Vorlage des Regierungsrates vom 21. Mai 2019

Bericht und Antrag des Regierungsrats des Kantons Schaffhausen an den Kantonsrat betreffend Änderung des Gesetzes über den Schutz von Personendaten (Kantonales Datenschutzgesetz)

19-43

Sehr geehrter Herr Präsident
Sehr geehrte Damen und Herren

Wir unterbreiten Ihnen hiermit Bericht und Antrag zur Änderung des Gesetzes über den Schutz von Personendaten (Kantonales Datenschutzgesetz) vom 7. März 1994 [1)].

Die vorzunehmenden Änderungen sind einerseits notwendig, um der fortschreitenden Digitalisierung im Bereich des Datenschutzes Rechnung zu tragen. Andererseits ist die Schweiz verpflichtet, bestimmte neue Vorgaben des europäischen Rechts in die innerstaatliche Rechtsordnung umzusetzen. Die neuen Bestimmungen sollen dabei insbesondere die Rechte der von Datenbearbeitungen betroffenen Personen stärken, indem die Anforderungen an die Transparenz bei Datenbearbeitungen erhöht und datenbearbeitende Behörden für Themen des Datenschutzes sensibilisiert werden. Ausserdem soll die Unabhängigkeit der kantonalen Aufsichtsstelle gestärkt werden.

Zur Ausarbeitung des revidierten Datenschutzgesetzes wurde unter Zuhilfenahme eines von der Konferenz der Kantonsregierungen erarbeiteten Leitfadens analysiert, welcher zwingende Anpassungsbedarf im kantonalen Datenschutzgesetz aufgrund der neuen europäischen Vorgaben besteht. Gestützt darauf wurde ein Vorentwurf der anzupassenden Bestimmungen erarbeitet und ein Vernehmlassungsverfahren unter Einbezug der politischen Parteien, der Gemeinden und der kantonalen Verwaltung durchgeführt. Der vorliegende Gesetzesentwurf wurde schliesslich unter Berücksichtigung der eingegangenen Vernehmlassungsergebnisse erarbeitet. Er beschränkt sich auf die aufgrund der europäischen Normen zwingend notwendigen Anpassungen.

---

1) SHR 174.100.

I. Ausgangslage

Die Gesetzgebung im Bereich des Datenschutzes befasst sich mit dem Umgang mit Personendaten, das heisst mit Daten, die sich auf bestimmte oder bestimmbare Personen beziehen. Verfügt ein Dritter - sei dies ein öffentliches Organ oder eine juristische oder natürliche Person - über Daten einer anderen Person, ist zu regeln, wie diese Daten bearbeitet werden dürfen. Kern des Datenschutzrechts ist der Schutz der Persönlichkeit der von einer Datenbearbeitung betroffenen Person, insbesondere deren Recht auf informationelle Selbstbestimmung. Die Datenschutzgesetze regeln deshalb, wie der Inhaber der Daten mit diesen umzugehen hat, welche Rechte der von der Bearbeitung betroffenen Person zukommen und wie die Aufsicht über Datenbearbeitungen zu gestalten ist.

In der Schweiz ist es Aufgabe des Bundes, Datenbearbeitungen durch Private und öffentliche Organe des Bundes zu regeln. Dieser Aufgabe ist der Bund mit Erlass des Bundesgesetzes über den Datenschutz (DSG) vom 19. Juni 1992 [2)] nachgekommen.

Den Kantonen obliegt die Regelung von Datenbearbeitungen durch kantonale und kommunale öffentliche Organe. Im Kanton Schaffhausen ist diesbezüglich insbesondere das kantonale Datenschutzgesetz relevant.

Die rasante technologische Entwicklung der letzten Jahre hat dazu geführt, dass Datenbearbeitungen heute sehr weitgehend auf elektronischem Weg geschehen. Dies bedeutet einerseits, dass die nationale Gesetzgebung sich dieser Entwicklung anzupassen hat, um die Entstehung rechtsfreier Räume zu vermeiden. Andererseits bringen Digitalisierung und Globalisierung auch mit sich, dass dem grenzüberschreitenden Datenverkehr immer grössere Bedeutung zukommt. In diesem Zusammenhang sind internationale Vereinbarungen und Rechtssetzungsakte im Bereich des Datenschutzes von wachsender Relevanz. Aus den genannten Gründen haben die Europäische Union und der Europarat ihre Datenschutzgesetzgebungen jüngst umfassend revidiert. Diese Revisionen haben Auswirkungen auf die Gesetzgebung der Schweiz und zwar sowohl auf jene des Bundes wie auch auf jene der Kantone. Soweit die Rechtsetzungszuständigkeit beim Bund liegt, nimmt dieser die Anpassungen in der derzeit laufenden Revision des Bundesgesetzes über den Datenschutz vor. Im Kanton Schaffhausen resultiert Anpassungsbedarf im kantonalen Datenschutzgesetz.

II. Relevante europäische Rechtssetzungsakte

Für die Schweiz sind im europäischen Kontext folgende neuen oder umfassend revidierten Rechtssetzungsakte von Bedeutung:

[2)] SR 235.1, derzeit in Totalrevision.

1. Verordnung (EU) 2016/679

In der Europäischen Union ist die Verordnung (EU) 2016/679 der grundlegende Datenschutzerlass. Es handelt sich um einen neuen Rechtssetzungsakt der Europäischen Union, der Ende Mai 2018 Geltung erlangte. Die Verordnung regelt hauptsächlich den Schutz von Personen, deren Daten im Rahmen des Binnenmarkts bearbeitet werden. Sie gilt sowohl für Private als auch für den öffentlichen Sektor. Die Bestimmungen der Verordnung (EU) 2016/679 sind nicht schengenrelevant und damit für die Schweiz nicht verbindlich. Dies bedeutet aber nicht, dass die Verordnung in der Schweiz gänzlich ausser Acht gelassen werden kann. Die Schweiz ist auf einen funktionierenden Datenaustausch mit der Europäischen Union angewiesen. Dies gilt einerseits für die international tätige Wirtschaft, die mit Blick auf den elektronischen Handel vom Marktzutritt in den EU-Raum abhängig ist. Andererseits sind auch die Behörden auf einen funktionierenden Datenaustausch angewiesen. Die Verordnung (EU) 2016/679 legt Minimalstandards fest, die in Drittstaaten eingehalten werden müssen, damit das dortige Datenschutzniveau als angemessen beurteilt wird. Der Angemessenheitsbeschluss der Europäischen Kommission ist Voraussetzung für den Datentransfer zwischen der Europäischen Union und der Schweiz ohne zusätzliche Massnahmen. Will die Schweiz im bisherigen Rahmen vom europäischen Datenaustausch profitieren können, hat sie ein angemessenes Datenschutzniveau im Sinne der Verordnung zu garantieren.

2. Richtlinie (EU) 2016/680

Die Richtlinie (EU) 2016/680 bildet Teil des Schengener-Assoziierungs-Abkommens und ist seit dem 5. Mai 2016 in Kraft. Sie wurde von der Schweiz am 1. August 2016 notifiziert und ist damit für die Schweiz verbindlich. Allerdings ist sie sowohl in den EU-Mitgliedstaaten als auch in der Schweiz nicht direkt anwendbar, sondern bedarf der Umsetzung in das jeweilige nationale Recht. Um den Schengen-Verpflichtungen nachzukommen, war vorgesehen, die Richtlinie innert zwei Jahren, bis am 1. August 2018, in die innerstaatliche Rechtsordnung umzusetzen. Die Richtlinie hat einen eingeschränkten Geltungsbereich und ist darauf ausgerichtet, personenbezogene Daten zu schützen, die zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung bearbeitet werden. Sie soll ein hohes Schutzniveau für diese sensiblen Daten gewährleisten und gleichzeitig den Austausch dieser Daten zwischen den zuständigen Behörden der verschiedenen Schengen-Staaten erleichtern. Sie gilt sowohl für grenzüberschreitende Datenbearbeitungen als auch für Datenbearbeitungen, die von den Polizei- und Justizbehörden auf innerstaatlicher Ebene durchgeführt werden.

