahrensakten. Die übrigen Bestimmungen, zum Beispiel die Pflicht zur Gewährleistung der Datensicherheit durch technische und organisatorische Massnahmen (§ 12 IDAG) oder der Sicherstellung des Datenschutzes bei Outsourcing (§ 18 IDAG) sind auch auf Gerichte und im Rahmen von hängigen Verfahren anwendbar.

§ 2 Abs. 3 (geändert)

[3] Soweit ein öffentliches Organ am wirtschaftlichen Wettbewerb teilnimmt und dabei privatrechtlich sowie nicht in Erfüllung einer öffentlichen Aufgabe handelt, sind auf seine Datenbearbeitungen die Bestimmungen des Bundesgesetzes über den Datenschutz (DSG) vom 19. Juni 1992 anwendbar. Die Aufsicht richtet sich nach diesem Gesetz. Die Bestimmungen über das Öffentlichkeitsprinzip finden keine Anwendung.

Es bleibt zulässig, für das Datenbearbeiten privatrechtlich handelnder Organe die Regeln des Bundesdatenschutzgesetzes für anwendbar zu erklären. Für die kantonalen und kommunalen öffentlichen Organe, welche privatrechtlich und nicht in Erfüllung einer öffentlichen Aufgabe handeln, bleibt – analog zur Regelung beim Bund (Art. 23 Abs. 2 DSG und Art. 33 Abs. 2 VE-DSG) – die kantonale Aufsichtsbehörde zuständig.

§ 3 Begriffe

§ 3 Abs. 1 lit. d und e (geändert)

d) Personendaten: Daten, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen,
e) Betroffene Person: Natürliche Person, über die Personendaten bearbeitet werden,

Anders als die internationalen Vorgaben (und die meisten europäischen Staaten) schützen die schweizerischen Datenschutzgesetze bisher nicht nur natürliche, sondern auch juristische Personen. Art. 3 lit. b VE-DSG will die juristischen Personen aus dem Schutzbereich des DSG streichen. Die Kantone sind nicht verpflichtet, diese Änderung nachzuvollziehen. Eine zur Bundesregelung unterschiedliche Regelung erscheint jedoch nicht sinnvoll. Es bleibt ein umfassender Schutz für juristische Personen bestehen, wie er durch die Art. 28 ff. ZGB (Persönlichkeitsverletzungen wie beispielsweise Rufschädigung), das Bundesgesetz über das Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz, URG) vom 9. Oktober 1992, das UWG oder durch die Bestimmungen zum Schutz von Berufs-, Geschäfts- und Fabrikationsgeheimnissen sowie Art. 13 BV auf Verfassungsebene gewährleistet wird.

§ 3 Abs. 1 lit. f (geändert)

f) Profiling: jede Auswertung von Daten, um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen, insbesondere bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, Intimsphäre oder Mobilität.

Die Richtlinie (EU) 2016/680 regelt neu das Profiling als besondere, persönlichkeitsgefährdende Art des Bearbeitens von Personendaten, das denselben Anforderungen genügen muss wie das Bearbeiten besonders schützenswerter Personendaten. Dies muss auch in die kantonalen Gesetze übernommen werden. Zur einfacheren Verständlichkeit wird "Profiling" in die Begriffsdefinitionen aufgenommen. Der Begriff des "Persönlichkeitsprofils", der an die Art der Daten anknüpfte – während "Profiling" auf die Art des Bearbeitens Bezug nimmt – kann gestrichen werden. Bei den Grundsätzen des Datenbearbeitens sind die entsprechenden Anpassungen vorzunehmen.

Bemerkung zu § 3 Abs. 1 lit. k

Das geltende Recht definiert in § 3 Abs. 1 lit. k besonders schützenswerte Personendaten wie folgt: "Daten, bei denen aufgrund ihrer Bedeutung, des Zusammenhangs, Zwecks oder der Art der Bearbeitung, der Datenkategorie oder anderer Umstände eine besondere Gefahr der Persönlichkeitsverletzung besteht." § 7 VIDAG enthält eine nicht abschliessende Aufzählung der besonders schützenswerten Daten:

a) die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Tätigkeiten
b) die Gesundheit, die Intimsphäre oder die ethnische Zugehörigkeit
c) Massnahmen der sozialen Hilfe
d) administrative oder strafrechtliche Verfolgungen und Sanktionen.

Neu fallen Daten über das Sexualleben oder die sexuelle Orientierung, genetische und biometrische Daten ausdrücklich in diese Kategorie. Weil die generelle Umschreibung der besonders schützenswerten Personendaten im Gesetz auch diese besonderen Daten umfasst, können sie im Verordnungsrecht explizit genannt werden.

§ 3 Abs. 1 lit. i (aufgehoben)

Der Begriff der Datensammlung war in Zusammenhang mit der Pflicht der öffentlichen Organe, ein Verzeichnis der Datensammlungen zu führen, relevant. Er hat zunehmend an Schärfe verloren, da aufgrund der Suchmöglichkeiten in elektronischen Dokumenten immer nach Daten einer bestimmten Person gesucht werden kann und die Grenzen einer Datensammlung nicht mehr gezogen werden können. Die Richtlinie (EU) 2016/680 verlangt für den justiziellen und polizeilichen Bereich, dass ein Register der Datenbearbeitungen zu führen ist und knüpft damit praxisbezogener an die Tätigkeit an; eine entsprechende Regelung erfolgt im EG StPO und im Polizeigesetz. Für die anderen öffentlichen Organe erweist sich die Führung eines Registers als entbehrlich, wurde doch im Zeitraum von zehn Jahren bei der beauftragten Person ein einziges Mal nach einem Registereintrag gefragt. Der Aufwand für die Registerführung rechtfertigt sich nicht mehr. Die bereits früher von den Behörden für die Registerführung erarbeiteten Angaben können aber direkt als Grundlage für die Umsetzung der Informationspflichten dienen.

§ 6 Amtliche Dokumente mit Personendaten Dritter

§ 6 Abs. 2 und 3 (geändert)

[2] Ist dies nicht oder nur mit unverhältnismässigem Aufwand möglich, wird der Zugang gewährt, soweit ein überwiegendes Interesse an der Bekanntgabe des Dokuments besteht.

[3] Die Absätze 1 und 2 gelangen nicht zur Anwendung, wenn

a) die Betroffenen die Personendaten selbst öffentlich zugänglich machen,
b) der öffentliche Zugang offensichtlich im Interesse der Betroffenen liegt, oder
c) ein überwiegendes Interesse an der Bekanntgabe der Personendaten besteht.

Nach geltendem Recht ist gestützt auf das Öffentlichkeitsprinzip eine Einsicht in amtliche Dokumente nicht möglich, wenn diese nicht anonymisierbare Personendaten enthalten. Dies ist vor allem dann der Fall, wenn selbst bei Schwärzung der Namen bekannt oder eruierbar ist, welche Personen betroffen sind. Eine Datenbekanntgabe ist nur in den speziellen Fällen von § 15 IDAG zulässig, das heisst nur bei Vorliegen einer Rechtsgrundlage oder mit Einwilligung der betroffenen Person. Ob ein überwiegendes öffentliches Interesse an der Einsicht besteht, ist nach geltendem Recht irrelevant, wenn das Dokument nicht anonymisierbar ist (Verwaltungsgerichtsentscheid vom 28. Juni 2016 in Sachen Beauftragte für Öffentlichkeit und Datenschutz ca. Regierungsrat des Kantons Aargau).

Am 1. Juni 2014 trat für die Schweiz die AK in Kraft, welche – neben der Beteiligung der Öffentlichkeit an Entscheidungsverfahren und dem Zugang zu Gerichten in Umweltangelegenheiten – den Zugang zu Umweltinformationen zum Gegenstand hat und die Vertragsparteien verpflichtet, diesen sicherzustellen (Art. 4 Abs. 1 AK). Der Begriff der "Informationen über die Umwelt" wird in Art. 2 Abs. 3 AK präzisiert. Darunter fallen unter anderem sämtliche Informationen über Faktoren wie Lärm sowie Tätigkeiten oder Massnahmen, die sich auf den Zustand von Umweltbestandteilen wie Luft und Atmosphäre, Wasser, Boden, Land, Landschaft und natürliche Lebensräume, die Artenvielfalt und ihre Bestandteile sowie die Wechselwirkungen zwischen diesen Bestandteilen auswirken oder wahrscheinlich auswirken. Ein Gesuch um Einsicht in solche Informationen kann abgelehnt werden, wenn die Einsicht negative Auswirkungen auf die Vertraulichkeit personenbezogener Daten hätte (Art. 4 Abs. 4 lit. f AK). Anders als nach dem aargauischen Öffentlichkeitsprinzip ist dieser Ablehnungsgrund eng auszulegen und es ist eine Abwägung zwischen dem öffentlichen Interesse an der Bekanntgabe und dem privaten Geheimhaltungsinteresse vorzunehmen (Art. 4 Abs. 4 AK). Dieses muss unter Berücksichtigung des öffentlichen Interesses an der Bekanntgabe der Umweltinformation im konkreten Fall schützenswert sein. Dies wird allgemein vom Grad des Sozialbezugs, den die jeweiligen personenbezogenen Informationen aufweisen, abhängig gemacht. So scheiden stark persönlichkeitsorientierte Angaben wie etwa Informationen über private Lebensumstände, Neigungen und Interessen, aber auch Personalakten sowie Angaben über das Einkommen von einer Offenlegung grundsätzlich aus (DANIEL R. KLEIN, Umweltinformation im Völker- und Europarecht, Tübingen 2011, Seiten 370 f.). Zudem können nur Angaben mit Bezug zu einer natürlichen Person der Einsicht entgegenstehen (KLEIN, am angegebenen Ort, Seite 369 mit Hinweisen). Die Anpassung ist aus den in Ziffer 2.4 aufgeführten Gründen nicht auf den Umweltbereich zu beschränken; ein überwiegendes öffentliches Interesse kann etwa bei Verträgen Privater mit der öffentlichen Hand bestehen (vgl. auch Ziffer 2.4 hiervor). Enthält ein Dokument Personendaten, die nicht anonymisiert werden können, bleibt eine Bekanntgabe gestützt auf das Öffentlichkeitsprinzip weiterhin unzulässig, wenn nur private Interessen an der Einsicht bestehen. Das Öffentlichkeitsprinzip dient der Herstellung von Transparenz über das Verwaltungshandeln und der Verbesserung der Kontrolle durch die Öffentlichkeit. Eine Einsichtnahme gestützt auf andere Bestimmungen als § 6 E-IDAG, etwa § 15 IDAG, Einsicht in das Grundbuch (Art. 970 ZGB) oder bei Bestehen schützenswerter Interessen an der Einsicht (gemäss der Rechtsprechung zu Art. 29 Abs. 2 BV) bleibt unverändert. In diesen Fällen wird in der Regel nur einer bestimmten Person oder einer bestimmten Behörde Einsicht gewährt, während im Öffentlichkeitsrecht jedermann der Zugang gestattet werden muss.

