KANTON AARGAU

DEPARTEMENT
VOLKSWIRTSCHAFT UND INNERES

29. März 2017

ANHÖRUNGSBERICHT

EU-Datenschutzreform – Anpassung des kantonalen Rechts

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

Inhaltsverzeichnis

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), 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 dadurch zudem der Zugriff auf das europaweite Fahndungssystem – das Schengener Informationssystem (SIS) – garantiert.

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, d.h., 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 Datenschutzgesetzes behoben werden, die aufgrund der rasanten technologischen Entwicklung entstanden sind. Andererseits soll die Revision den Entwicklungen auf der Ebene des Europarates und der Europäischen Union Rechnung tragen.

Auch auf internationaler Ebene wird dem Datenschutz immer grössere Beachtung geschenkt. So hat die Europäische Union 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 Europäischen Rats 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 Europäische Union der Schweiz im Rahmen der Schengen-Evaluation gemacht hat. Dabei wurde insbesondere empfohlen, die Kompetenzen des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten 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 aber 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 Sinne 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, d.h. zumindest vom Verantwortlichen und vom Auftragsbearbeiter Zugang zu den verarbeiteten Daten und allen Informationen erhält, die zur Erfüllung ihrer Aufgaben notwen-

dig 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 Artikel 2 Absatz 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 Bundesgesetzes über den Datenschutz 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 Europäische Union 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 sich zurzeit im Vernehmlassungsverfahren befindliche Entwurf des revidierten DSG 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 Da-

tenschutz 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 Staates 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 Europäischen Union. 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 bzw. Vorgaben zu einem angemessenen Datenschutz sind bei der Anwendung der beiden anderen Rechtserlasse im öffentlich-rechtlichen wie auch privat-rechtlichen

(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 Europäischen Union 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

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 Aarhus-Konvention das Bundesgesetz über den Umweltschutz (Umweltschutzgesetz, USG) vom 7. Oktober 1983 angepasst und darin in einem neuen Absatz 8 zu Artikel 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 entsprach. 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 Schutz der Menschenrechte und Grundfreiheiten (EMRK) verstösst. Die Regelung des Öffentlichkeitsprinzips im Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (IDAG) 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 (z.B. des Ausländer- und des Asylgesetzes, des Bundespersonalgesetzes, des Zivilgesetzbuchs 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 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, wie nachfolgend in Ziffer 5 aufgezeigt wird.

3. Umsetzung und Rechtsgrundlagen

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 (bspw. Regelungen des Zivilprozessrechts, des Strafrechts, des Strafprozessrechts etc.). Der Vorentwurf 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.

Die Vorlage beschränkt sich 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 Arbeitslosenversicherung und die Insolvenzentschädigung sowie zum Bundesgesetz über die Arbeitsvermittlung und den Personalverleih (EG AVIG/AGV) vom 14. September 2004.

Die im Vordergrund stehende Revision des IDAG verfolgt im Wesentlichen folgende sieben Stossrichtungen:

- Eine erste Stossrichtung der Revision bildet der risikobasierte Ansatz. Der Revisionsentwurf orientiert sich konsequent an den potentiellen 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 (z.B. 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 (z.B. Datenbearbeitungen, die in einem Dokumentenmanagementsystem ohne besonders schützenswerte Daten erfolgen).
- Eine zweite Stossrichtung ist die Beibehaltung des technologieneutralen Charakters des IDAG. Dadurch bleibt das Gesetz offen für weitere technologische Entwicklungen und verhindert keine

Innovationen. Weil sie dem technologieneutralen Charakter des Erlasses widerspricht, wird beispielsweise die Anforderung der formellen gesetzlichen Grundlage für die "Abrufverfahren" aufgegeben.