3. Übereinkommen SEV 108

Nebst der Europäischen Union hat auch der Europarat seine datenschutzrechtliche Gesetzgebung revidiert, namentlich das von der Schweiz ratifizierte Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen Nr. 108 der Sammlung der Europäischen Verträge, kurz: Übereinkommen SEV 108). Der beratende Ausschuss des Übereinkommens SEV 108 hat einen Entwurf zur Revision erarbeitet. Das Änderungsprotokoll zum Übereinkommen muss vom Ministerkomitee noch definitiv verabschiedet werden. Substantielle

Änderungen des Revisionsentwurfs sind aber nicht mehr zu erwarten. Mit der Revision des nationalen Rechts soll sichergestellt werden, dass dieses mit dem revidierten Übereinkommen SEV 108 vereinbar ist und die Schweiz auch das revidierte Übereinkommen ratifizieren kann. Das Übereinkommen SEV 108 soll den Datenschutz auf internationaler Ebene vereinheitlichen und verbessern. Dadurch wird auch der Schutz der Schweizer Bürgerinnen und Bürger verstärkt, wenn ihre Personendaten im Ausland bearbeitet werden. Auch trägt das Übereinkommen dazu bei, die Bekanntgabe von Daten zwischen den Vertragsparteien zu vereinfachen. Die Schweizer Unternehmen erhalten so einen besseren Zugang zu den Märkten dieser Länder. Das Übereinkommen ist auf alle Datenbearbeitungen im öffentlichen und privaten Sektor anwendbar und in den nationalen Rechtsordnungen der Vertragsparteien umzusetzen.

III. Nationale Gesetzgebung

1. Bund

Um den dargelegten gesetzgeberischen Entwicklungen des Europarates und der Europäischen Union Rechnung zu tragen und die aufgrund der rasanten technologischen Entwicklung entstandenen Schwächen des Datenschutzgesetzes zu beheben, wird das Bundesgesetz über den Datenschutz derzeit totalrevidiert. Im September 2017 hat der Bundesrat nach durchgeführtem Vernehmlassungsverfahren die Botschaft zur Totalrevision des DSG sowie den Entwurf (E-DSG) veröffentlicht. Im Zusammenhang mit dieser Revision will der Bund zudem in zahlreichen weiteren Erlassen Anpassungen des materiellen Datenschutzrechts vornehmen (z.B. im Zivilprozessrecht, Strafrecht, Strafprozessrecht etc.).

Der Nationalrat beschloss in der Sommersession 2018, die Revision des Datenschutzrechts in zwei Etappen anzugehen. Jene Anpassungen, welche aufgrund der Richtlinie (EU) 2016/680 erforderlich sind und damit nur Datenbearbeitungen durch Bundesorgane betreffen, wurden angesichts der Dringlichkeit zuerst vorgenommen und das Bundesgesetz über den Datenschutz im Rahmen der Anwendung des Schengen-Besitzstands in Strafsachen (Schengen-Datenschutzgesetz, SDSG [3)]) verabschiedet und per 1. März 2019 in Kraft gesetzt. Das SDSG wird voraussichtlich nur während kurzer Zeit gelten. Es ist geplant, die erlassenen Bestimmungen im Rahmen einer zweiten Revisionsetappe wieder in das eidgenössische Datenschutzgesetz zu integrieren. Diese zweite Etappe der Revision, welche die Totalrevision des Bundesgesetzes über den Datenschutz umfasst und insbesondere die Datenbearbeitungen durch Private regeln soll, wird frühestens in der Sommersession 2019 im Nationalrat behandelt.

2. Kanton Schaffhausen

Da die Gesetzgebung des Europarates und der Europäischen Union auch die Datenbearbeitung durch kantonale und kommunale Behörden betrifft, ist im Kanton Schaffhausen das Gesetz über den Schutz von Personendaten zu revidieren.

[3)] SR 235.3.

Im kantonalen Vernehmlassungsverfahren wurde seitens eines Vernehmlassungsteilnehmers angeregt, mit dieser Revision zuzuwarten, bis das eidgenössische Datenschutzgesetz verabschiedet ist. Aus Sicht des Regierungsrats ist ein weiteres Zuwarten mit der vorliegenden Revision nicht angebracht. Die Umsetzung der Richtlinie (EU) 2016/680 ins innerstaatliche Recht hätte grundsätzlich bereits bis am 1. August 2018 erfolgen müssen. Mit einem weiteren Zuwarten würden die von der Schweiz gegenüber der Europäischen Union eingegangenen Verpflichtungen verletzt. Entsprechend hat denn auch der Bund die in diesem Zusammenhang relevanten Verpflichtungen mit dem SDSG bereits umgesetzt. Es ist davon auszugehen, dass diese Bestimmungen keine substantiellen Änderungen erfahren werden, wenn das SDSG wieder in das eidgenössische Datenschutzgesetz integriert wird. Das SDSG enthält bereits die zentralen Bestimmungen, welche die Datenbearbeitung durch Behörden betreffen. Die weiteren parlamentarischen Beratungen werden grösstenteils die Regelung von Datenbearbeitungen durch Private zum Gegenstand haben, welche ohnehin ausserhalb des Geltungsbereichs des kantonalen Datenschutzgesetzes liegen. Die bundesrechtlichen Regelungen für behördliche Datenbearbeitungen stehen mit anderen Worten bereits jetzt weitestgehend fest. Vor diesem Hintergrund haben auch zahlreiche andere Kantone die erforderlichen Anpassungen ihrer kantonalen Datenschutzgesetze vorgenommen.

IV. Die wichtigsten Änderungen des kantonalen Datenschutzgesetzes im Überblick

1. Vorbemerkung

Das geltende Datenschutzrecht, sowohl auf Bundesebene als auch auf kantonaler Ebene, unterscheidet nicht zwischen Daten natürlicher und juristischer Personen (vgl. Art. 1 und Art. 2 it. a und b). Bearbeiten Behörden Daten juristischer Personen, gelten daher die gleichen Voraussetzungen wie bei der Bearbeitung von Daten natürlicher Personen. Juristischen Personen, deren Daten bearbeitet werden, kommen die gleichen Rechte zu wie natürlichen Personen.

Der Bund sieht vor, Daten juristischer Personen künftig vom Schutzbereich des Datenschutzgesetzes auszunehmen (Art. 2 Abs. 1 E-DSG). Dieses soll nur noch auf natürliche Personen Anwendung finden. Begründet wird der Entscheid damit, dass die datenschutzrechtlichen Bestimmungen der Europäischen Union und des Europarates sowie der meisten ausländischen Rechtsordnungen keinen solchen Schutz vorsehen. Die praktische Bedeutung des Schutzes von Daten juristischer Personen wird als gering beurteilt, da dieser durch andere spezifische Gesetze hinreichend gewährleistet sei (Persönlichkeitsschutz, unlauterer Wettbewerb, Urheberrecht). Die Kantone sind nicht verpflichtet, die vom Bund vorgesehene Anpassung des Geltungsbereichs ebenfalls vorzunehmen.

Auf Bundesebene macht die Aufhebung des Schutzes von Daten juristischer Personen eine Reihe von neuen Bestimmungen in anderen Bundesgesetzen notwendig, insbesondere im Regierungs- und Verwaltungsorganisationsgesetz vom 21. März 1997 [4)]. So sind unter anderem die Bekanntgabe von Daten juristischer Personen, der Zugang zu amtlichen Dokumenten mit Daten juristischer Personen und die Auskunftsrechte gesetzlich zu regeln [5)]. Auch bei einer Änderung des Geltungsbereichs des kantonalen Datenschutzgesetzes wären sämtliche Gesetzesgrundlagen, welche Bearbeitungen von Personendaten berühren, auf Anpassungsbedarf zu prüfen. Ausserdem wären an geeigneter Stelle neue gesetzliche Bestimmungen zu schaffen, die einerseits gewährleisten, dass Daten juristischer Personen weiterhin hinreichend geschützt sind und anderseits, dass sie weiterhin Auskunft über Datenbearbeitungen erhalten, die sie betreffen. Letztlich würde der Schutz von Daten juristischer Personen lediglich vom Datenschutzgesetz in andere Gesetze verlagert. Der Nutzen einer solchen Verlagerung ist nicht ersichtlich. Umgekehrt ist auch nicht ersichtlich, welchen Nachteil es mit sich bringt, wenn das kantonale Datenschutzgesetz weiterhin sowohl auf Personendaten natürlicher als auch juristischer Personen Anwendung findet.

Im vorliegenden Gesetzesentwurf wird daher davon abgesehen, Daten juristischer Personen vom Geltungsbereich des kantonalen Datenschutzgesetzes auszunehmen. Soweit die Vernehmlassungsteilnehmer sich zu dieser Entscheidung geäussert haben, wurde die vorgeschlagene Lösung ausdrücklich begrüsst. Ein Vernehmlassungsteilnehmer hat richtigerweise darauf hingewiesen, dass die konkreten Folgen unterschiedlicher Anwendungsbereiche der Datenschutzgesetze von Bund und Kanton schwer abzuschätzen und die Situation deshalb auf jeden Fall im Auge zu behalten sei. Die diesbezüglichen Entwicklungen werden aufmerksam zu verfolgen sein. Gegenwärtig besteht aus Sicht der Regierung aber kein Anlass, juristische Personen vom Geltungsbereich des kantonalen Datenschutzgesetzes auszunehmen.