Enthält ein amtliches Dokument Personendaten, ist wie bei allen amtlichen Dokumenten vorab zu prüfen, ob dem Zugang spezielle Gesetzesbestimmungen oder überwiegende öffentliche oder private Interessen entgegenstehen (§ 5 Abs. 3 IDAG). § 6 E-IDAG konkretisiert die durch die zuständige Behörde vorzunehmende Prüfung für den Umgang mit Personendaten im betreffenden Dokument.

§ 8 Grundsatz

§ 8 Abs. 2 (geändert)

[2] Die Bearbeitung von besonders schützenswerten Personendaten und das Profiling sind nur zulässig, wenn

Vgl. die Ausführungen zu § 3 Abs. 1 lit. f.

§ 8 Abs. 2 lit. b (geändert)

b) dies für die Erfüllung einer klar umschriebenen gesetzlichen Aufgabe erforderlich ist, oder

Die Bearbeitung von Personendaten, die besonders persönlichkeitsnah sind und ein grosses Stigmatisierungs- oder Diskriminierungspotenzial besitzen (besonders schützenswerte Personendaten), stellt einen schweren Eingriff in das informationelle Selbstbestimmungsrecht (Datenschutzrecht) dar und verlangt nach qualifizierten Voraussetzungen. Nach der bundesgerichtlichen Rechtsprechung zu Art. 36 Abs. 1 BV wird eine unmittelbare formell-gesetzliche Grundlage verlangt oder es werden an die Erforderlichkeit zur Erfüllung einer Aufgabe sowie an die gesetzliche Umschreibung der Aufgabe höhere Anforderungen gestellt (mittelbare gesetzliche Grundlage). Weder Art. 36 Abs. 1 BV noch die Richtlinie (EU) 2016/680 setzen voraus – wie in § 8 Abs. 2 lit. b des geltenden Gesetzes verlangt –, dass es sich um einen Einzelfall handeln muss. Die Praxis hat gezeigt, dass eine unmittelbare gesetzliche Grundlage ("darf besonders schützenswerte Personendaten bearbeiten") keinen höheren Schutz bewirkt als eine mittelbare gesetzliche Grundlage. Je klarer die Aufgabendefinition im Gesetz erfolgt, desto eindeutiger lässt sich ableiten, welche Datenbearbeitungen zur Erfüllung geeignet und erforderlich sind. Die Grundlage gemäss § 8 Abs. 2 lit. a und b werden daher als gleichwertig betrachtet und die Reduktion auf den Einzelfall in Litera b gestrichen.

§ 8 Abs. 3 (aufgehoben)

Diese Bestimmung ist die Grundlage für die Vorabkontrolle, welche in der VIDAG näher umschrieben wird. Nachdem die Vorabkontrolle durch die Vorabkonsultation ersetzt und auf Gesetzesstufe geregelt wird (vgl. § 17 E-IDAG), ist § 8 Abs. 3 zu streichen.

§ 12 Datensicherheit

§ 12 Abs. 2 (geändert)

[2] Das verantwortliche öffentliche Organ ist verpflichtet, den Nachweis zu erbringen, dass es die Datenschutzbestimmungen einhält. Der Regierungsrat regelt die Einzelheiten durch Verordnung.

Mehrfach wird in den neuen Rechtsgrundlagen verlangt, dass das verantwortliche öffentliche Organ oder die Auftragsdatenbearbeitenden die Einhaltung der Datenschutzbestimmungen nachweisen können muss respektive müssen. Dieser Nachweis kann in einem Datenschutzmanagementsystem (DSMS) erbracht werden. DSMS basieren auf den ISO-Standards des Qualitätsmanagements (ISO 9001) und der Informationssicherheit (ISO 27001 usw.). Verzichtet das öffentliche Organ auf eine Zertifizierung, ist festzulegen, welche Dokumente notwendig sind, um diesen Nachweis zu erbringen. Dies kann auf Verordnungsstufe geschehen. Grösserer Mehraufwand für die öffentlichen Organe ist nicht zu befürchten, sind diese doch schon nach geltendem Verordnungsrecht verpflichtet, gestützt auf eine Risikoabschätzung technische und organisatorische Massnahmen zur Wahrung der Datensicherheit zu treffen (§ 4 Abs. 1 und 2 VIDAG) und in Reglementen ihr Datensicherheitskonzept festzulegen (§ 4 Abs. 3 VIDAG). Für die Vorabkontrolle von Datenbearbeitungen, die geeignet sind, die Freiheitsrechte Betroffener zu verletzen, technikbedingte Fehler und/oder Missbräuche zu fördern (§ 6 Abs. 1 VIDAG), wird schon jetzt die Vorlage eines Informationssicherheits- und Datenschutzkonzepts verlangt.

§ 13 Informationspflicht

§ 13 Abs. 1, 2 (geändert) und 3 (neu)

[1] Das öffentliche Organ beschafft die Personendaten nach Möglichkeit bei der betroffenen Person selbst. Es informiert diese über jede Beschaffung von Daten. Die Informationspflicht gilt auch, wenn die Daten bei Dritten beschafft werden. Die Information umfasst insbesondere Angaben über

a) das verantwortliche öffentliche Organ samt Kontaktdaten,
b) die bearbeiteten Daten oder die Kategorien der bearbeiteten Daten,
c) die Rechtsgrundlage und den Zweck des Bearbeitens,
d) die Empfängerinnen und Empfänger der Daten oder deren Kategorien, falls die Daten Dritten bekanntgegeben werden und
e) die Rechte der betroffenen Person.

[2] Die Informationspflicht entfällt, wenn

a) die betroffene Person bereits über die Angaben gemäss Absatz 1 verfügt,
b) das Bearbeiten der Personendaten gesetzlich ausdrücklich vorgesehen ist oder
c) die Information nicht oder nur mit unverhältnismässigem Aufwand möglich ist.

[3] Die Übermittlung der Informationen kann unter denselben Voraussetzungen eingeschränkt werden wie die Auskunft über die eigenen Personendaten (§ 25).

Transparenz bezüglich der Bearbeitung von Personendaten ist eines der Kernanliegen des Datenschutzrechts. Das Transparenzgebot verlangt unter anderem bei jeder Beschaffung von Personendaten eine aktive Information der Betroffenen. Werden die Daten bei Dritten beschafft, gilt die Informationspflicht nicht mehr nur beim Beschaffen von besonders schützenswerten Personendaten. Der Katalog der abzugebenden Informationen muss zur Verbesserung der Transparenz und des Rechtsschutzes erweitert werden um:

- das verantwortliche öffentliche Organ (samt Kontaktdaten)
- die bearbeiteten Daten oder die Kategorien der bearbeiteten Daten
- die Rechtsgrundlage des Bearbeitens
- die Rechte der betroffenen Person.

Werden die Daten systematisch erhoben (zum Beispiel auf einem Anmelde- oder Gesuchsformular, auf Papier oder online), können die Angaben auf dem Formular angebracht werden. Bei anderen Datenbeschaffungen sind die betroffenen Personen individuell zu informieren, sofern und soweit nicht eine Einschränkung zulässig ist. Dies ist dann der Fall,

- wenn die betroffene Person bereits über die notwendigen Informationen verfügt, insbesondere, wenn sie in einer früheren Phase der Beschaffung bereits informiert wurde,
- wenn die Beschaffung oder Bekanntgabe der Daten gesetzlich ausdrücklich vorgesehen ist, das heisst, wenn die betroffene Person aus den gesetzlichen Grundlagen mit hinreichender Genauigkeit herauslesen kann, welche Daten über sie zu welchem Zweck bearbeitet werden, oder
- wenn die Information der betroffenen Person nicht oder nur mit unverhältnismässigem Aufwand möglich ist.

Die Informationspflicht der öffentlichen Organe beruht auf einem Informationsanspruch der betroffenen Person. In hängigen Verfahren der Zivil-, Straf- und Verwaltungsrechtspflege richtet sie sich daher nach dem anwendbaren Verfahrensrecht und nicht nach § 13 E-IDAG (vgl. § 2 Abs. 2^{bis} E-IDAG). Werden beispielsweise in einem Beschwerdeverfahren betreffend Baubewilligung Akten abgeschlossener Baubewilligungsverfahren beigezogen, ist in Anwendung der entsprechenden Verfahrensregeln zu entscheiden, ob Personen, deren Daten in den beigezogenen Akten enthalten sind, informiert werden müssen. Im Untersuchungsverfahren der Staatsanwaltschaft richtet sich die Informationspflicht nach den Vorschriften der Strafprozessordnung. Bei abgeschlossenen Verfahren gilt

die Amts- und Rechtshilfe als Grundlage für die Bekanntgabe archivierter Daten, mit der Folge, dass eine solche Bekanntgabe die Informationspflicht nicht (mehr) auslöst.

Ausserdem kann die Information im gleichen Mass eingeschränkt (ganz oder teilweise eingeschränkt oder aufgeschoben werden) wie der Zugang zu den eigenen Personendaten im Rahmen des Rechts auf Auskunft (§ 25 IDAG). Im Bereich der selbstständigen Ermittlung durch die Polizei entfällt die Informationspflicht, wenn dadurch der Ermittlungszweck gefährdet würde.

§ 14 Bekanntgabe an öffentliche Organe

§ 14 Abs. 1 (geändert) und 2 (aufgehoben)

[1] Personendaten können unter Vorbehalt besonderer Geheimhaltungsbestimmungen inner- und ausserkantonalen öffentlichen Organen bekannt gegeben werden, wenn

a) die Voraussetzungen gemäss den §§ 8 und 9 erfüllt sind oder

b) dies zur Erfüllung einer klar umschriebenen gesetzlichen Aufgabe des datenempfangenden Organs erforderlich ist. Vorbehalten bleiben besondere Geheimhaltungsbestimmungen.

[2] Aufgehoben.

§ 14 regelt unter dem Randtitel "Bekanntgabe an öffentliche Organe" die Amtshilfe. Sie ist neu auch dann zulässig, wenn sie nicht nur im Einzelfall erfolgt, das heisst auch dann, wenn ein öffentliches Organ regelmässig Personendaten bei einem anderen öffentlichen Organ beschaffen muss. Die Voraussetzungen gemäss §§ 8 und 9 IDAG müssen weiterhin gegeben sein.

Amtshilfe ist erforderlich, wenn die Daten für die Aufgabenerfüllung der datenempfangenden Behörde benötigt werden. Hier ist eine Klärung gegenüber dem geltenden Gesetzeswortlaut anzubringen. Der Datenbekanntgabe dürfen aber keine besonderen Geheimhaltungsvorschriften wie das medizinische Berufsgeheimnis oder sozialversicherungsrechtliche Geheimhaltungspflichten entgegenstehen.

Die Voraussetzungen für eine Bekanntgabe folgen denjenigen für die Bearbeitung von Personendaten gemäss § 8 IDAG und sind ebenfalls anzupassen, das heisst, dass die Beschaffung von besonders schützenswerten Personendaten zulässig ist, wenn eine unmittelbare oder mittelbare gesetzliche Grundlage oder die Einwilligung der betroffenen Person die Beschaffung rechtfertigen. Das Erfordernis, dass besonders schützenswerte Personendaten nur bekanntgegeben werden dürfen, wenn ein (formelles) Gesetz dies ausdrücklich erlaubt, wird aufgehoben.