- Die dritte Stossrichtung besteht in der Modernisierung der Terminologie, 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.
- Eine vierte, besonders bedeutsame Stossrichtung der Revision ist die Stärkung der Rechte der betroffenen Personen. Diese erfolgt über verschiedene Instrumente, die den Betroffenen insgesamt erlauben sollen, ihre Daten besser zu kontrollieren und besser darüber bestimmen zu können.
- Eng mit der vierten verbunden ist die fünfte Stossrichtung, wonach die Pflichten der Verantwortlichen präzisiert und stärker auf den Schutz der betroffenen Person ausgerichtet werden. Die verantwortlichen öffentlichen Organe werden auch dazu verpflichtet, bei gewissen Arten von Datenbearbeitungen eine Datenschutz-Folgenabschätzung durchzuführen. Technische Vorkehren sollen für eine datenschutzfreundliche Ausgestaltung von Systemen sorgen.
- Die sechste Stossrichtung ist die Stärkung der Kontrolle. Die Befugnisse der beauftragten Person für Öffentlichkeit und Datenschutz werden künftig mit den Befugnissen der entsprechenden ausländischen Kontrollbehörden vergleichbar sein. Anders als ihre Kolleginnen und Kollegen im europäischen Ausland wird sie jedoch nicht befugt sein, Verwaltungssanktionen auszusprechen. Auf die Einführung von neuen Strafbestimmungen auf kantonaler Ebene wird verzichtet.
- Die siebte Stossrichtung ist die Gleichwertigkeit von Öffentlichkeitsprinzip und Datenschutz. Der beauftragten Person für Öffentlichkeitsprinzip und Datenschutz sollen für beide Bereiche die gleichen Befugnisse zustehen. Dies erweist sich schon daher als notwendig, weil bei der praktischen Anwendung häufig beide Aspekte eine Rolle spielen und nicht voneinander zu trennen sind.

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 Europäische Union 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 Europäischen Union 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 bzw. im Falle 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. Erläuterungen zu einzelnen Gesetzesbestimmungen

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

5.1.1 Wesentliche Neuerungen des Entwurfs

Mit der Änderung wird vorgeschlagen, auf den Schutz der Daten juristischer Personen zu verzichten. In den datenschutzrechtlichen Bestimmungen der Europäischen Union und des Europarates 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 Vorentwurf 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 Auftragsbearbeiter verbindlich sind. Nur das öffentliche Organ, gegen das die Untersuchung eingeleitet wurde, ist in einem Untersuchungsverfahren Partei.

5.1.2 Einzelne Bestimmungen

§ 2 Geltungsbereich

§ 2 Abs. 2 und 2bis (geändert)

[2] Richterliche Behörden fallen nicht in den Bereich der Aufgaben und Befugnisse der beauftragten Person für Öffentlichkeit und Datenschutz gemäss §§ 17b f. und 31 f. dieses Gesetzes. Die Justizleitung regelt in einem Reglement die Einsicht in Gerichtsakten abgeschlossener Verfahren bis zur Archivierung.

[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 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, z.B. das Polizeigesetz, das Schulgesetz oder das Bundesgesetz über den allgemeinen Teil des Sozialversicherungsrechts) weiter ihre Gültigkeit (vgl. dazu BEAT RUDIN, Überholte Ausnahmen beim Geltungsbereich, digma 2016, 122 ff.). Die Regelungen z.B. der Strafprozessordnung gelten weiterhin, aber auch die Grundsätze des IDAG (z.B. 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 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.

Um Kollisionen zwischen den verfahrensrechtlichen und 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, d.h. auch diejenigen, deren Daten nicht verändert, sondern zur Kenntnis genommen werden, z.B. beim Beizug alter Verfahrensakten. Die übrigen Bestimmungen, z.B. die Pflicht zur Gewährleistung der Datensicherheit durch technische und organisatorische Massnahmen (§ 12) oder der Sicherstellung des Datenschutzes bei Outsourcing (§ 18) 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 handelt, sind auf seine Datenbearbeitungen die Bestimmungen des Bundesgesetzes über den Datenschutz (DSG) vom 19. Juni 1992 anwendbar. Die Aufsicht richtet sich nach dem vorliegenden 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. Da solche kantonalen und kommunalen öffentlichen Organe nicht Private werden, sondern nur wie Private 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 Artikel 28 ff. des Schweizerischen Zivilgesetzbuchs vom 10. Dezember 1907 (ZGB), (Persönlichkeitsverletzungen wie beispielsweise Rufschädigung), das Bundesgesetz vom 9. Oktober 1992 über das Urheberrecht und verwandte Schutzrechte (URG), das Bundesgesetz gegen den unlauteren Wettbewerb (UWG) vom 19. Dezember 1986 oder durch die Bestimmungen zum Schutz von Berufs-, Geschäfts- und Fabrikationsgeheimnissen sowie Art. 13 der Bundesverfassung (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 der Verordnung zum Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (VIDAG) vom 26. September 2007enthält 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 10 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. 1, 2 (geändert) und 3 (aufgehoben)

[1] Enthält das amtliche Dokument Personendaten Dritter, sind diese auszusondern oder zu anonymisieren, sofern kein überwiegendes öffentliches Interesse an deren Bekanntgabe besteht.