2. Transparenzbestimmungen

Zentralstes Anliegen der Richtlinie (EU) 2016/680 und des Übereinkommens SEV 108 ist die Erhöhung der Transparenz gegenüber den von Datenbearbeitungen betroffenen Personen. Die für Datenbearbeitungen verantwortlichen öffentlichen Organe treffen daher verschiedene neue Pflichten. Dazu gehören die Pflicht zur Vornahme einer Datenschutz-Folgenschabschätzung, eine umfassende Informationspflicht und die Pflicht, den betroffenen Personen Verletzungen von Datenschutzbestimmungen mitzuteilen.

Bei der Datenschutz-Folgenabschätzung hat das verantwortliche öffentliche Organ zu dokumentieren, welche Risiken bei einer geplanten Datenbearbeitung für die Grundrechte der betroffenen Personen bestehen und welche Massnahmen zum Schutz der Grundrechte vorzusehen sind. Bereits bisher durften automatisierte Verfahren zur Bearbeitung von personenbezogenen

---

4) SR 172.010.

5) vgl. Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017

Daten, die mit besonderen Risiken für die Rechte und Freiheit der betroffenen Personen verbunden sein konnten, nur eingesetzt werden, wenn sichergestellt war, dass den Risiken mit geeigneten technischen oder organisatorischen Massnahmen begegnet wird (Art. 16a). Die Pflicht konnte nur erfüllt werden, wenn bei geplanten Vorhaben geprüft wurde, ob im Zusammenhang mit dem Vorhaben besondere Risiken bestehen und wie diesen gegebenenfalls zu begegnen ist. Wurden diese Vorhaben, wie gesetzlich vorgesehen (Art. 16a Abs. 2), dem Datenschutzbeauftragten zur Genehmigung unterbreitet, verlangte dieser bereits bisher vom verantwortlichen öffentlichen Organ, dass die Risiken, die mit der geplanten Bearbeitung einhergehen sowie die diesbezüglich geplanten Massnahmen dokumentiert werden. In dieser Hinsicht stellt die Datenschutz-Folgenabschätzung keine grosse Neuerung in der Tätigkeit der öffentlichen Organe dar.

Neu festzuhalten ist sodann eine umfassende Informationspflicht von öffentlichen Organen bei der Beschaffung von Personendaten. Bisher hatte eine Information der betroffenen Person nur zu erfolgen, wenn die Personendaten systematisch erhoben wurden (Art. 7 Abs. 2). Allerdings darf und soll eine Ausnahme von der neuen umfassenden Informationspflicht bestehen, wenn die Datenbearbeitung durch das öffentliche Organ gesetzlich vorgesehen ist. Dies dürfte bei einem Grossteil der Datenbearbeitungen der Fall sein, da Datenbearbeitungen durch öffentliche Organe stets einer gesetzlichen Grundlage bedürfen. Es wird daher nur wenig Mehraufwand erwartet.
Das Gleiche gilt für die neu festzuhaltende Meldepflicht von Datenschutzverletzungen an den Datenschutzbeauftragten. Zu melden sind insbesondere unbefugte Bearbeitungen oder der Verlust von Personendaten, sofern diese zu einer Gefährdung der Grundrechte der betroffenen Person führen (zum Beispiel durch einen Hacker-Angriff). Da solch gravierende Verletzungen die absolute Ausnahme darstellen, wird der mit dieser Verpflichtung einhergehende Mehraufwand für die öffentlichen Organe minimal sein.

Hinzu kommt, dass der Entwurf des neuen kantonalen Datenschutzgesetzes eine Aufhebung der allgemeinen Registerführungspflicht über Datensammlungen vorsieht (Art. 15). Die europäischen Normen verlangen die Führung von Registern über Datenbearbeitungstätigkeiten nur im Bereich der Strafverfolgung und des Strafvollzugs. Künftig sind daher nur noch die Polizei, die Staatsanwaltschaft und die Justizvollzugsbehörde zu verpflichten, ein Register über Datenbearbeitungstätigkeiten zu führen (Art. 17b). Im Übrigen ist angesichts der neuen Transparenzbestimmungen eine umfassende Information der betroffenen Personen auch ohne die Führung eines Registers hinreichend gewährleistet. Eine Aufrechterhaltung der Registerführungspflicht über Datensammlungen ist auch deshalb nicht mehr gerechtfertigt, weil der Begriff der Datensammlung nicht mehr aussagekräftig ist (vgl. Erläuterungen in Synopse). Die Abschaffung der Registerführungspflicht vermindert den Aufwand der öffentlichen Organe im Zusammenhang mit Datenbearbeitungen.

3. Stärkung der kantonalen Aufsichtsstelle

Ein weiteres wichtiges Anliegen der Revisionen ist es, die Datenschutzbeauftragten in ihrer Stellung zu stärken. Im Kanton Schaffhausen kamen der kantonalen Aufsichtsstelle bereits bisher weitge-

hende Befugnisse zu: Sie konnte insbesondere verbindliche Verfügungen, auch in Form vorsorglicher Massnahmen, zulasten der verantwortlichen öffentlichen Organe erlassen. Diese Möglichkeiten müssen auch künftig bestehen bleiben.

Gestärkt werden soll die Unabhängigkeit der kantonalen Aufsichtsstelle. Neu soll im Kanton Schaffhausen gesetzlich festgehalten werden, dass der oder die kantonale Datenschutzbeauftragte keine anderen öffentlichen Ämter bekleiden und keine leitenden Funktionen in politischen Parteien ausüben darf. Eine Abwahl aus dem Amt soll ferner nur dann zulässig sein, wenn Amtspflichten in schwerer Weise vorsätzlich oder grobfahrlässig verletzt werden.

Da die technologischen Entwicklungen der letzten Jahre und die fortschreitende Digitalisierung die Aufgaben der Aufsichtsstelle zunehmend komplexer werden lassen, ist es denkbar, dass die kantonale Aufsichtsstelle in Zukunft auf grössere personelle Ressourcen angewiesen sein wird. Künftig soll deshalb die Möglichkeit bestehen, dass der Aufsichtsstelle durch die Wahlbehörde Kooperationen mit Aufsichtsstellen anderer Kantone oder der Beizug von Fachpersonal genehmigt wird. Diese Regelung wurde von den Vernehmlassungsteilnehmern grundsätzlich begrüsst, wobei Kooperationen mit anderen Kantonen tendenziell bevorzugt werden.

V. Finanzielle und personelle Auswirkungen

Für datenbearbeitende kommunale und kantonale Behörden entsteht aufgrund der Gesetzesrevision ein minimaler Mehraufwand. Dieser wird jedoch dadurch ausgeglichen, dass die Abschaffung der allgemeinen Registerführungspflicht die Behörden entlastet. Unter Umständen werden bei der Staatsanwaltschaft, der Polizei und der Justizvollzugsbehörde Aus- und Weiterbildungskosten für die zu ernennenden Datenschutzberater anfallen. Der hierfür allenfalls anfallende finanzielle Mehraufwand ist voraussichtlich aber überschaubar.

Ganz grundsätzlich bringt es die fortschreitende Digitalisierung mit sich, dass die Aufgaben der Behörden im Bereich Datenschutz zunehmend komplexer werden und für alle Beteiligten ein gewisser Mehraufwand entsteht. Von der zunehmenden Komplexität der Aufgaben besonders betroffen ist aber die kantonale Aufsichtsstelle.

Derzeit besteht die kantonale Aufsichtsstelle aus einer Person, welche ihre Aufgaben nebenamtlich, im Mandatsverhältnis und unter Vorgabe des kantonalen Budgets wahrnimmt. Das Arbeitspensum bewegte sich in den letzten Jahren zwischen 20% und 30%. Es ist möglich, dass mit steigender Arbeitsbelastung und einer Zunahme der Anforderungen an die fachspezifischen Anforderungen künftig Kooperationen mit anderen Kantonen erforderlich werden und ein erhöhter Bedarf an personellen und finanziellen Ressourcen entsteht. Mittelfristig ist mit einem moderaten Anstieg der Kosten für die Aufsichtsstelle zu rechnen, der allerdings nicht genau beziffert werden kann. Eine Aufstockung der personellen Ressourcen der kantonalen Aufsichtsstelle auf 250 Stellenprozente, wie sie seitens eines Vernehmlassungsteilnehmers angeregt wurde, ist aus Sicht der Regierung derzeit nicht angezeigt. Die Entwicklung des Aufwands der Aufsichtsstelle wird aber auf jeden Fall im Auge

zu behalten sein. Sollte ein Mehrbedarf an Mitteln und Stellen für die Aufsichtsstelle festgestellt werden, wäre dieser vom Regierungsrat wie bisher mit dem Budget beim Kantonsrat zu beantragen oder mittels Nachtragskredit einzuholen.