§ 14 Abs. 2 regelt nur die datenschutzrechtliche Voraussetzung für die Amtshilfe; ob die ersuchte Behörde zur Leistung von Amtshilfe verpflichtet ist, ergibt sich aus dem allgemeinen Verwaltungsrecht. Die Bekanntgabe an öffentliche Organe wird neu als "kann"-Bestimmung formuliert.

§ 17 Abrufverfahren (aufgehoben)

§ 17 Abs. 1 und 2 (aufgehoben)

Eine spezielle Regelung des Abrufverfahrens ist nicht mehr erforderlich. Die gesetzliche Grundlage muss bereits nach den allgemeinen Vorschriften genügend klar sein, um einen Datenbezug durch Dritte ohne Einwilligung des Datenherrn im Einzelfall zu rechtfertigen. Aufgrund der vielfältigen technischen Möglichkeiten der Einschränkung des Zugriffs auf Informationssysteme haben sich bei der Feststellung, ob es sich um ein Abrufverfahren gemäss § 17 IDAG handelt, stets Abgrenzungsprobleme ergeben. Die Anforderungen an eine gesetzliche Grundlage sollen sich konkret nach der Schwere des Eingriffs richten und technologieneutral bleiben.

§ 17a Datenschutz-Folgenabschätzung (neu)

§ 17a Abs. 1 und 2 (neu)

[1] Führt die vorgesehene Datenbearbeitung voraussichtlich zu einem erhöhten Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person, muss das öffentliche Organ vorgängig eine Datenschutz-Folgenabschätzung durchführen.

[2] Die Datenschutz-Folgenabschätzung umschreibt die geplante Bearbeitung, die Risiken für die Persönlichkeit und die Grundrechte der betroffenen Person sowie die Massnahmen, die vorgesehen sind, um das Risiko einer Verletzung der Persönlichkeit und der Grundrechte der betroffenen Person zu verringern.

Neu verlangen die übergeordneten Rechtsgrundlagen eine Datenschutz-Folgenabschätzung durch das verantwortliche öffentliche Organ, wenn die vorgesehene Bearbeitung voraussichtlich zu einem erhöhten Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person führt. Das verantwortliche öffentliche Organ ist dadurch verpflichtet, eine Prognose darüber zu machen, welche Folgen eine geplante Datenbearbeitung für die betroffene Person hat. Diese Abschätzung enthält zumindest eine allgemeine Beschreibung der geplanten Bearbeitungsvorgänge, eine Bewertung der in Bezug auf die Persönlichkeit und die Grundrechte der betroffenen Personen bestehenden Risiken sowie eine Darstellung und Bewertung der geplanten Abhilfemassnahmen, Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz der Persönlichkeit und der Grundrechte der betroffenen Personen sichergestellt und der Nachweis erbracht werden soll, dass dieses Gesetz eingehalten wird. Die Datenschutz-Folgenabschätzung ist im Grund genommen nichts anderes als die Vorbereitung des verantwortlichen öffentlichen Organs, damit es die Voraussetzungen für den Nachweis der Einhaltung der Datenschutzvorschriften erbringen kann. Ausserdem beschlägt sie dieselben Punkte, die bei Vorhaben, die nach dem Ergebnis der Datenschutz-Folgenabschätzung zu einem erhöhten Risiko für die Persönlichkeit und die Grundrechte der betroffenen Personen führen, für eine Vorabkonsultation erarbeitet werden müssen.

§ 17b Vorab-Konsultation (neu)

§ 17b Abs. 1, 2, 3 und 4 (neu)

[1] Das öffentliche Organ gibt der beauftragten Person für Öffentlichkeit und Datenschutz Kenntnis, wenn

a) aus der Datenschutz-Folgenabschätzung hervorgeht, dass die Bearbeitung ein erhöhtes Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person zur Folge hätte, oder
b) die Form der Bearbeitung insbesondere bei Verwendung neuer Technologien, Mechanismen oder Verfahren ein erhöhtes Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person zur Folge hätte.

[2] Die beauftragte Person für Öffentlichkeit und Datenschutz gibt innert zwei Monaten nach Erhalt aller erforderlichen Informationen eine Empfehlung gemäss § 32 Abs. 3 ab, wenn die geplante Bearbeitung Vorschriften über den Datenschutz verletzen würde. Sie kann die Frist um einen Monat verlängern.

[3] Die beauftragte Person für Öffentlichkeit und Datenschutz kann auf Antrag des verantwortlichen öffentlichen Organs oder von Amtes wegen die versuchsweise Durchführung der Datenbearbeitung empfehlen, wenn die praktische Umsetzung eine Testphase zwingend erforderlich macht, weil die Erfüllung der Aufgabe

a) technische Neuerungen erfordert, deren Auswirkungen zunächst evaluiert werden müssen, oder
b) bedeutende organisatorische oder technische Massnahmen erfordert, deren Wirksamkeit zunächst geprüft werden muss, insbesondere die Zusammenarbeit zwischen öffentlichen Organen.

[4] Das verantwortliche öffentliche Organ hat die vorgesehene Datenbearbeitung spätestens zwei Jahre nach der Empfehlung gemäss Absatz 3 erneut zur Vorab-Konsultation vorzulegen.

Die Richtlinie (EU) 2016/680 wie auch die Datenschutz-Grundverordnung sehen vor, dass bestimmte Vorhaben der Datenschutzaufsicht vorab zur Konsultation (nach dem früheren Recht: "Vorabkontrolle", § 6 VIDAG) zu unterbreiten sind. Neben den in § 17a Abs. 1 lit. a und b E-IDAG vorgesehenen Massnahmen verlangt die Richtlinie (EU) 2016/680 auch, dass Rechtsetzungsvorhaben, welche das Bearbeiten von Personendaten betreffen, der Datenschutzaufsicht mit der Möglichkeit zur Stellungnahme vorzulegen sind. Diese Pflicht ist im geltenden Recht bereits enthalten (§ 31 Abs. 1 lit. c IDAG, § 21 Abs. 3 VIDAG) und erfordert keine Anpassungen.

Bei anderen als Rechtsetzungsvorhaben kann die beauftragte Person für Öffentlichkeit und Datenschutz Empfehlungen gemäss § 32 Abs. 3 E-IDAG abgeben, wenn die geplante Datenbearbeitung gegen Datenschutzbestimmungen verstossen würde, insbesondere, weil das verantwortliche öffentliche Organ die Risiken für die Persönlichkeit und die Grundrechte nicht hinreichend ermittelt oder nicht genügend eingedämmt hat. Gemäss Abs. 2 gibt die beauftragte Person für Öffentlichkeit und Datenschutz dem verantwortlichen öffentlichen Organ nach Erhalt aller erforderlichen Informationen eine Empfehlung ab, falls sie gegen die vorgesehenen Datenbearbeitungen und Massnahmen zum Schutz der Persönlichkeit und der Grundrechte Einwände hat. Aufgrund der teilweisen hohen inhaltlichen und technischen Komplexität der vorgesehenen Datenbearbeitungen (es sind nur diejenigen Datenbearbeitungen zur Vorabkonsultation vorzulegen, bei denen ein erhöhtes Risiko besteht) sowie den zur Verfügung stehenden knappen Ressourcen, beträgt die Frist, innert welcher eine Empfehlung abzugeben ist, zwei Monate. Entgegen der anlässlich der Anhörung vertretenen Meinung ist diese Frist nicht zu kürzen. Kleine Vorabkonsultationen sollen dagegen deutlich rascher erledigt werden können.

Nachdem sie über eine Datenschutz-Folgenabschätzung benachrichtigt worden ist, überprüft die beauftragte Person lediglich, ob die vorgeschlagenen Massnahmen zum Schutz der Persönlichkeit und der Grundrechte der betroffenen Person ausreichend sind. Hingegen nimmt sie keine umfassende Prüfung des gesamten Bearbeitungsvorgangs vor; diese Prüfung ist bereits Gegenstand der Datenschutz-Folgenabschätzung. Der beauftragten Person bleibt es indes unbenommen, zu einem späteren Zeitpunkt eine Untersuchung zu eröffnen. Dies kann insbesondere dann der Fall sein, wenn im Rahmen der Datenschutz-Folgenabschätzung die Risiken nicht korrekt eingeschätzt worden sind und sich dementsprechend auch die fraglichen Massnahmen nicht als zielgenau oder als nicht ausreichend erweisen.

Lassen sich die Risiken zu wenig genau eruieren respektive der Erfolg von Massnahmen zur Einschränkung der Risiken zu wenig genau voraussagen, kann auf Antrag der verantwortlichen Behörde zunächst ein Pilotprojekt durchgeführt werden. Dies kann vor allem dann der Fall sein, wenn die Datenbearbeitungen mit neuen technischen Methoden durchgeführt werden, deren Auswirkungen zuerst evaluiert werden müssen, oder wenn bedeutende organisatorische oder technische Massnahmen erforderlich sind, deren Wirksamkeit zuerst geprüft werden muss, etwa bezüglich Durchsetzung und Kontrolle von Zugriffsbeschränkungen bei gemeinsamer Datenhaltung von mehreren öffentlichen Organen. Die versuchsweise Durchführung kann von der beauftragten Person auch von Amts wegen empfohlen werden, wenn dies aufgrund der vorgelegten Unterlagen nötig erscheint. Die Bestimmung lehnt sich inhaltlich an die bisherigen Bestimmungen zur automatisierten Bearbeitung von Personendaten im Rahmen von Pilotprojekten (§§ 18a und 18b IDAG) an (siehe hiernach).

Die Datenschutzaufsicht muss eine Liste der Bearbeitungsvorgänge erstellen können, die vorab zur Konsultation zu unterbreiten sind. Kriterien dafür können etwa die Zahl der erfassten Personen, die Zahl der beteiligten öffentlichen Organe, die Sensitivität der Daten usw. sein (Art. 28 Abs. der Richtlinie [EU] 2016/680). Dies ist notwendig, weil sonst die Fälle, in denen das öffentliche Organ die Risiken für die betroffenen Personen nicht richtig ermittelt und daher zu Unrecht zum Schluss kommt, dass die Bearbeitung keine erhöhtes Risiko zur Folge hätte, keiner Vorab-Konsultation unterzogen würden. Eine solche Liste kann aufgrund der Aufsichtsfunktion der beauftragten Person auch ohne explizite gesetzliche Ermächtigung erstellt werden.

In Sinn eines Controllings ist nach der Testphase, spätestens aber zwei Jahre nach der Empfehlung, die vorgesehene Datenbearbeitung erneut der beauftragten Person für Öffentlichkeit und Datenschutz zur Konsultation vorzulegen.

§ 17c Meldungen von Verletzungen der Datensicherheit (neu)

§ 17c Abs. 1, 2 und 3 (neu)

[1] Das öffentliche Organ meldet der beauftragten Person für Öffentlichkeit und Datenschutz unverzüglich eine unbefugte Datenbearbeitung oder den Verlust von Daten, es sei denn, die Verletzung der Datensicherheit führt voraussichtlich nicht zu einem Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person.