[2] Absatz 1 gelangt nicht zur Anwendung bei Personendaten, die von den Betroffenen selbst öffentlich zugänglich gemacht wurden oder bei denen der öffentliche Zugang offensichtlich im Interesse der Betroffenen liegt.

[3] Aufgehoben.

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, d.h. 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 i.S. Beauftragte für Öffentlichkeit und Datenschutz ca. Regierungsrat des Kantons Aargau).

Am 1. Juni 2014 trat für die Schweiz die 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 (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, S. 370 f.). Zudem können nur Angaben mit Bezug zu einer natürlichen Person der Einsicht entgegenstehen (KLEIN, a.a.O., S. 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 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 Diskriminierungspotential 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 lit. b gestrichen.

§ 12 Datensicherheit

§ 12 Abs. 2 (geändert)

[2] Das verantwortliche öffentliche Organ ist verpflichtet, den Nachweis erbringen zu können, 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 Datenempfänger oder die Kategorien der Datenempfänger, 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) wenn 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 (z.B. 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, d.h., 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 (§ 2 Abs. 2^{bis} des Entwurfs). 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.

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). Im Bereich der selbständigen 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 §§ 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, d.h. auch dann, wenn ein öffentliches Organ regelmässig Personendaten bei einem anderen öffentlichen Organ beschaffen muss. Die Voraussetzungen gemäss § 8 und 9 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 und sind ebenfalls anzupassen, d.h., 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 Erforder-nis, 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 im Sinn von § 17 handelt, stets Abgrenzungsprobleme ergeben. Die Anforderungen an eine gesetzliche Grundlage sollen sich konkret nach der Schwere des Eingriffs richten und technologieneutral bleiben.

§ 17a Datenschutz-Folgeabschätzung (neu)

§ 17a Abs. 1 und 2 (neu)

[1] Führt die vorgesehene Datenbearbeitung voraussichtlich zu einem erhöhten Risiko für 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 Grundrechte der betroffenen Person sowie die Massnahmen, die vorgesehen sind, um das Risiko einer Verletzung 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 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 Grundrechte der betroffenen Personen bestehenden Risiken sowie eine Darstellung und Bewertung der geplanten Abhilfemassnahmen, Garantien, Sicherheitsvorkehren und Verfahren, durch die der Schutz der Grundrechte der betroffenen Personen sichergestellt und der Nachweis erbracht werden soll, dass dieses Gesetz eingehalten wird. Die Datenschutz-Folgenabschätzung ist im Grunde 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 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 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 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 im Sinn von § 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 im Sinn von § 32 Abs. 3 abgeben, wenn die geplante Datenbearbeitung gegen Datenschutzbestimmungen verstossen würde, insbesondere, weil das verantwortliche öffentliche Organ die Risiken für 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 innerhalb von zwei Monaten nach Erhalt aller erforderlichen Informationen eine Empfehlung ab, falls sie gegen die vorgesehenen Datenbearbeitungen und Massnahmen zum Schutz der Grundrechte Einwände hat.

Nachdem sie über eine Datenschutz-Folgenabschätzung benachrichtigt worden ist, überprüft die beauftragte Person lediglich, ob die vorgeschlagenen Massnahmen zum Schutz der Grundrechte und der Persönlichkeit 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 der Fall sein, wenn im Rahmen der Datenschutz-Folgenabschätzung die Risiken nicht korrekt eingeschätzt wurden 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 Amtes 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) an (s. 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 Richtli-

nie (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.

§ 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 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] Der Auftragsbearbeiter informiert das verantwortliche öffentliche Organ unverzüglich über eine unbefugte Datenbearbeitung.

Verletzungen des Datenschutzes sind unverzüglich der beauftragten Person für Öffentlichkeit und Datenschutz 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 Persönlichkeits- oder andere Grundrechte der betroffenen Person führt. Damit soll vermieden werden, dass Bagatellfälle gemeldet werden müssen oder Verletzungen der Datensicherheit, die hinreichend eingedämmt oder beseitigt werden konnten (z.B. 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 bzw. 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, z.B. weil zur Wahrung der Sicherheit oder weil die Information den Zweck behördlicher oder gerichtlicher Ermittlungen, Untersuchungen oder Verfahren in Frage 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 Auftragnehmern 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 (z.B. 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 bzw. 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 bzw. der Auftragsdatenbearbeiter Dienste eines Unterauftragnehmers oder einer Unterauftragnehmerin 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), 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 Rechnung getragen.

Weil die beauftragte Person für Öffentlichkeit und Datenschutz gemäss Entwurf über erweiterte Befugnisse verfügt, insbesondere über die Möglichkeit, bei offensichtlicher Gefährdung der Grundrechte der betroffenen Personen eine Datenbearbeitung vorsorglich zu untersagen (§ 32 Abs. 3^{bis}) 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).