VI. Weitere Rückmeldungen aus dem Vernehmlassungsverfahren

Nebst den bereits erwähnten Rückmeldungen aus dem Vernehmlassungsverfahren wurde seitens der Vernehmlassungsteilnehmer in verschiedenen anderen Bereichen Handlungsbedarf verortet. Beispielweise sei mit Blick auf die mächtigen Datensammler wie Google, Facebook, Amazon usw. zu prüfen, ob ein Gerichtsstand zur Durchsetzung von Persönlichkeitsrechten im Kanton Schaffhausen geschaffen werden könne. Auch Internet-Provider seien mehr in die Pflicht zu nehmen, indem sie zu verpflichten seien, für Schäden, die aufgrund von IT-Kriminalität entstehen, aufzukommen. Weiter gibt der mangelnde Schutz von Minderjährigen im Internet Anlass zur Sorge und es wird gefordert, die Bekämpfung von Cyberkriminalität gesetzlich anzugehen.

Diese Vorbringen und Anregungen haben durchaus ihre Berechtigung und zeigen, wie breit die im Zusammenhang mit dem Datenschutz stehenden Herausforderungen gestreut sind. Zu beachten ist aber, dass der Kanton bei seiner Gesetzgebung an die vom Bund vorgegebenen Kompetenzordnungen gebunden ist. Im Zusammenhang mit Datenbearbeitungen hat der Kanton lediglich die Kompetenz, Datenbearbeitungen durch kantonale Behörden zu regeln. Die Kompetenz zur Regelung der Pflichten privater Datenbearbeiter wie Facebook, Google, Amazon und von Internet-Providern liegt beim Bund, ebenso die dazugehörige Festlegung der Folgen von Pflichtverletzungen durch diese Datenbearbeiter. Auch im Bereich des Zivilrechts (Persönlichkeitsschutz) und des Strafrechts (Cyberkriminalität) liegen die Gesetzgebungskompetenzen beim Bund. Für den Erlass entsprechender Regelungen im kantonalen Datenschutzgesetz besteht daher kein Raum.

In der Vernehmlassung ebenfalls gefordert wurde, dass die Verwendung von AHV-Nummern für die kantonale Verwaltung freizugeben sei. In diesem Zusammenhang sei auf die laufende Revision des Bundesgesetzes über die Alters- und Hinterlassenenversicherung (AHVG [6)]) verwiesen, mit welcher der Bund plant, die Verwendung der AHV-Nummer durch Behörden generell zuzulassen, um effizientere und kostengünstigere Verwaltungsabläufe zu fördern. Das diesbezügliche Vernehmlassungsverfahren wurde vom Bund bereits durchgeführt und der Regierungsrat hat die entsprechenden Änderungsvorschläge in seiner Vernehmlassungsantwort grundsätzlich begrüsst. Im Geltungsbereich des kantonalen Datenschutzgesetzes besteht in diesem Zusammenhang derzeit kein Regelungsbedarf.

Auf die weiteren Vorbringen der Vernehmlassungsteilnehmer wird im Rahmen der Erläuterungen zu den einzelnen Gesetzesbestimmungen eingegangen.

---

6) SR 831.10

VII. Erläuterungen zu den einzelnen Gesetzesbestimmungen

Art. 2 Begriffe

Art. 2 lit. d

Die Bestimmung definiert, welche Daten zur Kategorie der besonders schützenswerten Personendaten gehören. Für die Bearbeitung solcher Daten gelten besonders strenge Voraussetzungen (Art. 5). In die Kategorie der besonders schützenswerten Personendaten fallen unter anderem Daten über die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit einer Person. Der Begriff der Rasse ist in Bezug auf Menschen nicht wissenschaftlicher Natur. Seine Verwendung ist nicht mehr zeitgemäss. Er ist durch den Begriff der ethnischen Herkunft zu ersetzen.

In die Kategorie der besonders schützenswerten Personendaten sind neu genetische Daten und biometrische Daten ausdrücklich aufzunehmen. Genetische Daten sind Informationen über das Erbgut einer Person, die durch eine genetische Untersuchung gewonnen werden; darin eingeschlossen ist auch das DNA-Profil. Biometrische Daten sind mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, welche die eindeutige Identifizierung dieser Person ermöglichen oder bestätigen. Die Aufnahme dieser Begriffe macht redaktionelle Anpassungen der vorangehenden Ziffern notwendig.

Art. 2 lit. e

Sowohl auf Bundesebene als auch in den europäischen Normen wird das Profiling als besonders "gefährliche" Art der Datenbearbeitung eingeführt. Das Profiling ersetzt den bisher verwendeten Begriff des Persönlichkeitsprofils. Der Begriff des Profilings nimmt auf die Art des Bearbeitens von Personendaten Bezug (dynamisch). Demgegenüber knüpfte der bisher verwendete Begriff des Persönlichkeitsprofils an die Art der Daten an (statisch).

Bei der Vornahme eines Profilings werden die über eine Person vorhandenen Daten ausgewertet, um Aussagen über ihr künftiges Verhalten oder weitere Eigenschaften der Person zu treffen. Zu denken ist beispielsweise an Aussagen über die Arbeitsleistung, die wirtschaftlichen Verhältnisse, die Gesundheit, die Vorlieben, den Aufenthaltsort, die Mobilität oder das Gefahrenpotential.
Ein Vernehmlassungsteilnehmer hat angeregt, das Profiling in einem eigenen Absatz zu regeln, um dessen Bedeutung besonderen Ausdruck zu verleihen. Gesetzessystematisch drängt sich aber die vorgeschlagene Regelung der Definition als neue bzw. geänderte lit. e auf. Am Schutzbereich ändert sich nichts. Es wird deshalb an der bereits im Vernehmlassungsverfahren vorgeschlagenen Variante festgehalten.

Art. 2 lit. f

Die Formulierung wird an die Bestimmungen des Bundesrechts und des europäischen Rechts angepasst.

Art. 2 lit. h (aufgehoben)
vgl. Erläuterungen zu Art. 15

Art. 3 Geltungsbereich

Art. 3 Abs. 2 und 4 (neu)
Bisher wurden hängige Verfahren der Zivil-, Verwaltungs- und Strafrechtspflege generell vom Geltungsbereich des Datenschutzgesetzes ausgenommen. Eine solch generelle Ausnahme für gerichtliche Verfahren ist aufgrund der europäischen Vorgaben nicht mehr zulässig. Zwar können und sollen auch künftig in hängigen Verfahren der Rechtspflege betreffend Informationsansprüche (Akteneinsichtsrechte Dritter sowie Rechte der Parteien) die entsprechenden Prozessordnungen zur Anwendung kommen. Das Datenschutzgesetz soll aber insbesondere hinsichtlich der Bestimmung der für die Bearbeitung verantwortlichen Behörde, die Datensicherheit etc. zur Anwendung kommen.

Keine Anwendung soll dem Datenschutzgesetz zukommen, soweit in einem Verfahren die entsprechenden Prozessordnungen zur Anwendung gelangen. Im Bereich des Strafprozessrechts wird damit nicht nur das gerichtliche Verfahren erfasst, sondern auch das in der eidgenössischen Strafprozessordnung geregelte Vorfahren der Ermittlungs- und Untersuchungsbehörden.

Ein Vernehmlassungsteilnehmer bemängelt die in Abs. 2 getroffene Regelung als zu wenig klar. Die Bestimmung legt aber unmissverständlich fest, für welche Bereiche das Datenschutzgesetz in gerichtlichen Verfahren nicht zur Anwendung gelangt, nämlich soweit in hängigen Verfahren die Rechte der von den Datenbearbeitungen betroffenen Personen sowie die Akteneinsichtsrechte Dritter betroffen sind. Wie eine genauere Formulierung aussehen sollte, wurde vom Vernehmlassungsteilnehmer nicht näher erläutert.

Auch im Bereich der Aufsicht darf und soll aus Gründen der richterlichen Unabhängigkeit weiterhin eine generelle Ausnahme vom Geltungsbereich der datenschutzrechtlichen Bestimmungen für Gerichte vorgesehen werden. Gerichte unterstehen damit nicht der kantonalen Aufsichtsstelle gemäss Art. 23 ff.. Sie haben die Aufsicht selbständig zu regeln. Soweit öffentliche Organe privatrechtlich handeln und ohne hoheitliche Befugnisse am wirtschaftlichen Wettbewerb teilnehmen, darf weiterhin eine Ausnahme vom Geltungsbereich des kantonalen Datenschutzgesetzes vorgesehen werden. Es ist damit weiterhin zulässig, die für private Datenbearbeiter anwendbaren Regeln des Bundesdatenschutzgesetzes in diesem Fällen auch für öffentliche Organe für anwendbar zu erklären. Der bestehende Abs. 3 kann daher beibehalten werden.