[2] Das öffentliche Organ informiert ausserdem die betroffene Person, wenn es zu deren Schutz erforderlich ist oder die beauftragte Person für Öffentlichkeit und Datenschutz es verlangt. Die Information kann eingeschränkt oder aufgeschoben werden, wenn überwiegende öffentliche Interessen dies erfordern.

[3] Die Auftragsbearbeitenden informieren das verantwortliche öffentliche Organ unverzüglich über eine unbefugte Datenbearbeitung.

Verletzungen des Datenschutzes sind unverzüglich der beauftragten Person für Öffentlichkeit und Datenschutz zu melden. Darunter sind unbefugte Zugriffe oder Datenverluste aufgrund von Brüchen der technischen und organisatorischen Informations- und Informatiksicherheit zu verstehen. Diese Meldung kann ausbleiben, wenn die Verletzung voraussichtlich zu keinem Risiko für die Persönlichkeitsrechte oder andere Grundrechte der betroffenen Person führt. Damit soll vermieden werden, dass Bagatellfälle oder Verletzungen der Datensicherheit, die hinreichend eingedämmt oder beseitigt werden konnten, gemeldet werden müssen (zum Beispiel bei Verlust von Daten durch die Wiederherstellung über ein Back-up). Der Inhalt der Meldung (Beschreibung der Verletzung, der wahrscheinlichsten Folgen der Verletzung sowie der ergriffenen und vorgesehenen Massnahmen zur Wiederherstellung des Schutzes beziehungsweise Abmilderung der Folgen der Verletzung) kann auf Verordnungsebene umschrieben werden.

Das verantwortliche öffentliche Organ informiert ausserdem die betroffenen Personen, wenn es zu deren Schutz erforderlich ist oder die beauftragte Person es verlangt. Die Benachrichtigung hat insbesondere zu erfolgen, wenn die betroffenen Personen zur Abwendung des Schadens Massnahmen ergreifen können. Die Benachrichtigung kann unterbleiben, wenn durch nachträgliche Vorkehrungen sichergestellt werden konnte, dass das hohe Risiko für die Grundrecht der betroffenen Personen aller Wahrscheinlichkeit nach nicht mehr besteht. Die Benachrichtigung kann ausserdem ganz oder teilweise unterbleiben, wenn öffentliche Interessen überwiegen, zum Beispiel weil zur Wahrung der Sicherheit oder weil die Information den Zweck behördlicher oder gerichtlicher Ermittlungen, Untersuchungen oder Verfahren infrage stellen würde.

Datenbearbeitung im Auftrag

§ 18 Abs. 1 (geändert)

[1] Lässt ein öffentliches Organ Personendaten durch Dritte bearbeiten, stellt es den Datenschutz durch Vereinbarungen, Auflagen oder in anderer Weise sicher. Insbesondere dürfen Auftragsdatenbearbeitende Bearbeitungen von Personendaten ohne vorgängige schriftliche Zustimmung des öffentlichen Organs keinen weiteren Auftragnehmenden übertragen.

Die neue Richtlinie (EU) 2016/680 stellt klarere Voraussetzungen für das Bearbeitenlassen von Personendaten durch Dritte auf. So darf nur mit Auftragsdatenbearbeitenden zusammengearbeitet werden, die hinreichende Garantien dafür bieten, dass durch geeignete technische und organisatorische Massnahmen sichergestellt wird, dass die Bearbeitung gesetzeskonform erfolgt und die Rechte der betroffenen Personen gewährleistet sind. Die Datenbearbeitung darf nur mit schriftlicher Genehmigung des auftraggebenden öffentlichen Organs auf weitere Auftragsdatenbearbeitende übertragen werden. Die Übertragung muss durch Vertrag erfolgen oder durch ein anderes Rechtsinstrument, das die Auftragsdatenbearbeitenden bindet (zum Beispiel durch Gesetz, Verordnung, Regierungs-

oder Gemeinderatsbeschluss). Darin müssen der Gegenstand und die Dauer der Bearbeitung, die Art der Bearbeitung, die Art der zu bearbeitenden Personendaten, die Kategorien betroffener Personen und die Rechte und Pflichten der Auftragsdatenbearbeitenden und des auftraggebenden öffentlichen Organs festgelegt sein. Insbesondere muss gewährleistet sein,

- dass die Auftragsdatenbearbeiterin beziehungsweise der Auftragsdatenbearbeiter nur auf Weisung des auftraggebenden öffentlichen Organs handelt,
- dass die zur Auftragsdatenbearbeitung beigezogenen Personen sich zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen,
- dass die Rechte der betroffenen Personen uneingeschränkt wahrgenommen werden können,
- dass bei Vertragsende die Daten nach Wahl des auftraggebenden öffentlichen Organs vernichtet oder dem auftraggebenden öffentlichen Organ zurückgegeben werden,
- dass die Auftragsdatenbearbeiterin beziehungsweise der Auftragsdatenbearbeiter Dienste einer Unterauftragnehmerin oder eines Unterauftragnehmers nicht oder nur mit vorgängiger schriftlicher Genehmigung durch das auftraggebende öffentliche Organ in Anspruch nimmt.

Diese Erfordernisse wurden in der Praxis schon bisher gestützt auf den geltenden Gesetzestext verlangt; neu ist die Notwendigkeit einer schriftlichen Genehmigung für die Beauftragung eines Unterauftragnehmers im Gesetz festzuhalten. Die Einzelheiten können auf dem Verordnungsweg geregelt werden.

§ 18a Automatisierte Bearbeitung von Personendaten im Rahmen von Pilotprojekten (aufgehoben)

§ 18a (aufgehoben)

Die Bewilligung der automatisierten Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen nach geltendem Recht soll ermöglichen, vor der Schaffung der gesetzlichen Grundlage ein Pilotprojekt durchzuführen, um eine sachgerechte Gesetzgebung zu ermöglichen. Die Durchführung eines Pilotprojekts rechtfertigt sich vor allem bei Abrufverfahren, die besondere Schutzmassnahmen zum Schutz der Grundrechte erfordern. Die Bewilligung setzt aber voraus, dass die Aufgaben, die die Bearbeitung erforderlich machen, bereits in einem Gesetz geregelt sind. Weil der Entwurf keine explizite gesetzliche Grundlage für die Bearbeitung von besonders schützenswerten Personendaten im Rahmen des Abrufverfahren mehr verlangt und eine mittelbare gesetzliche Grundlage für die Bearbeitung von besonders schützenswerten Personendaten und das Profiling ausreicht (vgl. Ausführungen zu § 8 Abs. 2 E-IDAG), wird die Pilotprojektnorm obsolet. Dem Bedürfnis, etwa bei neuen technischen Verfahren die Datenbearbeitungen im Rahmen eines Versuchs zu testen, wird durch die neue Bestimmung in § 17b Abs. 3 und 4 E-IDAG Rechnung getragen.

Weil die beauftragte Person für Öffentlichkeit und Datenschutz gemäss Entwurf über erweiterte Befugnisse verfügt, insbesondere über die Möglichkeit, bei offensichtlicher Gefährdung der Persönlichkeit und der Grundrechte der betroffenen Personen eine Datenbearbeitung vorsorglich zu untersagen (§ 32 Abs. 3^{bis} E-IDAG) und ihr bestimmte, persönlichkeitsgefährdende Datenbearbeitungen zur Vorab-Konsultation zu unterbreiten sind, ist es sachgerecht und effizient, die versuchsweise Durchführung in diesem Zusammenhang zu prüfen.

§ 18b Evaluation (aufgehoben)

§ 18b (aufgehoben)

Durch die Aufhebung der Pilotprojektnorm wird die Pflicht zur Evaluation und Vorlage des Berichts an den Regierungsrat, der beauftragten Person für Öffentlichkeit und Datenschutz sowie der zuständigen Kommission des Grossen Rats obsolet. Nach Abschluss des Versuchs, spätestens aber zwei Jahre nach der den Versuch gutheissenden Empfehlung, ist die geplante Datenbearbeitung nochmals zur Vorab-Konsultation vorzulegen (vgl. Ausführungen zu § 17b E-IDAG).

§ 21 Vernichtung; Archivierung (geändert)

§ 21 Abs. 3 und 4 (neu)

[3] Der Regierungsrat regelt durch Verordnung die Löschfristen und die Massnahmen zur regelmässigen Überprüfung, ob die Personendaten noch benötigt werden.

[4] Die Justizleitung regelt in einem Reglement die Archivierung von Akten der Gerichte und der Schlichtungsbehörden sowie die Aufbewahrungsdauer, die Ablieferung an das Staatsarchiv und deren Vernichtung.

Das Bearbeiten von Personendaten muss – wie jedes behördliche Handeln – verhältnismässig sein. Schon bisher gehörte zur Verhältnismässigkeit, dass das Bearbeiten von Personendaten zeitlich befristet sein muss. Neu wird verlangt, dass für die Löschung von Personendaten beziehungsweise für eine regelmässige Überprüfung, ob Personendaten zur Aufgabenerfüllung noch erforderlich sind, Fristen vorzusehen sind und durch verfahrensrechtliche Vorkehren sicherzustellen ist, dass diese Fristen eingehalten werden. Der Regierungsrat wird ermächtigt, auf Verordnungsebene die entsprechenden Löschfristen und die Massnahmen zur Sicherstellung der regelmässigen Überprüfung festzulegen. Damit können für die unterschiedlichen Bereiche angepasste Lösungen getroffen werden. Indem diese Regelung dem Regierungsrat obliegt, können zudem die Löschfristen und die Massnahmen zur regelmässigen Überprüfung der weiteren Notwendigkeit der Datenaufbewahrung entsprechend rasch an sich verändernde Umstände angepasst werden.

In Absatz 4 wird die Justizleitung ermächtigt, Regelungen zur gerichtsinternen Archivierung, der Aufbewahrungsdauer und zur Vernichtung zu erlassen. Der Wortlaut entspricht dem Geltungsbereich des Reglements der Justizleitung über die Archivierung der Akten der Gerichte und der Schlichtungsbehörden des Kantons Aargau vom 21. Dezember 2012 (vgl. auch Ausführungen zu § 2 Abs. 2).

Titel 3.4 Register der Datensammlung (aufgehoben)

§ 22 Registerpflicht, Registerinhalt (aufgehoben)

§ 22 Abs. 1, 2, 3 und 4 (aufgehoben)

Nur die Justizbehörden, die Staatsanwaltschaften und die Polizeiorgane haben neu ein Register über ihre Datenbearbeitungstätigkeiten zu führen. Die entsprechenden gesetzlichen Grundlagen werden im EG StPO und im Polizeigesetz verankert. Vgl. Ausführungen zu "§ 3 Abs. 1 lit. i (aufgehoben)" hiervor.

Angesichts der geringen praktischen Bedeutung des zentralen Registers wird dieses ersatzlos aufgehoben. Die Datensammlungen selbst sind selbstredend von allen Organisationseinheiten weiterhin zu führen.

§ 24 Vorgehen

§ 24 Abs. 1 lit. b (geändert) und lit. c (neu)

[1] Die verantwortliche Behörde muss der betroffenen Person in allgemein verständlicher Form, in der Regel schriftlich, mitteilen:

b) den Zweck und gegebenenfalls die Rechtsgrundlagen des Bearbeitens, die Kategorien der bearbeiteten Personendaten, die Aufbewahrungsdauer der Personendaten oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer, die Herkunft der Personendaten und die Empfängerinnen oder Empfänger der Personendaten,

c) die Rechte der betroffenen Person.