§ 21 Vernichtung; Archivierung (geändert)

§ 21 Abs. 3 (neu)

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

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.

Titel 3.4 Register der Datensammlung (aufgehoben)

§ 22 Registerpflicht, Registerinhalt (aufgehoben)

§ 22 Abs. 1, 2, 3 und 4 (aufgehoben)

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.

§ 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) 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 (z.B. 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 (z.B. 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 Öffentlichkeitsprinzips zusätzlich auch Erfahrung vorliegen muss. Eine Vorschrift, dass nur Personen gewählt werden dürfen, die in beiden Bereichen über Erfahrung verfügen, würde den Kreis der in Frage 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 Amtes nur enthoben werden darf, wenn er oder sie 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 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 für den Schutz von Personendaten und das Öffentlichkeitsprinzip massgeblichen Entwicklungen.

Litera d: Das Schlichtungsverfahren wird abgeschafft (vgl. Ausführungen zu § 36) 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, z.B. 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 welches 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 (z.B. 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) oder erteilt Privaten gemäss § 31 Abs. 1 lit. b 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 (§ 36 Abs. 1 E-IDAG).

§ 35 Gesuch

§ 35 Gesuch (geändert)

[1] Ansprüche gemäss §§ 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. 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, z.B. 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 aufwändig 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 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.

5.1.3 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 Datenschutzfolgenabschätzung
- Definition der Datenschutzverletzung
- Löschfristen und Massnahmen zur Sicherstellung der Überprüfung

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

5.2 Einführungsgesetz zur Schweizerischen Strafprozessordnung (EG StPO)

§ 49 Information am Vollzug mitwirkender Dritter und anderer Behörden

§ 49 Abs. 1 (geändert) und 1bis (neu)

[1] Die Vollzugsbehörde und die Bewährungshilfe informieren Personen, Institutionen und Amtsstellen, die mit der Behandlung, Betreuung oder Kontrolle von Personen im Straf- oder Massnahmenvollzug oder mit dem Schutz der Öffentlichkeit vor Straftätern betraut sind, soweit diese für die korrekte Aufgabenerfüllung darauf angewiesen sind. In diesem Rahmen stellen sie auch die erforderlichen Akten zur Verfügung.

[1bis] Die mit der Behandlung, Betreuung oder Kontrolle von Personen im Straf- oder Massnahmenvollzug oder mit dem Schutz der Öffentlichkeit vor Straftätern betrauten Personen, Institutionen und Amtsstellen 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 Strafgesetzbuchs 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 EG StPO auch für die Jugendanwaltschaft.

§ 55b Register über Datenbearbeitungstätigkeiten (neu)

§ 55b Abs. 1 (neu)

[1] Die Gerichts- und Strafverfolgungsbehörden 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 Datenschutzberater (neu)

§ 55c Abs. 1 und 2 (neu)

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

[2] Der Datenschutzberater hat folgende Aufgaben:

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

b) er nimmt Datenschutzfolgeabschätzungen gemäss § 17a IDAG vor,

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

Die Richtlinie (EU) 2016/680 verlangt die Benennung eines Datenschutzberaters. Auf einen solchen Datenschutzberater kann aber für Gerichte im Rahmen ihrer justiziellen Tätigkeit verzichtet werden. Bei der Person des Datenschutzberaters kann es sich um ein Mitglied des vorhandenen Personals handeln, das eine besondere Schulung auf dem Gebiet der Datenschutzvorschriften 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. Der Datenschutzberater sollte die Beschäftigten, die personenbezogene Daten verarbeiten, unterstützen, indem er diese Personen über die Einhaltung ihrer jeweiligen Datenschutzpflichten unterrichtet und berät. Zudem nimmt er die Datenschutzfolgeabschätzungen gemäss § 17a E-IDAG vor und ist Ansprechperson der beauftragten Person für Öffentlichkeit und Datenschutz.

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

5.3.1 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 ein Datenschutzberater einzusetzen ist.

5.3.2 Einzelne Bestimmungen

§ 49 Grundsatz

§ 49 Abs. 1 (geändert)

[1] Die Polizei kann Personendaten bearbeiten sowie Profiling betreiben, sofern 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, welche 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 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 Bekanntgabe von Daten

§ 50 Abs. 3 (neu)

^{3} Der Regierungsrat regelt die in den Datenbanksystemen zu bearbeitenden Datenkategorien und den Bearbeitungszweck in einer Verordnung.