Art. 4

Art. 4 Abs. 1
Ein Vernehmlassungsteilnehmer hat darauf hingewiesen, dass die Bearbeitung "normaler" Personendaten gemäss bestehendem Art. 4 stets einer gesetzlichen Grundlage bedürfe und die Einwilligung der betroffenen Person, anders als bei besonders schützenswerten Personendaten, die gesetzliche Grundlage nicht ersetze. Im Resultat bestünden deshalb höhere Anforderungen an die

Bearbeitung "normaler" Personendaten als an die Bearbeitung besonders schützenswerter Personendaten.

Ausserdem sei aufgrund der Formulierung in Abs. 1 nicht klar, ob für die Bearbeitung eine ausdrückliche gesetzliche Grundlage bestehen müsse, oder ob es ausreiche, wenn die Datenbearbeitung im Rahmen eines gesetzlichen Auftrags erfolge.

Diese Vorbringen sind berechtigt. Tatsächlich ist nicht einzusehen, weshalb die Einwilligung der betroffenen Person bei der Bearbeitung "normaler" Personendaten die gesetzliche Grundlage nicht zu ersetzen vermögen soll, bei besonders schützenswerten Personendaten hingegen schon. Art. 4 ist entsprechend anzupassen. Der Klarheit halber ist sodann festzuhalten, dass behördliche Datenbearbeitungen auch dann zulässig sind, wenn sie zur Erfüllung der gesetzlich umschriebenen Aufgaben geeignet und erforderlich sind. Dies entspricht der bereits heute angewandten Praxis.

Art. 5

Für das neu einzuführende Profiling haben die gleichen Anforderungen zu gelten wie für die Bearbeitung besonders schützenswerter Personendaten (vgl. Ausführungen zu Art. 2 lit. e). Ein Profiling darf entsprechend nur vorgenommen werden, wenn eine gesetzliche Grundlage in Form eines formellen Gesetzes besteht oder wenn die betroffene Person der Bearbeitung ausdrücklich zugestimmt hat bzw. ihre Zustimmung unzweifelhaft vorausgesetzt werden darf.

Art. 5a Informationspflicht beim Beschaffen von Personendaten

Art. 5a Abs. 1-4

Art. 5a verpflichtete den Inhaber einer Datensammlung bisher, die betroffene Person über die Beschaffung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen zu informieren. Art. 7bis des Übereinkommens SEV 108 und Art. 13 der Richtlinie (EU) 2016/680 verlangen nun, dass das verantwortliche öffentliche Organ die betroffene Person über sämtliche Beschaffungen von Personendaten informiert, unabhängig davon, ob es sich um besonders schützenswerte Daten handelt. Diese generelle Informationspflicht trägt dem Hauptanliegen der Revision nach einer verbesserten Transparenz bei der Datenbearbeitung Rechnung. Die Informationspflicht hat auch zu gelten, wenn die Daten bei Dritten beschafft werden. Sie entfällt, wenn die betroffene Person bereits über die Informationen verfügt, die Bearbeitung gesetzlich vorgesehen ist oder die Information nicht oder nur mit unverhältnismässigem Aufwand möglich ist. Da Datenbearbeitungen durch öffentliche Organe ohnehin nur zulässig sind, wenn dafür eine gesetzliche Grundalge besteht (Art 4 Abs. 1) und bei Vorliegen einer gesetzlichen Grundlage für die Bearbeitung keine Informationspflicht besteht, wird der allgemeinen Informationspflicht indessen bei behördlichen Datenbearbeitungen wenig praktische Bedeutung zukommen.

Die Information muss nicht zwingend individuell erfolgen, sondern ist auch in allgemeiner Form z.B. auf einer Homepage zulässig. Das verantwortliche öffentliche Organ muss aber sicherstellen, dass

die betroffene Person die Information tatsächlich zur Kenntnis nehmen kann. Werden Daten systematisch erhoben (z.B. auf Anmelde-/Gesuchsformularen) können die Angaben direkt auf dem Formular angebracht werden.

In Verfahren der Zivil-/Straf- und Verwaltungsrechtspflege richten sich die Informationsansprüche weiterhin nach dem anwendbaren Verfahrensrecht (vgl. Art. 3).

Verschiedene Vernehmlassungsteilnehmer kritisieren die vorgeschlagene Bestimmung als zu restriktiv. Es wird vorgeschlagen, die Informationspflicht auf besonders schützenswerte Personendaten zu beschränken oder Ausnahmen gemäss Abs. 4 zu erweitern, indem beispielsweise keine "ausdrückliche" gesetzliche Grundlage gefordert werde. Eine weniger restriktive Formulierung, insbesondere eine Beschränkung der Informationspflicht auf besonders schützenswerte Personendaten, wäre aber mit den europäischen Normen nicht vereinbar. Zur in Abs. 4 geforderten "ausdrücklichen" gesetzlichen Grundlage ist erläuternd zu bemerken, dass eine solche gegeben ist, wenn aus der fraglichen Gesetzesbestimmung für die betroffene Person hervorgeht, zu welchem Zweck welche Daten von ihr erhoben werden und was mit diesen geschieht. Ist dies nicht der Fall, hat eine Information nach Abs. 2 zu erfolgen.

Ferner wurde in der Vernehmlassung darauf hingewiesen, dass eine Informationspflicht nur bei der Beschaffung von Personendaten bei Dritten Sinn mache. Würden die Daten bei der betroffenen Person erhoben, sei diese automatisch über die Beschaffung informiert. Dies trifft nur teilweise zu, denn es reicht eben gerade nicht aus, wenn die betroffene Person zwar über die Beschaffung Bescheid weiss, aber nicht darüber aufgeklärt wird, gestützt auf welche Grundlage die Erhebung erfolgt, wozu und von wem die Daten verwendet werden und welche Rechte sie im Zusammenhang mit der Datenbearbeitung hat.

Art. 6 Verantwortung

Art. 6 Abs. 1 und 2

Art. 6 regelt, welches öffentliche Organ die Verantwortung für die rechtmässige Bearbeitung von Personendaten trägt. Die Definition des verantwortlichen öffentlichen Organs wird mit jener des Bundesrechts, der Richtlinie (EU) 2016/680 sowie des Übereinkommens SEV 108 in Einklang gebracht. Die Aufhebung des Begriffs der Datensammlung (vgl. Art. 2 lit. h) macht sodann eine Anpassung von Abs. 2 notwendig.

Art. 7 Erhebung

Art. 7 Abs. 2 (aufgehoben)

Die neue und umfassende Informationspflicht bei der Beschaffung von Personendaten von Art. 5a macht eine besondere Regelung für die systematische Erhebung von Personendaten überflüssig.

Art. 8 Bekanntgabe a) allgemein

Art. 8 Abs. 3 (neu)

Die Bekanntgabe von Daten stellt eine Form des Bearbeitens dar (vgl. Art. 2 lit. f). Die Bekanntgabe von besonders schützenswerten Personendaten und von Resultaten eines Profilings ist daher nur unter den erhöhten Anforderungen von Art. 5 zulässig. Der Klarheit halber ist ausdrücklich auf diesen Umstand hinzuweisen.

Das kantonale Organisationsgesetz vom 18. Februar 1985 [7)] stellt für die Bekanntgabe von besonders schützenswerten Personendaten keine hinreichende gesetzliche Grundlage dar. Zwar ist in dessen Art. 8a als Ausfluss des Öffentlichkeitsprinzips unter gewissen Voraussetzungen für jedermann ein Einsichtsrecht in amtliche Akten vorgesehen. Besonders schützenwerte Personendaten werden dort aber nicht ausdrücklich erwähnt, weshalb das Organisationsgesetz nicht als hinreichende formellgesetzliche Grundlage im Sinne von Art. 5 gesehen werden kann. Verlangt eine Person gestützt auf Art. 8a des Organisationsgesetzes Einsicht in amtliche Dokumente, die besonders schützenswerte Personendaten enthalten, dürfen diese mit anderen Worten nur bekannt gegeben werden, wenn die betroffene Person dem ausdrücklich zustimmt. Ansonsten ist zu prüfen, ob eine Anonymisierung der Daten möglich oder das Einsichtsgesuch abzuweisen ist.