Schon bisher musste die verantwortliche Behörde der betroffenen Person auf Anfrage hin den Zweck und gegebenenfalls die Rechtsgrundlagen des Bearbeitens sowie die Kategorien der bearbeiteten Personendaten, die an der Personendatensammlung Beteiligten, die Herkunft der Personendaten und die Empfängerinnen oder Empfänger der Personendaten bekanntgeben. Neu ist auch die Aufbewahrungsdauer der Daten anzugeben (vgl. Erläuterungen zu § 21 E-IDAG) sowie auf die Rechte der betroffenen Person hinzuweisen (Berichtigungs- und Löschungsansprüche, Recht zur Anzeige bei der beauftragten Person für Öffentlichkeit und Datenschutz). Die an der Personendatensammlung Beteiligten sind nicht mehr aufzuführen, weil der Begriff der Datensammlung nicht mehr verwendet wird (vgl. Erläuterungen zu § 3 lit. i E-IDAG) und weil schon bei der Datenbeschaffung selbst über die verantwortliche Behörde und deren Kontaktdaten zu informieren ist. Die Auskunft über die Personendaten ist von der verantwortlichen Behörde zu erteilen, so dass ohnehin ersichtlich ist, um welche Behörde es sich handelt.

§ 28 Ansprüche

§ 28 Abs. 1 lit. a (geändert)

[1] Die betroffene Person kann vom öffentlichen Organ verlangen, dass es

a) das widerrechtliche Bearbeiten unterlässt, insbesondere dass die widerrechtlich bearbeiteten Personendaten gelöscht werden,

Werden Daten unrechtmässig bearbeitet, kann die betroffene Person verschiedene Ansprüche geltend machen: die Unterlassung der widerrechtlichen Bearbeitung, die Beseitigung der Folgen der wiederrechtlichen Bearbeitung (zum Beispiel durch Löschung, Mitteilung an Datenempfänger, Veröffentlichung, Schadenersatz, Genugtuung) und die Feststellung der Widerrechtlichkeit der Bearbeitung. Neu ist der Anspruch auf Löschung im Gesetz vorzusehen: er kann geltend gemacht werden bei widerrechtlich bearbeiteten Personendaten. Der Löschungsanspruch kann spezialgesetzlich eingeschränkt werden (zum Beispiel zum Schutz der öffentlichen Sicherheit, Nichtbehinderung behördlicher oder gerichtlicher Untersuchungen etc.). In der Regel wird es in diesen Fällen aber bereits an der Widerrechtlichkeit der Bearbeitung fehlen.

§ 30 Organisation

§ 30 Abs. 1 (geändert)

[1] Der Regierungsrat wählt auf die Dauer von 8 Jahren eine in Datenschutzfragen ausgewiesene Fachperson als Beauftragte für Öffentlichkeit und Datenschutz sowie deren Stellvertretung. Die Wiederwahl ist zulässig. Die §§ 33–36 des Gesetzes über die Grundzüge des Personalrechts (Personalgesetz, PersG) vom 16. Mai 2000 gelten sinngemäss.

Gemäss Art. 43 Abs. 2 der Richtlinie (EU) 2016/680 muss jedes Mitglied über die für die Erfüllung seiner Aufgaben und Ausübung seiner Befugnisse erforderliche Qualifikation, Erfahrung und Sachkunde insbesondere im Bereich des Schutzes personenbezogener Daten verfügen. Es versteht sich von selbst, dass nur qualifizierte Personen in ein Amt zu wählen sind. Die beauftragte Person für Öffentlichkeit und Datenschutz muss daher über die Qualifikation verfügen, beide Bereiche zu betreuen und zu beaufsichtigen; dies bedeutet aber nicht zwingend, dass im Bereich des Öffentlich-

keitsprinzips zusätzlich auch Erfahrung vorliegen muss. Eine Vorschrift, dass nur Personen gewählt werden dürfen, die in beiden Bereichen über Erfahrung verfügen, würde den Kreis der infrage kommenden Personen zu stark einschränken. Ein Ausweis über die Erfahrung wird daher nur in Bezug auf den Datenschutzbereich verlangt. Weil Datenschutz und Öffentlichkeitsprinzip eng verwandt sind, sollte dies für die Durchsetzung des Öffentlichkeitsprinzips keine negativen Folgen haben.

§ 30 Abs. 1bis (neu)

[1bis] Der Regierungsrat kann die beauftragte Person für Öffentlichkeit und Datenschutz ihres Amtes entheben, wenn sie

a) vorsätzlich oder grobfahrlässig Amtspflichten schwer verletzt hat, oder
b) die Fähigkeit, das Amt auszuüben, auf Dauer verloren hat.

Art. 43 Abs. 4 der Richtlinie (EU) 2016/680 verlangt, dass der oder die Datenschutzbeauftragte des Amts nur enthoben werden darf, wenn sie oder er eine schwere Amtspflichtverletzung begangen hat oder die Voraussetzungen für die Erfüllung seiner Aufgaben nicht mehr erfüllt.

§ 30 Abs. 4 (neu)

[4] Die beauftragte Person für Öffentlichkeit und Datenschutz darf kein anderes öffentliches Amt, keine leitende Funktion in einer politischen Partei und keine andere Erwerbstätigkeit ausüben. Der Regierungsrat kann Ausnahmen bewilligen. Versieht die beauftragte Person für Öffentlichkeit und Datenschutz ein Teilpensum, darf die Bewilligung einer anderen Erwerbstätigkeit nicht verweigert werden, wenn durch diese Erwerbstätigkeit die Ausübung der Funktion sowie Unabhängigkeit und Ansehen dieser Stelle nicht beeinträchtigt werden.

Art. 42 Abs. 3 der Richtlinie (EU) 2016/680 verlangt, dass die Mitglieder von Aufsichtsbehörden von allen mit den Aufgaben ihres Amts nicht zu vereinbarenden Handlungen absehen und während ihrer Amtszeit keine anderen, mit ihrem Amt nicht zu vereinbarenden entgeltlichen oder unentgeltlichen Tätigkeiten ausüben.

Variante: anstelle eines neuen Absatzes 4 könnte in § 30 Abs. 1 ein Verweis auf die sinngemässe Anwendung von § 27 des Gesetzes über die Grundzüge des Personalrechts (Personalgesetz, PersG) vom 16. Mai 2000 eingefügt werden.

§ 31 Aufgaben

§ 31 lit. d (geändert), e und f (neu)

[1] Die beauftragte Person für Öffentlichkeit und Datenschutz

d) vermittelt zwischen Behörden und Privaten,
e) sensibilisiert die Bevölkerung, insbesondere schutzbedürftige Personen, in Bezug auf den Datenschutz,
f) verfolgt die massgeblichen Entwicklungen in den Bereichen Datenschutz und Öffentlichkeitsprinzip.

Litera d: Das Schlichtungsverfahren wird abgeschafft (vgl. nachfolgende Ausführungen zu § 36 E-IDAG) und die Aufgaben der beauftragten Person sind dementsprechend anzupassen.

Litera e: Zu den Aufgaben der beauftragten Person für Öffentlichkeit und Datenschutz gehört auch die Sensibilisierung der verantwortlichen öffentlichen Organe für ihre Pflichten und der Öffentlichkeit für die Anliegen des Datenschutzes, zum Beispiel auch im Hinblick auf die Eigenverantwortung der betroffenen Personen (Art. 46 Abs. 1 lit. b und d der Richtlinie [EU] 2016/680).

Litera f: Die Aufsichtsbehörde hat massgebliche Entwicklungen zu verfolgen, soweit sie sich auf den Schutz personenbezogener Daten auswirken, insbesondere die Entwicklung der Informations- und Kommunikationstechnologie (Art. 46 Abs. 1 lit. j der Richtlinie [EU] 2016/680). Es rechtfertigt sich, diese Weiterbildungspflicht auch für den Bereich des Öffentlichkeitsprinzips vorzusehen.

§ 32 Befugnisse

§ 32 Abs. 3 (geändert), 3bis (neu), 4 und 5 (geändert)

3 Stellt die beauftragte Person für Öffentlichkeit und Datenschutz fest, dass Vorschriften über das Öffentlichkeitsprinzip oder über den Datenschutz verletzt werden, kann sie den verantwortlichen öffentlichen Organen eine Empfehlung abgeben. Das öffentliche Organ hat zu erklären, ob es der Empfehlung folgen wird.

3bis Wird die Privatsphäre betroffener Personen offensichtlich gefährdet oder verletzt, kann die beauftragte Person vorsorglich verfügen, dass die Datenbearbeitung eingeschränkt oder eingestellt wird. Die Beschwerde gegen die vorsorgliche Verfügung hat keine aufschiebende Wirkung.

4 Lehnt das öffentliche Organ die Befolgung der Empfehlung ab oder entspricht es dieser nicht, kann die beauftragte Person für Öffentlichkeit und Datenschutz die Empfehlung ganz oder teilweise als Verfügung erlassen.

5 Das öffentliche Organ, an das die Verfügung gerichtet ist, kann sie mit Verwaltungsbeschwerde anfechten. Die beauftragte Person für Öffentlichkeit und Datenschutz ist berechtigt, gegen einen allfälligen Entscheid der Beschwerdebehörde Beschwerde beim Verwaltungsgericht zu führen. Der weitere Rechtsweg richtet sich nach einschlägigem Bundesrecht.

Der Aufsichtsbehörde muss neu die Befugnis zukommen, bei Verstössen gegen das Datenschutzrecht verbindliche Anordnungen (in Form einer Verfügung) anordnen zu können (zum Beispiel ein widerrechtliches Datenbearbeiten einzustellen oder auf eine widerrechtliche Datenbekanntgabe zu verzichten). Die Anordnung kann nach der Ablehnung einer Empfehlung erlassen werden. Sie ist mit Beschwerde durch das öffentliche Organ anfechtbar. Die beauftragte Person ist ihrerseits befugt, den Entscheid der Beschwerdeinstanz (Regierungsrat) mit Verwaltungsgerichtsbeschwerde beim Verwaltungsgericht anzufechten.

Falls schutzwürdige Interessen offensichtlich gefährdet oder verletzt werden, muss die beauftragte Person für Öffentlichkeit und Datenschutz die Befugnis haben, vorsorglich eine Datenbearbeitung zu untersagen (Art. 47 Abs. 2 lit. c der Richtlinie [EU] 2016/680).

Variante: Gemäss Leitfaden der Konferenz der Kantone (KdK) vom 2. Februar 2017 ist es möglich,

- neben dem Erlass einer Verfügung nach Ablehnung der Empfehlung durch das öffentliche Organ zusätzlich vorzusehen, dass die Verfügung direkt erlassen wird, wenn absehbar ist, dass das öffentliche Organ eine Empfehlung ablehnen oder ihr keine Folge leisten wird,
- den Rechtsweg direkt an das Verwaltungsgericht festzulegen.