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 Verzeichnis 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 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.

§ 54 Vernichtung von Daten

§ 54 Abs. 3 (neu)

^{3} Der Regierungsrat regelt die Aufbewahrungsfristen der Daten in einer Verordnung.

Die Richtlinie (EU) 2016/680 verlangt im Zusammenhang mit der Verhältnismässigkeit der Datenbearbeitung, dass für diese Aufbewahrungs- resp. 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 Datenschutzberater (neu)

§ 54 Abs. 1 und 2 (neu)

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

[2] Der Datenschutzberater hat folgende Aufgaben:

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

b) er nimmt Datenschutzfolgeabschätzungen gemäss § 17a IDAG vor,

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

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

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

5.4.1 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 mittels Abrufverfahren erlaubt. Damit sollen die Möglichkeiten, die das Bundesrecht bei der Arbeitsmarktintegration für den elektronischen Datenaustausch vorsieht, kantonalrechtlich umgesetzt bzw. die kantonalrechtlichen Voraussetzungen für einen reibungslosen elektronischen Datenaustausch zwischen den Behörden geschaffen werden.

5.4.2 Einzelne Bestimmungen

§ 9a Datenschutz bei der interinstitutionellen Arbeitsmarktintegration (neu)

§ 9a Abs. 1, 2, 3, 4 und 5 (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 sich alle, auch besonders schützenswerte Personendaten gegenseitig bekanntgeben, soweit sie benötigt werden, um Stellensuchende in den Arbeitsmarkt zu integrieren.

[2] Im Einzelfall dürfen sie sich alle Personendaten gemäss Absatz 1durch Abrufverfahren gegenseitig zugänglich machen. Sie gewähren sich dazu gegenseitig die erforderlichen Zugangs- und Bearbeitungsrechte.

[3] Sie können alle Personendaten gemäss Absatz 1 auch im kantonalen Einwohnerregister abfragen.

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

[5] Der Regierungsrat legt die zur Arbeitsmarktintegration erforderlichen Personendaten durch Verordnung fest.

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.

Absatz 2 bestimmt, dass sich die genannten Behörden im Einzelfall gegenseitig besonders schützenswerte Personendaten auf elektronischem Weg zugänglich machen dürfen. Dazu gewähren sie sich gegenseitig die nötigen Zugriffs- und Bearbeitungsrechte, d.h. Lese- und Schreibrechte.

In Absatz 3 wird geregelt, dass Personendaten, die für die Arbeitsmarktintegration benötigt werden, auch im kantonalen Einwohnerregister abgefragt, d.h. gelesen werden können.

Um eine stellensuchende Person eindeutig identifizieren zu können, sollen die datenaustauschenden Behörden systematisch die AHV-Versichertennummer verwenden (Absatz 4).

Die Bestimmung von Absatz 5 verpflichtet den Regierungsrat dazu, die für die Arbeitsmarktintegration nötigen Personendaten, die im Einzelnen ausgetauscht werden dürfen bzw. auf die im Einzelnen zugegriffen werden darf, auf dem Verordnungsweg zu konkretisieren. Damit wird die Reichweite der erlaubten Datenbearbeitung transparent geregelt bzw. für die betroffenen Personen vorhersehbar.

6. Auswirkungen

6.1 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 Datenschutz-Folgeabschätzungen 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 des Datenschutzberaters bedarf keiner separaten, eigenständigen Stelle und wird mit bestehenden Ressourcen abgedeckt.

6.2 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.

6.3 Auswirkungen auf die Gemeinden

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

6.4 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.

7. 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, d.h. 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 die Anhörungsfrist für die kantonalen Gesetzesänderungen ausnahmsweise auf zwei statt drei Monate festgelegt sowie 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.

Anhörung	April/Mai
Verabschiedung Botschaft für 1. Beratung	August 2017
1. Beratung im Grossen Rat	3./4. Quartal 2017
Verabschiedung Botschaft für 2. Beratung	4. Quartal 2017
2. Beratung im Grossen Rat	1. Quartal 2018
Redaktionskommission	1. Quartal 2018
Evtl. Redaktionslesung im Grossen Rat	2. Quartal 2018
Vorzeitiges Inkrafttreten	1. August 2018
Evtl. Volksabstimmung	3. Quartal 2018

Beilagen

- Synopse IDAG (Beilage 1)
- Synopse EG StPO (Beilage 2)
- Synopse PolG (Beilage 3)
- Synopse EG AVIG/AVG (Beilage 4)