Art. 11a e) Bekanntgabe an europäische Staaten

Art. 11a und 11b regeln die Voraussetzungen für die Bekanntgabe von Daten an ausländische Staaten. Art. 11a hält fest, dass für die Bekanntgabe an Mitgliedstaaten der Europäischen Union sowie des Europäischen Wirtschaftsraums die gleichen Voraussetzungen gelten wie für die Bekanntgabe im Inland. Bei diesen Staaten wird mit anderen Worten ohne weiteres davon ausgegangen, dass sie über ein angemessenes Datenschutzniveau verfügen. Da sämtliche Mitgliedstaaten des Übereinkommen SEV 108 über ein gleichwertiges und angemessenes Datenschutzniveau verfügen müssen, darf eine Vertragspartei die Weitergabe von Personendaten an eine andere Vertragspartei nicht von einer besonderen Genehmigung abhängig machen (Art. 12 Ziff. 1 des Übereinkommens SEV 108). Art. 11a muss daher richtigerweise festhalten, dass auch die Bekanntgabe an Mitgliedstaaten des Übereinkommens SEV 108 an keine weitergehenden Voraussetzungen geknüpft ist, als die innerstaatliche Datenbekanntgabe.

Art. 11b f) Bekanntgabe von Personendaten an Drittstaaten

Art. 11b Abs. 1 und 2

Unter Drittstaaten sind in Abgrenzung zur Regelung von Art. 11a Staaten zu verstehen, die weder Mitglied der Europäischen Union noch des Europäischen Wirtschaftsraums oder Vertragspartei des Übereinkommens SEV 108 sind. An diese Staaten dürfen Daten nur bekannt gegeben werden, wenn dort ein angemessenes Datenschutzniveau gewährleistet ist. Zur Beurteilung der An-

7) SHR 172.100.

gemessenheit des Datenschutzniveaus wurde bisher fälschlicherweise auf Art. 2 Ziff. 2 des *Zusatzprotokolls des Europarats vom 8. November 2001* zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung von personenbezogenen Daten (SEV Nr. 108) verwiesen. Richtigerweise ist auf das Übereinkommen SEV 108 zu verweisen, welches die grundsätzlichen Leitlinien dafür enthält, wie ein Staat ein angemessenes Datenschutzniveau zu gestalten hat.

Im Hinblick auf die Beurteilung, ob ein Staat ein angemessenes Datenschutzniveau gewährleistet, veröffentlichte der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) bisher eine Liste, in welcher die Staaten mit einer angemessenen Datenschutzgesetzgebung aufgeführt sind. Der Entwurf des revidierten Datenschutzgesetzes des Bundes sieht vor, dass künftig der Bundesrat die Angemessenheit der ausländischen Gesetzgebungen und deren Anwendung prüft und die Resultate in einer Verordnung festhält. Sehen sich kantonale Behörden mit der Frage konfrontiert, ob ein Drittstaat über ein angemessenes Datenschutzniveau verfügt, sind die entsprechenden Vorgaben und Prüfungsergebnisse des Bundes zu beachten.

Art. 13 Bearbeiten im Auftrag

Art. 13 Abs. 1 und 2 sowie Abs. 3 und 4 (neu)

Art. 13 schafft die gesetzliche Grundlage dafür, dass öffentliche Organe eine dritte Stelle mit der Bearbeitung von Daten beauftragen können. Die Bestimmung ist von grosser praktischer Bedeutung und findet auf eine Vielzahl von Fällen Anwendung. Aufgrund der technologischen Entwicklung der letzten Jahre haben elektronische Datenbearbeitungen stark zugenommen. Gerade in diesem Bereich sind öffentliche Organe vermehrt darauf angewiesen, Informatikleistungen von Dritten in Anspruch zu nehmen. Solche Dienstleistungen können beispielsweise in Betrieb und Wartung von IT-Infrastruktur oder Software bestehen, im Hosting von Websites oder Analysetools oder in der Inanspruchnahme von Cloud Services. Auftragsdatenbearbeitungen im Sinne des Gesetzes liegen aber auch dann vor, wenn ein Dritter für das öffentliche Organ ein "Produkt" aus Informationen des öffentlichen Organs herstellt. Dies ist beispielsweise der Fall, wenn ein Dritter im Auftrag des öffentlichen Organs ein Gutachten verfasst oder das Inkasso für ausstehende Rechnungen ausgelagert wird. Beim beauftragten Dritten kann es sich um andere öffentliche Organe oder um Private handeln und die Bearbeitungen können im Kanton Schaffhausen oder ausserhalb stattfinden.

Art. 22 f. RL 2016/680 stellt klare Voraussetzungen für das Bearbeiten von Personendaten durch einen Dritten auf. Es 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. Das öffentliche Organ bleibt für die Rechtmässigkeit der Bearbeitung verantwortlich. Die Übertragung auf weitere Auftragsdatenbearbeitende darf nur mit schriftlicher Genehmigung des verantwortlichen öffentlichen Organs erfolgen.

Art. 14 Informationssicherheit (neuer Randtitel)

Art. 14 verpflichtet die öffentlichen Organe, Daten durch technische und organisatorische Massnahmen vor Verlust, Entwendung und unbefugtem Bearbeiten zu schützen. Der im Randtitel verwendete Begriff der Datensicherung ist überholt und missverständlich. Stattdessen soll der Begriff der Informationssicherheit im Randtitel verwendet werden.

Art. 14 Abs. 2 (neu)

Neu ist vom verantwortlichen öffentlichen Organ nachzuweisen, dass die Bestimmungen der Informationssicherheit bei sämtlichen Datenbearbeitungen eingehalten werden. Der Nachweis ist durch den Erlass geeigneter Organisationsvorschriften, Informationssicherheitsrichtlinien und Zugriffskonzepte zu erbringen und in der kantonalen Datenschutzverordnung näher zu regeln.

Art. 14a Meldung von Datenschutzverletzungen (neu)

Gemäss Art. 7 Ziff. 2 des Übereinkommens SEV 108 und Art. 30 und 31 der Richtlinie (EU) 2016/680 ist eine Meldung von Datenschutzverletzungen durch das verantwortliche öffentliche Organ an die Aufsichtsstelle und an die betroffene Person vorzusehen.

Der Begriff der Datenschutzverletzung wird in Abs. 5 definiert. Demnach sind darunter der unbeabsichtigte Verlust der Daten oder deren Vernichtung zu verstehen, die unbeabsichtigte oder unrechtmässige Veränderung oder Offenbarung an einen Dritten oder Fälle, in denen sich Dritte unbefugt Zugang zu den Daten beschaffen. In diesen Fällen hat eine Meldung des öffentlichen Organs an die kantonale Aufsichtsstelle zu erfolgen. Dies allerdings nur dann, wenn die Verletzung voraussichtlich zu einem hohen Risiko für die Grundrechte der betroffenen Person führt. Im Vernehmlassungsentwurf wurde in diesem Zusammenhang noch der Begriff der "Gefährdung von Grundrechten" verwendet. Dieser stiess von verschiedenen Seiten auf Kritik, da er zu unklar sei. Im vorliegenden Entwurf wird nun der Begriff des "hohen Risikos für die Grundrechte" verwendet. Auch hierbei handelt es sich um einen unbestimmten Rechtsbegriff, welcher der Konkretisierung durch Rechtsanwendung und Rechtsprechung bedarf. Der gleiche Begriff wird im SDSG und in der Richtlinie (EU) 2016/680 verwendet. Zur Konkretisierung wird also auf Erläuterungen und Entscheide zu diesen Bestimmungen abgestützt werden können. Grundsätzlich darf der Begriff nicht zu weit ausgelegt werden. Es geht bei der Einschränkung vielmehr darum, Bagatellfälle, (z.B. wenn verlorene Daten ohne weitere Folgen über ein Backup wieder hergestellt werden können) von der Meldepflicht auszunehmen.

Werden Daten im Auftrag bearbeitet, hat die beauftragte Stelle Datenschutzverletzungen unverzüglich dem verantwortlichen öffentlichen Organ mitzuteilen (Abs. 2), welches die Aufsichtsstelle und gegebenenfalls die betroffene Person zu informieren hat. Dieses Vorgehen steht im Einklang mit der Bestimmung von Art. 13, wonach das öffentliche Organ für Datenbearbeitungen verantwortlich bleibt. Bei der Erteilung des Auftrags ist sicherzustellen, dass die beauftragte Stelle sich an die Mitteilungspflicht hält. Im Vernehmlassungsverfahren wurde darauf hingewiesen, dass Abs. 1 den Begriff "ohne unangemessene Verzögerung" verwende, während in Abs. 2 eine "unverzügliche" Meldung vorgesehen sei. Es seien einheitliche Begriffe zu verwenden. Die genannte Unterscheidung ist

jedoch gewollt und soll deutlich machen, dass die Meldung von Auftragsdatenbearbeitenden an das verantwortliche öffentliche Organ weniger Aufschub zulässt, als dies bei der Meldung des öffentlichen Organs an die Aufsichtsstelle der Fall ist. Beide Meldungen haben aber natürlich so rasch wie möglich zu erfolgen.