§ 33 Pflichten

§ 33 Abs. 1 lit. a (geändert)

1 Die beauftragte Person für Öffentlichkeit und Datenschutz

a) behandelt Anzeigen von betroffenen Personen und informiert sie innerhalb von höchstens drei Monaten über das Ergebnis der Untersuchung oder den Stand der Abklärungen.

Es ist vorzusehen, dass jede betroffene Person ungeachtet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs das "Recht auf Beschwerde" bei der Datenschutzaufsicht hat, wenn sie der Ansicht ist, dass die Bearbeitung der sie betreffenden Personendaten gegen die datenschutzrechtlichen Vorschriften verstösst. Dabei handelt es sich der Rechtsnatur nach um eine Aufsichtsanzeige. Die beauftragte Person für Öffentlichkeit hat die Pflicht, sich mit dieser Anzeige zu befassen und hat der anzeigenden Person innert drei Monaten das Ergebnis der Abklärungen mitzuteilen. Bei Unzuständigkeit ist die Anzeige unverzüglich an die zuständige Datenschutzaufsicht weiterzuleiten (Art. 52 der Richtlinie [EU] 2016/680). Die Begriffe "Eingaben" und "Beschwerden" werden gestrichen.

Das geltende Recht statuiert die Pflicht, Anzeigen und Eingaben von betroffenen Personen zu behandeln und Beschwerden entgegenzunehmen, ohne dass im übrigen Gesetzestext die Eingaben und Beschwerden vorgesehen würden. In der Praxis wird die beauftragte Person für Öffentlichkeit und Datenschutz auf Anzeige hin tätig (§ 32 Abs. 1 IDAG) oder erteilt Privaten gemäss § 31 Abs. 1 lit. b IDAG Auskunft über ihre Rechte (auf Anfrage hin oder im Rahmen der Informationstätigkeit).

Die Rechte der betroffenen Person im Rahmen des Anspruchs auf Auskunft über die eigenen Daten oder des Anspruchs auf Berichtigung, Löschung oder Unterlassung bei widerrechtlicher Datenbearbeitung müssen auch durch die Aufsichtsbehörde ausgeübt werden können (Art. 17 Abs. 1 der Richtlinie [EU] 2016/680). Die betroffene Person kann in diesen Fällen Anzeige bei der beauftragten Person erstatten mit den sich daraus ergebenden Rechtsfolgen.

§ 35 Gesuch

§ 35 Gesuch (geändert)

[1] Ansprüche gemäss den §§ 5, 23 und 28 können mündlich oder schriftlich bei der verantwortlichen Behörde geltend gemacht werden. Der Gegenstand des Anspruchs ist näher zu bezeichnen.

Die bisherige Formulierung "Ansprüche nach diesem Gesetz" hat sich als zu offen erwiesen; die besonderen Verfahrensbestimmungen gemäss §§ 35 ff. E-IDAG sollen nur der Durchsetzung der spezifischen Ansprüche auf Zugang zu amtlichen Dokumenten, Einsicht in eigene Daten und Ansprüche auf Unterlassung, Berichtigung etc. der Betroffenen bei der Bearbeitung von Personendaten dienen. Andere Ansprüche, zum Beispiel auf Amtshilfe oder der Anspruch privater Dritter auf Datenbekanntgabe durch die Einwohnerkontrolle, sind nach den Regeln des übrigen Verwaltungsrechts geltend zu machen.

§ 36 Rechtliches Gehör

§ 36 Abs. 1 und 2 (geändert)

[1] Zieht die Behörde die teilweise oder vollständige Abweisung des Gesuchs in Betracht, hat sie der gesuchstellenden Person vorgängig Mitteilung zu machen.

[2] Sind schutzwürdige Interessen Dritter betroffen, ist diesen vor Erlass der Verfügung das rechtliche Gehör zu gewähren. Zieht das öffentliche Organ in Betracht, dem Zugangsgesuch entgegen der eingeholten Stellungnahme zu entsprechen, hat es den Drittpersonen vorgängig Mitteilung zu machen.

Die Durchführung eines Schlichtungsverfahrens ist nach dem übergeordneten Recht nicht notwendig. In der Praxis hat es sich als aufwendig erwiesen, weil bei Fehlen einer Einigung in jedem Fall – ungeachtet der Bedeutung des Anspruchs für die Rechte der gesuchstellenden Person – eine Empfehlung zu erlassen war. Ein sehr hoher Anteil an Einigungen wird auf dem informellen Weg der Vermittlung durch die beauftragte Person erzielt. Wenn dies nicht möglich ist, ist in der Regel auch bei nachfolgender Durchführung des formellen Schlichtungsverfahrens keine Einigung der (zunehmend anwaltlich vertretenen) Parteien möglich. Der Wert der an eine Schlichtungsverfahren anschliessenden Empfehlung ist zudem gering, weil die beauftragte Person nicht wie bei Empfehlungen nach § 32 Abs. 3 E-IDAG berechtigt ist, die Verfügung des öffentlichen Organs anzufechten, wenn dieses entgegen der Empfehlung entscheidet. Eine Schlichtungsaufgabe ist zudem problematisch, weil es im Vorfeld die Beratung des öffentlichen Organs und eventuell der gesuchstellenden Person praktisch ausschliesst, weil im nachfolgenden Schlichtungsverfahren eine Vorbefassung bestehen würde. Das Schlichtungsverfahren wird daher gestrichen.

§ 37 Schlichtungsverfahren

§ 37 Abs. 1 und 2 (aufgehoben)

Es wird auf die Ausführungen zu § 36 hiervor verwiesen.

§ 38 Verfügung

§ 38 Abs. 1 (geändert)

[1] Innert 30 Tagen nach Eingang der Mitteilung gemäss § 36 Abs. 1 und 2 können die gesuchstellende Person oder die Drittperson beim öffentlichen Organ den Erlass einer anfechtbaren Verfügung verlangen.

Die öffentlichkeits- und datenschutzrechtlichen Ansprüche können formlos geltend gemacht werden, auch mündlich oder per E-Mail. Es besteht daher das praktische Bedürfnis, dass durch das öffentliche Organ in gleicher Weise auf das Gesuch geantwortet werden kann und nicht direkt, sondern erst auf Verlangen eine anfechtbare Verfügung erlassen werden muss. Gerade auf Stufe der Gemeinden kann so eine Beantwortung rascher erfolgen, andernfalls müsste unter Umständen eine Gemeinderatssitzung abgewartet werden.

§ 40 Kosten und Gebühren (aufgehoben)

§ 40 Abs. 4 (aufgehoben)

Das Schlichtungsverfahren gemäss § 37 IDAG wird aufgehoben. Dementsprechend ist auch die Regelung von § 40 Abs. 4 IDAG über die Kostenlosigkeit des Schlichtungsverfahrens aufzuheben.

6.1.2 Änderungen auf Verordnungsstufe

Die unter Ziffer 5.1.2 dargelegten Gesetzesanpassungen im IDAG bedürfen noch einer weiteren Ausführung auf Verordnungsstufe im VIDAG. Insbesondere sind folgende Punkte in der VIDAG zu regeln:

- Erweiterung des (nicht abschliessenden) Katalogs der besonders schützenswerten Personendaten um biometrische und genetische Daten
- Regelung, wie der Nachweis über die Einhaltung der Datenschutzvorschriften erbracht werden kann
- Voraussetzungen für die Datenbearbeitung im Auftrag (notwendiger Vertragsinhalt)
- Umfang der Informationspflicht bei Datenbeschaffung
- Inhalt der Datenschutz-Folgenabschätzung
- Definition der Datenschutzverletzung
- Löschfristen und Massnahmen zur Sicherstellung der Überprüfung.

Der Regierungsrat wird die entsprechenden Verordnungsänderungen nach Inkraftsetzung des revidierten IDAG beschliessen.

6.2 Einführungsgesetz zur Schweizerischen Strafprozessordnung (EG StPO)

§ 49 Information am Vollzug mitwirkender Dritter und anderer Behörden

§ 49 Abs. 1 (geändert)

[1] Die mit der Behandlung, Betreuung oder Kontrolle von Personen im Straf- oder Massnahmenvollzug oder mit dem Schutz der Öffentlichkeit vor Straftätern und -täterinnen betrauten Personen, Institutionen und Amtsstellen

a) erhalten von der Vollzugsbehörde und der Bewährungshilfe Informationen über diese Personengruppen, soweit sie für die korrekte Aufgabenerfüllung darauf angewiesen sind. In diesem Rahmen sind ihnen die erforderlichen Akten zur Verfügung zu stellen,

b) sind verpflichtet, die Vollzugsbehörde und die Bewährungshilfe umgehend über wichtige Erkenntnisse und Ereignisse im Zusammenhang mit den Personen im Straf- oder Massnahmenvollzug zu informieren.

Die geltende Regelung des § 49 Abs. 1 EG StPO sieht bereits eine ausdrückliche Ermächtigung der Vollzugsbehörde zur umfassenden Information der am Vollzug mitwirkenden Dritten vor. Der Vollständigkeit halber soll nun zusätzlich ausdrücklich darauf hingewiesen werden, dass dieses Informationsrecht auch die Überlassung von Akten umfasst. Damit wird eine gelebte und grundsätzlich von der bisherigen Bestimmung bereits getragene Praxis ausdrücklich im Gesetz erwähnt. Neu soll aber zugleich auch eine bisher nur im Rahmen der konkreten Vollzugsverfügung jeweils ausdrücklich angeordnete Pflicht der mit dem Vollzug beauftragten Dritten, die Vollzugsbehörde umgehend über alle wichtigen Erkenntnisse und Ereignisse im Vollzugsverfahren zu informieren, im Gesetz verankert werden.

Diese Anpassungen sind nicht zwingend erforderlich für die Umsetzung der EU-Datenschutzreform, sie helfen aber, allfällige Unklarheiten von vornherein zu beseitigen.

Titel 12.^{bis} Bearbeitung von Personendaten (neu)

Hinsichtlich der neuen Bestimmungen zur Bearbeitung von Personendaten ist auch ein neuer Titel 12.^{bis} einzuführen.

Da in der parallel laufenden Änderung des EG StPO zur Umsetzung der Ausschaffungsinitiative und der Änderung des Allgemeinen Teils des Schweizerischen Strafgesetzbuchs (StGB) vom 21. Dezember 1937 ein neuer § 55a EG-StPO vorgesehen ist, werden vorliegend ein neuer § 55b und ein neuer § 55c EG StPO vorgeschlagen.

Gemäss § 1 Abs. 2 des Einführungsgesetzes zur Schweizerischen Jugendstrafprozessordnung (EG JStPO) vom 16. März 2010 gelten § 55b und § 55c E-EG StPO auch für die Jugendanwaltschaft.

§ 55b Register über Datenbearbeitungstätigkeiten (neu)

§ 55b Abs. 1 (neu)

[1] Die Strafverfolgungs- und Gerichtsbehörden führen ein Register über die Datenbearbeitungstätigkeiten in ihrem Zuständigkeitsbereich.