Die betroffene Person ist über die Datenschutzverletzung zu informieren, wenn dies zu ihrem Schutz erforderlich ist (zu denken ist etwa an Änderungen von Zugangsdaten oder Passwörtern) oder wenn die kantonale Aufsichtsstelle dies verlangt (Abs. 3). Die Information der betroffenen Person kann aber eingeschränkt oder aufgehoben werden, wenn überwiegende öffentliche oder private Geheimhaltungsinteressen vorliegen (Abs. 4). Auf entsprechende Anregung im Vernehmlassungsverfahren wird vorgesehen, dass der Verzicht auf eine Information der betroffenen Person gestützt auf Abs. 4 stets der Aufsichtsstelle zu melden ist. So ist sichergestellt, dass die Information nicht in ungerechtfertigter Weise unterbleibt.

Ein Vernehmlassungsteilnehmer hat beantragt, die vorgeschlagene Bestimmung ersatzlos zu streichen. Dies mit der Begründung, die strafrechtlichen Folgen bei unbeabsichtigtem Handeln seien nicht klar, fahrlässiges und grobfahrlässiges Handeln dürfe nicht belangt werden. Es ist in diesem Zusammenhang darauf hinzuweisen, dass es sich bei Art. 14a nicht um eine Strafbestimmung handelt. Ob eine Datenschutzverletzung auf ein strafbares Verhalten der Behörden zurückzuführen ist, ist anhand des Strafgesetzbuches, nicht des Datenschutzgesetzes zu beurteilen. Art. 14a soll lediglich den Schutz der von Datenschutzverletzungen betroffenen Personen sicherstellen bzw. generell einen ausreichenden Datenschutz gewährleisten. In diesem Zusammenhang spielt es keine Rolle, ob eine Verletzung vorsätzlich oder fahrlässig erfolgt ist, die Aufsichtsstelle und die betroffene Person müssen in beiden Fällen über die Verletzung informiert werden.

Art. 14b Datenschutz-Folgenabschätzung (neu)

Die übergeordneten Rechtsgrundlagen (namentlich Art. 8bis Ziff. 3 des Übereinkommens SEV 108 und Art. 27 der Richtlinie (EU) 2016/680) statuieren für geplante Datenschutzvorhaben die Pflicht zur Vornahme einer sogenannten "Datenschutz-Folgenabschätzung" durch das verantwortliche öffentliche Organ. Dieses Instrument dient dazu, Risiken zu erkennen und zu bewerten, welche für die betroffene Person durch den Einsatz bestimmter Datenbearbeitungen entstehen können. Auf der Basis der Abschätzung sollen gegebenenfalls angemessene Massnahmen definiert werden, um diese Risiken für die betroffene Person zu bewältigen. Dem verantwortlichen öffentlichen Organ erlaubt die Abschätzung, allfällige datenschutzrechtliche Probleme präventiv anzugehen.

Eine Datenschutz-Folgenabschätzung ist nicht bei jeder geplanten Bearbeitung vorzunehmen, sondern nur dann, wenn die vorgesehene Bearbeitung voraussichtlich zu einem erhöhten Risiko für die Grundrechte der betroffenen Person führen kann. Davon ist beispielsweise auszugehen, wenn es sich um eine umfangreiche Bearbeitung besonders schützenswerter Personendaten handelt oder wenn öffentliche Bereiche systematisch und umfangreich überwacht werden. Ergibt sich aus der

Datenschutz-Folgenabschätzung, dass die Bearbeitung tatsächlich ein hohes Risiko für die Grundrechte der betroffenen Person mit sich bringt, ist das Vorhaben der Aufsichtsstelle zur Vorabkonsultation zu unterbreiten (vgl. Art. 14c).

Auch Art. 8bis Ziff. 2 des Übereinkommens SEV 108 und Art. 27 der Richtlinie (EU) 2016/680 sehen die Verpflichtung vor, bei Vorhaben für Personendatenverarbeitungen eine Datenschutz-Folgenabschätzung vorzunehmen.

Zwar war das Instrument der Datenschutzfolgenabschätzung bisher im Gesetz nicht verankert. Wurde dem kantonalen Datenschutzbeauftragten aber ein automatisiertes Verfahren zur Verarbeitung von personenbezogenen Daten zur Vorabkontrolle unterbreitet (alter Art. 16a), verlangte dieser vom öffentlichen Organ bereits bisher die nun ausdrücklich in Art. 14b genannten Auskünfte. In diesem Sinne ändert sich in der Praxis für die öffentlichen Organe wenig.

Art. 14c Vorabkonsultation (neu)

Ergibt sich aus der Datenschutz-Folgenabschätzung, dass die geplante Bearbeitung ein hohes Risiko für die Grundrechte der betroffenen Person zur Folge hat, ist eine Stellungnahme der kantonalen Aufsichtsstelle einzuholen. Ziel der Vorabkonsultation ist es, den Datenschutz rechtzeitig sicherzustellen. Die Vorabkonsultation entspricht inhaltlich im Wesentlichen der Vorabkontrolle gemäss bisherigem Art. 16a.

Die Aufsichtsstelle hat dem verantwortlichen Organ innert angemessener Frist allfällige Einwände mitzuteilen. Da im Vernehmlassungsverfahren vorgebracht wurde, es bestünden nicht in jedem Fall Einwendungen der Aufsichtsstelle, ist im vorliegenden Entwurf von "allfälligen Einwänden" und nicht mehr nur von "Einwänden" die Rede. Ist die Aufsichtsstelle der Ansicht, dass die geplante Bearbeitung Datenschutzvorschriften verletzt und weigert sich das öffentliche Organ, geeignete Massnahmen zum Schutz der Daten zu treffen, kann sie Massnahmen nach Art. 26 ergreifen.

Art. 15 Register (aufgehoben)

Datenbestände, die so aufgebaut sind, dass sie nach einer bestimmten Person erschliessbar sind, wurden bisher als Datensammlungen bezeichnet. Die öffentlichen Organe waren verpflichtet, über die bei ihnen vorhandenen Datensammlungen ein öffentliches Register zu führen. Die kantonale Aufsichtsstelle hatte sodann ein zentrales Register über sämtliche bei den öffentlichen Organen vorhandenen Datensammlungen zu führen (Art. 16). Die Register sollten Transparenz darüber schaffen, welche Daten zu welchem Zweck von Behörden über einzelne Personen gesammelt werden. Der Begriff der Datensammlung hat angesichts der technologischen Entwicklungen an Bedeutung und Schärfe verloren. Es bezieht sich auf in Karteikartensystemen oder Ordnern nach Namen abgelegte Daten. Heute ist praktisch jede elektronische Ablage von Dokumenten mittels Suchfunktion nach bestimmten Personen erschliessbar und als Datensammlung im Sinne der gesetzlichen Definition zu beurteilen.

Angesichts dieser Entwicklung sagt das Vorhandensein einer nach Namen aufgebauten Datensammlung nicht mehr viel darüber aus, welche Daten, die von öffentlichen Organen bearbeitet werden, in Bezug zu einer bestimmten Person gesetzt werden können. Der Zusammenzug von Daten aus elektronischen Ablagen erlaubt auch dann umfassende Aussagen über eine betroffene Person, wenn keine eigentlich nach Namen aufgebaute Datensammlung vorhanden ist. Um für die betroffenen Personen weiterhin Transparenz zu schaffen, ist es zielführender, sie mit umfassenden Informations- und Auskunftsrechten zu versehen. Im revidierten Datenschutzgesetz werden die Behörden entsprechend verpflichtet, betroffene Personen über jede Datenbeschaffung zu informieren und nicht wie bisher nur über die Beschaffung besonders schützenswerter Personendaten (vgl. Art. 5a). Auch haben betroffene Personen Anspruch darauf, jederzeit von den Behörden Auskunft darüber zu erhalten, welche Daten zu welchem Zweck über sie konkret bearbeitet werden (vgl. Art. 19).

Die allgemeine Registerführungspflicht ist daher aufzuheben. Einzig im besonders sensiblen Bereich der Strafverfolgung (Polizei, Staatsanwaltschaft, Justizvollzug) verlangen die europäischen Normen weiterhin die Führung eines Registers. Diese Registerführungspflicht wird neu in Art. 17b geregelt.

Soweit die Vernehmlassungsteilnehmer sich zur Aufhebung der Registerführungspflicht geäussert haben, wurde diese begrüsst. Lediglich ein Vernehmlassungsteilnehmer hat sich für die Beibehaltung der Pflicht ausgesprochen, um den Betroffenen den bestmöglichen Datenschutz zu gewährleisten. Da die Registerführungspflicht für die öffentlichen Organe mit einem beträchtlichen Aufwand verbunden ist, der für die von den Datenbearbeitungen betroffenen Personen entstehende Mehrwert nach der vorliegenden Revision indessen marginal, wird an der vorgeschlagenen Aufhebung der Registerführungspflicht festgehalten.