Die Richtlinie (EU) 2016/680 verlangt für den justiziellen und polizeilichen Bereich, dass ein Register der Datenbearbeitungen zu führen ist und knüpft damit praxisbezogener an die Tätigkeit an. Das Register ist öffentlich, was sich bereits aus dem im IDAG festgeschriebenen Öffentlichkeitsprinzip ergibt und daher (anders wie die entsprechende Bundesregelung) nicht noch ausdrücklich erwähnt wird. Den Inhalt des Registers regelt der Regierungsrat durch Verordnung.

§ 55c Datenschutzberatung (neu)

§ 55c Abs. 1 und 2 (neu)

[1] Die Strafverfolgungsbehörden benennen innerhalb ihrer Organisationseinheit eine für den Datenschutz zuständige Person.

[2] Die für den Datenschutz zuständige Person hat folgende Aufgaben:

a) sie berät und unterstützt die Mitarbeitenden der Organisationseinheit bei der Bearbeitung von Personendaten hinsichtlich der Einhaltung der Datenschutzvorschriften und der Datensicherheit,

b) sie nimmt Datenschutz-Folgenabschätzungen gemäss § 17a des Gesetzes über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (IDAG) vom 24. Oktober 2006 vor,

c) sie ist Ansprechperson der beauftragten Person für Öffentlichkeit und Datenschutz.

Die Richtlinie (EU) 2016/680 verlangt die Benennung einer für den Datenschutz zuständige Person. Auf eine solche Funktion kann aber für Gerichte im Rahmen ihrer justiziellen Tätigkeit verzichtet werden. Bei der für den Datenschutz zuständigen Person kann es sich um ein Mitglied des vorhandenen Personals handeln, das eine besondere Schulung auf dem Gebiet der Datenschutzvorschrif-

ten und der Datenschutzpraxis erhalten hat. Der Grad des erforderlichen Fachwissens sollte sich insbesondere nach der Art der durchgeführten Datenverarbeitung und des erforderlichen Schutzes für die verarbeiteten personenbezogenen Daten richten. Die für den Datenschutz zuständige Person sollte die Beschäftigten, die personenbezogene Daten verarbeiten, unterstützen, indem sie diese Personen über die Einhaltung ihrer jeweiligen Datenschutzpflichten unterrichtet und berät. Zudem nimmt sie die Datenschutz-Folgeabschätzungen gemäss § 17a E-IDAG vor und ist Ansprechperson der beauftragten Person für Öffentlichkeit und Datenschutz.

6.3 Gesetz über die Gewährleistung der öffentlichen Sicherheit (Polizeigesetz, PolG)

6.3.1 Vorbemerkungen

Im Polizeirecht ist die rechtliche Grundlage für die Bearbeitung von Daten, namentlich besonders schützenswerter Personendaten, sowie für das Profiling an die Vorgaben der Richtlinie (EU) 2016/680 anzupassen. Zudem ist die Verantwortlichkeit für die Datenbearbeitung zu definieren, insbesondere für Fälle, in welchen mehrere Organisationseinheiten Daten bearbeiten. Die Richtlinie (EU) 2016/680 verlangt bezüglich der Transparenz bei der Datenbearbeitung, dass die Polizeibehörden ein Verzeichnis über die Datenbearbeitungstätigkeiten führen. Da im E-IDAG die Bestimmung betreffend Register und Datensammlung aufgehoben wird (vgl. Ziffer 5.1.2 hiervor), ist eine entsprechende Regelung im Polizeigesetz vorzusehen. Die Vorgabe der Richtlinie (EU) 2016/680, wonach im materiellen Datenschutzrecht Löschfristen für Daten vorzusehen sind, wurde im Polizeirecht mit der Verordnung über die Datenbearbeitungssysteme der Kantonspolizei bereits erfüllt. Im Polizeigesetz ist noch die entsprechende Delegationsnorm zu schaffen, welche dem Regierungsrat die Kompetenz zur Regelung dieser Materie in einer Verordnung gibt. Schliesslich ist im Polizeigesetz festzuhalten, dass im Polizeibereich eine für den Datenschutz zuständige Person einzusetzen ist.

6.3.2 Einzelne Bestimmungen

§ 49 Grundsatz

§ 49 Abs. 1 (geändert)

[1] Die Polizei kann Personendaten bearbeiten sowie Profiling betreiben, soweit dies zur Erfüllung der gesetzlichen Aufgaben erforderlich ist.

Der Begriff Personendaten umfasst sowohl 'normale' Personendaten wie auch besonders schützenswerte Personendaten. Letztere dürfen nur bearbeitet werden, wenn ein formelles Gesetz dies ausdrücklich vorsieht (unmittelbare Grundlage) oder wenn dies für die Erfüllung einer in einem Gesetz umschriebenen Aufgabe unentbehrlich ist (mittelbare Grundlage). In den §§ 2 ff. PolG sind die Aufgaben der Kantonspolizei sowie der Polizeikräfte der Gemeinden definiert. Die qualifizierten Anforderungen an die Bearbeitung besonders schützenswerter Personendaten werden erfüllt, indem auf die gesetzlich umschriebenen Aufgaben der Polizei verwiesen wird, zu deren Erfüllung die Bearbeitung notwendig ist.

Der Begriff des Beschaffens von Personendaten ist im Begriff des Bearbeitens von Personendaten bereits enthalten und kann somit gestrichen werden.

Neu wird das Profiling als besonders "gefährliche" Art des Bearbeitens von Personendaten geregelt, welche denselben Anforderungen genügen muss wie das Bearbeiten von besonders schützenswerten Personendaten (vgl. § 8 Abs. 2 E-IDAG). Insbesondere im Bereich der Kriminalitätsbekämpfung kann diese Art der Bearbeitung von Personendaten für die Polizei unentbehrlich sein, weshalb sie dazu befugt sein muss und demzufolge die entsprechende gesetzliche Grundlage geschaffen werden muss.

§ 50 Datenbearbeitungssysteme

§ 50 Abs. 1bis (neu)

[1bis] Die Hauptverantwortung für Datenbearbeitungssysteme, die von der Kantonspolizei und den Polizeikräften der Gemeinden gemeinsam betrieben werden, liegt bei der Kantonspolizei.

Die Verantwortung für Datenbearbeitungen muss klar zugeordnet werden. Das gilt insbesondere bei gemeinsamen Datenbearbeitungen, wo die Verantwortlichkeiten transparent zu regeln sind.

§ 50 Abs. 1 PolG regelt, dass die Polizei Datenbearbeitungssysteme betreiben kann. Daraus ergibt sich, dass der jeweilige Betreiber auch die Verantwortung für das Bearbeiten der Daten trägt. Neu wird in § 50 Abs. 1bis E-PolG geregelt, dass die Verantwortung für die Datenbearbeitung bei der Kantonspolizei liegt, wenn sie gemeinsam mit den Polizeikräften der Gemeinden Datenbearbeitungssysteme betreiben. Diese Regelung entbindet die Polizeikräfte der Gemeinden jedoch nicht davon, ihrerseits ebenfalls die notwendigen datenschutzrechtlichen Massnahmen zu ergreifen.

§ 50 Abs. 3 (neu)

[3] Der Regierungsrat regelt durch Verordnung die in den Datenbanksystemen zu bearbeitenden Datenkategorien und den Bearbeitungszweck.

Die Richtlinie (EU) 2016/680 sieht vor, dass Polizeibehörden ihre Datenbearbeitungstätigkeiten transparent machen. Neben dem Verzeichnis über die Datenbearbeitungstätigkeiten gemäss § 50a PolG kommt die Polizei der Pflicht zur Transparenz nach, indem sie die von ihr bearbeiteten Datenkategorien und den Zweck der Bearbeitung in der Verordnung über die Datenbanksysteme der Kantonspolizei definiert. Im Rahmen der vorliegenden Anpassungen ist es angebracht, dem Regierungsrat die entsprechende Regelungskompetenz im Polizeigesetz einzuräumen.

§ 50a Register über Datenbearbeitungstätigkeiten (neu)

§ 50a (neu)

[1] Die Polizei führt ein Register über ihre Datenbearbeitungstätigkeiten.

Die Richtlinie (EU) 2016/680 verlangt, dass in den Bereichen der Strafverfolgung und der Justiz unter dem Titel der Transparenzplicht ein Verzeichnis über die Datenbearbeitungstätigkeiten geführt wird. Diese ist der gemäss § 22 IDAG statuierten Registrierpflicht für öffentliche Organe sehr ähnlich. Da diese Norm im Rahmen der vorliegenden Umsetzung jedoch gestrichen werden soll, muss in den fachspezifischen Gesetzen die notwendige Grundlage für die Pflicht zur Führung eines Verzeichnisses über die Datenbearbeitungstätigkeiten geschaffen werden. Die Regelung in § 55b E-EG StPO erfasst jedoch nur die kriminalpolizeilichen Datenbearbeitungstätigkeiten der Polizei. Um sämtliche Datenbearbeitungstätigkeiten der Polizei zu umfassen, ist demzufolge eine entsprechende Grundlage im PolG notwendig.

§ 51 Bekanntgabe von Daten

§ 51 Abs. 2 (geändert)

[2] Der Zugriff auf polizeiliche Daten ist der Kantonspolizei sowie den Polizeikräften der Gemeinden vorbehalten und nur zulässig, soweit dies zur Erfüllung der polizeilichen Aufgaben erforderlich ist.

Da das Abrufverfahren aufgehoben wird, ist der Wortlaut von Absatz 2 anzupassen.

§ 54 Vernichtung von Daten

§ 54 Abs. 3 (neu)

[3] Der Regierungsrat regelt durch Verordnung die Aufbewahrungsfristen der Daten.

Die Richtlinie (EU) 2016/680 verlangt im Zusammenhang mit der Verhältnismässigkeit der Datenbearbeitung, dass für diese Aufbewahrungs- respektive Löschfristen definiert werden. In § 21 E-IDAG wird der Regierungsrat ermächtigt, solche auf Verordnungsstufe zu regeln. Die Aufbewahrungsfristen für die von der Polizei bearbeiteten Daten sind bereits in den §§ 13 ff. der Verordnung über die Datenbanksysteme der Kantonspolizei geregelt. Im Rahmen der vorliegenden Anpassungen wird dem Regierungsrat die entsprechende Regelungskompetenz explizit auch im Polizeigesetz eingeräumt.

§ 54a Datenschutzberatung (neu)

§ 54a Abs. 1 und 2 (neu)

[1] Die Polizeiorgane benennen innerhalb ihrer Organisationseinheit eine für den Datenschutz zuständige Person.

[2] Die für den Datenschutz zuständige Person hat folgende Aufgaben:

a) sie berät und unterstützt die Mitarbeitenden der Organisationseinheit bei der Bearbeitung von Personendaten hinsichtlich der Einhaltung der Datenschutzvorschriften und der Datensicherheit,
b) sie nimmt Datenschutz-Folgenabschätzungen gemäss § 17a des Gesetzes über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (IDAG) vom 24. Oktober 2006 vor,
c) sie ist Ansprechperson der beauftragten Person für Öffentlichkeit und Datenschutz.

Vgl. Ausführungen zu § 55c EG StPO (neu) hiervor.

6.4 Einführungsgesetz zum Bundesgesetz über die obligatorische Arbeitslosenversicherung und die Insolvenzentschädigung sowie zum Bundesgesetz über die Arbeitsvermittlung und den Personalverleih (EG AVIG/AVG)

6.4.1 Vorbemerkungen

Verschiedene Behörden befassen sich heute mit der Integration von stellensuchenden Personen in den Arbeitsmarkt. Wichtige Akteure in diesem Bereich sind etwa das kantonale Arbeitsamt, die kantonale IV-Stelle und die Sozialdienste der Gemeinden.

Arbeiten verschiedene Behörden zusammen, um stellensuchende Personen (wieder) in den Arbeitsmarkt einzugliedern, ist es nötig, dass sie sich gegenseitig über jene Daten der betreffenden Personen informieren, die für deren Eingliederung in den Arbeitsmarkt wesentlich sind. Dabei kann es sich auch um besonders schützenswerte Personendaten, wie Gesundheitsdaten handeln. Heutzutage werden solche Daten von den zuständigen Behörden in verschiedenen Informationssystemen bearbeitet. Effiziente Kommunikation zwischen den Behörden lässt sich am besten mittels Zugriff auf Informationssysteme erreichen, die solche Daten enthalten.

Der Bund hat im Bereich der interinstitutionellen Zusammenarbeit bereits gesetzliche Grundlagen geschaffen. Verlangt wird dabei eine enge Zusammenarbeit unter den beteiligten Institutionen. Mit Fokus auf den Datenschutz soll vorliegend eine kantonale gesetzliche Grundlage geschaffen werden, die den Austausch besonders schützenswerter Personendaten bei der Arbeitsmarktintegration sowie den Zugriff auf solche Daten erlaubt. Damit sollen die Möglichkeiten, die das Bundesrecht bei der Arbeitsmarktintegration für den elektronischen Datenaustausch vorsieht, kantonalrechtlich umgesetzt beziehungsweise die kantonalrechtlichen Voraussetzungen für einen reibungslosen elektronischen Datenaustausch zwischen den Behörden geschaffen werden.

6.4.2 Einzelne Bestimmungen

§ 9a Datenschutz bei der interinstitutionellen Arbeitsmarktintegration (neu)

§ 9a Abs. 1, 2, 3 und 4 (neu)

[1] Die in Hinblick auf die Arbeitsmarktintegration zusammenarbeitenden Behörden, namentlich die kantonalen Durchführungsorgane der Arbeitslosenversicherung und der Invalidenversicherung sowie die Sozialdienste der Gemeinden, dürfen im Rahmen des Bundesrechts einander alle, auch besonders schützenswerte Personendaten bekanntgeben, soweit diese benötigt werden, um Stellensuchende in den Arbeitsmarkt zu integrieren.

[2] Sie dürfen alle Personendaten gemäss Absatz 1 auch im kantonalen Einwohnerregister abfragen.

[3] Die zusammenarbeitenden Behörden verwenden beim Datenaustausch systematisch die AHV-Versichertennummer.

[4] Der Regierungsrat legt durch Verordnung die zur Arbeitsmarktintegration erforderlichen Personendaten fest und bezeichnet darin ausserdem die zur Bekanntgabe und zum Bezug der Personendaten legitimierten Behörden.

Absatz 1 schafft die gesetzliche Grundlage dafür, dass die für die Arbeitsmarktintegration wichtigen Partner, namentlich in der ALV, der IV und der Sozialhilfe auch besonders schützenswerte Personendaten austauschen dürfen, sofern dies zum Zweck der (Wieder-)Eingliederung nötig ist. Mit dieser Bestimmung werden die Behörden gegenseitig von der Schweigepflicht entbunden. Die genannten Behörden dürfen einander im Einzelfall gegenseitig besonders schützenswerte Personendaten auf elektronischem Weg zugänglich machen. Dazu gewähren sie sich gegenseitig die nötigen Zugriffs- und Bearbeitungsrechte, das heisst Lese- und Schreibrechte. Es dürfen aber weiterhin nur die für die Arbeitsmarktintegration der jeweiligen Stellensuchenden tatsächlich benötigten Daten bekannt gegeben werden. Die für die Arbeitsmarktintegration zusammenarbeitenden Behörden erhalten somit keine Blankovollmacht. Zudem sind die vom Bundesrecht für die Zulässigkeit des Datenaustauschs vorgesehenen Bedingungen zu beachten.

In Absatz 2 wird geregelt, dass Personendaten, die für die Arbeitsmarktintegration benötigt werden, auch im kantonalen Einwohnerregister abgefragt, das heisst gelesen werden können. Durch den Verweis auf Absatz 1 sind auch besonders schützenswerte Personendaten von der Abfrage erfasst.

Um eine stellensuchende Person eindeutig identifizieren zu können, sollen die datenaustauschenden Behörden systematisch die AHV-Versichertennummer verwenden (Absatz 3).

Die Bestimmung von Absatz 4 verpflichtet den Regierungsrat dazu, die für die Arbeitsmarktintegration nötigen Personendaten, die im Einzelnen ausgetauscht werden dürfen beziehungsweise auf die im Einzelnen zugegriffen werden darf, auf dem Verordnungsweg zu konkretisieren. Damit wird die Reichweite der erlaubten Datenbearbeitung transparent geregelt beziehungsweise für die betroffenen Personen vorhersehbar. Die im Hinblick auf die Arbeitsmarktintegration zusammenarbeitenden Behörden werden in Absatz 1 nur namentlich und nicht abschliessend erwähnt. Auf Verordnungsstufe ist daher ebenfalls festzulegen, welche Behörden Personendaten bekanntgeben beziehungsweise abfragen dürfen.

7. Auswirkungen

7.1 Personelle und finanzielle Auswirkungen auf den Kanton

Die Gesetzesanpassungen führen zu keinen personellen und finanziellen Auswirkungen auf den Kanton. Für die beauftragte Person für Öffentlichkeit und Datenschutz entsteht zwar einerseits durch die aus den Datenschutz-Folgenabschätzungen folgenden Vorab-Konsultationen und die neue Befugnis, bei Verstössen gegen das Datenschutzrecht verbindliche Anordnungen in Form einer Verfügung anordnen zu können, eine Mehrbelastung. Anderseits erfolgt durch die Aufhebung des Schlichtungsverfahrens auch eine Entlastung. Die bei der Staatsanwaltschaft, der Jugendanwaltschaft und der Kantonspolizei neu eingeführte Funktion einer für den Datenschutz zuständigen Person bedarf keiner separaten, eigenständigen Stelle und wird mit bestehenden Ressourcen abgedeckt.

7.2 Auswirkungen auf die Wirtschaft

Die vorgeschlagenen Anpassungen gewährleisten, dass die kantonalen Datenschutzbestimmungen dem europäischen Standard genügen. Für die Aargauer Volkswirtschaft als Ganzes dürfte es gesamthaft von Nutzen sein, wenn der Kanton Aargau wie der Bund über einen mit der EU gleichwertigen Datenschutz verfügt. Dadurch wird der Marktzutritt in der EU gesichert, wodurch insbesondere der zunehmende elektronische Handel und die international tätige Wirtschaft profitieren dürften. Insgesamt ist davon auszugehen, dass der für die Unternehmen entstehende Vorteil die ihnen anfallenden Kosten überwiegt.

7.3 Auswirkungen auf die Gemeinden

Die kantonalen Datenschutzbestimmungen gelten auch für die Gemeinden, womit für diese auch die Anpassungen verbindlich sind. Die Regionalpolizeien haben ebenfalls eine für den Datenschutz zuständige Person zu benennen (neuer § 54a PolG), wobei eine entsprechende Funktion bei den meisten Corps bereits einer oder einem Mitarbeitenden übertragen ist.

7.4 Auswirkungen auf die Beziehungen zum Bund und zu anderen Kantonen

Für die Zusammenarbeit mit dem Bund und den anderen Kantonen ist ein einheitliches Datenschutzniveau von zentraler Bedeutung.

8. Weiteres Vorgehen

Nach der Notifizierung der Richtlinie (EU) 2016/680 am 1. August 2016 beschloss der Bundesrat am 31. August 2016 deren Übernahme. Für die Schweiz gilt eine Umsetzungsfrist von zwei Jahren ab Notifikation des jeweiligen Rechtserlasses. Die EU-Datenschutzreform muss demzufolge auch von den Kantonen bis zum 1. August 2018 umgesetzt werden, das heisst die Gesetzesänderungen müssen daher auf diesen Zeitpunkt in Kraft treten.

Um den äusserst engen Zeitplan zur Umsetzung der EU-Datenschutzreform möglichst einhalten zu können, wird eine Verkürzung der Fristen zwischen der 1. und der 2. Beratung beantragt werden. Allenfalls wird eine vorzeitige Inkraftsetzung gemäss § 37 des Gesetzes über die Organisation des Grossen Rates und über den Verkehr zwischen dem Grossen Rat, dem Regierungsrat und der Justizleitung (Geschäftsverkehrsgesetz, GVG) vom 19. Juni 1990 notwendig sein. Es ergibt sich daher folgender Zeitplan (vorausgesetzt, es besteht auf die 2. Beratung hin kein grösserer Revisions- oder Abklärungsbedarf):

1. Beratung im Grossen Rat	November 2017
Verabschiedung Botschaft für 2. Beratung	November 2017
2. Beratung im Grossen Rat	Januar 2018
Redaktionskommission	Februar 2018
Eventuelle Redaktionslesung im Grossen Rat	Februar 2018
Referendumsfrist	März 2018 bis Mai 2018
(Vorzeitiges) Inkrafttreten IDAG, EG StPO, PolG, EG AVIG/AVG	1. August 2018
Eventuelle Volksabstimmung	3. Quartal 2018

Antrag

1.

Der vorliegende Entwurf einer Änderung des Gesetzes über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (IDAG) wird in 1. Beratung zum Beschluss erhoben.

2.

Der vorliegende Entwurf einer Änderung des Einführungsgesetzes zur Schweizerischen Strafprozessordnung (EG StPO) wird in 1. Beratung zum Beschluss erhoben.

3.

Der vorliegende Entwurf einer Änderung des Gesetzes über die Gewährleistung der öffentlichen Sicherheit (Polizeigesetz, PolG) wird in 1. Beratung zum Beschluss erhoben.

4.

Der vorliegende Entwurf einer Änderung des Einführungsgesetzes zum Bundesgesetz über die obligatorische Arbeitslosenversicherung und die Insolvenzentschädigung sowie zum Bundesgesetz über die Arbeitsvermittlung und den Personalverleih (EG AVIG/AVG) wird in 1. Beratung zum Beschluss erhoben.

Regierungsrat Aargau

Beilagen
- Synopse Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (IDAG) (Beilage 1)
- Synopse Einführungsgesetz zur Schweizerischen Strafprozessordnung (EG StPO) (Beilage 2)
- Synopse Gesetz über die Gewährleistung der öffentlichen Sicherheit (Polizeigesetz, PolG) (Beilage 3)
- Synopse Einführungsgesetz zum Bundesgesetz über die obligatorische Arbeitslosenversicherung und die Insolvenzentschädigung sowie zum Bundesgesetz über die Arbeitsvermittlung und den Personalverleih (EG AVIG/AVG) (Beilage 4)