Art. 16 zentrales Register (aufgehoben)

Da die allgemeine Registerführungspflicht aufgehoben wird, ist auch kein zentrales Register durch die Aufsichtsstelle mehr zu führen (vgl. vorstehende Ausführungen zu Art. 15 sowie zu Art. 2 lit. h).

Art. 16a Vorabkontrolle (aufgehoben)

Das Instrument der Vorabkontrolle wird aufgehoben und durch die weitgehend identische Vorabkonsultation ersetzt (vgl. Art. 14c).

Art. 17 Vernichtung und Archivierung

Art. 17 Abs. 1

Da der Begriff der Datensammlung aufzuheben ist (vgl. Art. 2 lit. h), muss vom verantwortlichen öffentlichen Organ auch nicht mehr festgelegt werden, wann Datensammlungen zu vernichten sind.

Art. 17a Information der Empfänger von Personendaten (neu)

Werden Personendaten berichtigt, gelöscht, vernichtet oder mit dem Vermerk versehen, dass ihre Richtigkeit bestritten ist, sich aber weder Richtigkeit noch Unrichtigkeit beweisen lässt, sind sämtliche Stellen und Personen, welche die Daten vorgängig empfangen haben, über diese Vorgänge zu

informieren. Diese Mitteilungspflicht wird von Art. 16 Abs. 5 der Richtlinie (EU) 2016/680 gefordert. Auf entsprechende Anregung im Vernehmlassungsverfahren wurde im Gesetz ausdrücklich ergänzt, dass die Empfänger nur dann zu informieren sind, wenn anzunehmen ist, dass die Daten von ihnen noch verwendet werden. Werden berichtigte Daten automatisiert in die Datensysteme der Empfänger übertragen, ist der Informationspflicht genüge getan.

Von einer Mitteilung darf nur abgesehen werden, wenn sie nicht oder nur mit unverhältnismässigem Aufwand erfolgen kann. Davon darf nicht leichthin ausgegangen werden. Das verantwortliche öffentliche Organ muss in der Regel zumindest versuchen, eine entsprechende Mitteilung vorzunehmen. Im Vernehmlassungsverfahren wurde angeregt, eine Meldepflicht sämtlicher Fälle an die Aufsichtsstelle vorzusehen, bei denen von einer Mitteilung abgesehen wird. Eine solche Meldepflicht würde einen beträchtlichen Aufwand einerseits für die datenbearbeitenden Behörden, insbesondere aber für die Aufsichtsstelle mit sich bringen. Dieser Aufwand steht in keinem angemessenen Verhältnis zum Schutz, der die Bestimmung für betroffene Personen bietet. Von einer entsprechenden Ergänzung wurde daher abgesehen.

Art. 17b Strafverfolgung und Justizvollzug, a) Register (neu)

Gemäss Art. 24 der Richtlinie (EU) 2016/680 sind die Strafverfolgungs- und Strafvollzugsbehörden zu verpflichten, ein Register über Datenbearbeitungstätigkeiten zu führen. Bisher bestand eine entsprechende Registerführungspflicht für alle öffentlichen Organe. Neu sind nur noch die Polizei, die Staatsanwaltschaft und die Justizvollzugsbehörde zur Führung solcher Register verpflichtet. Der notwendige Mindestinhalt der Register entspricht dem bisher in Art. 15 umschriebenen.

Art. 17c b) Datenschutzberatung (neu)

Art. 32-34 der Richtlinie (EU) 2016/680 verlangen, dass die Strafverfolgungs- und Strafvollzugsbehörden innerhalb ihrer Organisation einen sogenannten Datenschutzberater oder eine Datenschutzberaterin zu ernennen (in der Richtlinie als "Datenschutzbeauftragte" bezeichnet) haben. Die Datenschutzberater sind von der Behörde selbst zu benennen und in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen einzubinden. Sie haben die Mitarbeitenden der Behörde bei der Bearbeitung von Personendaten und der Einhaltung von Datenschutzvorschriften und der Datensicherheit zu beraten und zu unterstützen. Sodann beraten sie die Behörde im Zusammenhang mit der Durchführung von Datenschutz-Folgenabschätzungen (vgl. Art. 14b). Ausserdem fungieren sie als Anlaufstelle für die kantonale Aufsichtsstelle.

In der Vernehmlassung wurde angeregt, anstelle des Begriffs "Datenschutzberatung" den Begriff "Datenschutzverantwortliche" zu verwenden. Dieser Begriff würde allerdings ein falsches Bild vermitteln. Die für die Datenschutzberatung zuständigen Personen tragen keine formelle Verantwortung für die korrekte Datenbearbeitung durch die Behörde. Sie sollen lediglich kompetente Ansprechpersonen für datenschutzrechtliche Fragestellungen sein.

Art. 18 Auskunftsrecht; a) Grundsatz der Transparenz und Informationsanspruch

Im Sinne einer redaktionellen Berichtigung ist im Randtitel der Buchstabe a) einzufügen, da der folgende Art. 19 unter Buchstabe b) die Einschränkungen des Auskunftsrechts regelt.

Da der Begriff der Datensammlung aufgehoben wird (vgl. Art. 2 lit. h), kann Abs. 1 aufgehoben werden. Dem Auskunftsrecht gemäss Abs. 1 kommt angesichts der umfassenden Informations- und Auskunftsrechte hinsichtlich sämtlicher Datenbeschaffungen und Datenbearbeitungen durch öffentliche Organe ohnehin keine relevante selbständige Bedeutung mehr zu. So ist die betroffene Person grundsätzlich von Amtes wegen über sämtliche Datenbeschaffungen zu informieren (vgl. Art. 5a). Auch ist ihr aufgrund der Änderungen von Abs. 2 von den Behörden auf Verlangen Auskunft darüber zu erteilen, ob und welche Daten über sie bearbeitet werden und zwar unabhängig davon, ob die Daten sich in einer Datensammlung befinden oder nicht. Der betroffenen Person sind die gleichen Angaben zu machen wie bei der Information über Datenbeschaffungen gemäss Art. 5a. Zusätzlich ist über die Dauer der Aufbewahrung sowie über die Herkunft der Daten zu informieren.

Auf entsprechende Anregung in der Vernehmlassung wurde im vorliegenden Entwurf ein neuer Abs. 2^{bis} eingefügt, der klarstellt, dass persönliche Arbeitsmittel, namentlich persönliche Notizen, nicht vom Auskunftsrecht erfasst werden. Eine entsprechende Bestimmung kannte das bisherige Recht auch für Datensammlungen (Art. 15 Abs. 3 lit. b). Weitergehende Ausnahmen vom Recht auf Auskunft sind aufgrund der europäischen Normen nicht zulässig.

Die Auskunftserteilung hat dem Grundsatz nach weiterhin kostenlos zu erfolgen (Abs. 3). Sind zum Schutz berechtigter Interessen Dritten aufwendige administrative Massnahme zu treffen, darf von der zuständigen Behörde eine angemessene Gebühr verlangt werden (lit. a). Gemeint sind damit insbesondere Fälle, bei denen zum Schutz von Persönlichkeitsrechten Dritter umfangreiche Anonymisierungsmassnahmen (Schwärzungen) vorzunehmen sind. Eine angemessene Gebühr kann ferner verlangt werden, wenn der Auskunftsantrag rechtsmissbräuchlich ist, namentlich bei exzessiven Anträgen in derselben Angelegenheit oder bei offensichtlicher Unbegründetheit (lit. b). Diese Bestimmung wurde aufgrund verschiedener Rückmeldungen in der Vernehmlassung leicht angepasst, um zu verdeutlichen, dass nicht leichthin von diesen Ausnahmen ausgegangen werden darf. Auch ist darauf hinzuweisen, dass die Gebühr angemessen sein muss. Verursacht ein rechtsmissbräuchlicher Antrag keinen oder einen vernachlässigbaren Aufwand für die Behörde, ist die Erhebung einer Gebühr nicht gerechtfertigt.

Art. 19 b) Einschränkung

Abs. 2 (aufgehoben)

Die Transparenz bei Datenbearbeitungen ist ein Kernanliegen des Datenschutzrechts. Einschränkungen des Auskunftsrechts der betroffenen Person sind daher nur in engen Grenzen zulässig. Die bisher vorgesehenen Möglichkeiten der Einschränkung bei Vorliegen von überwiegenden öffentlichen Interessen (z.B. Schutz vor Vereitelung einer Strafverfolgung) oder schutzwürdigen Interessen Dritter (z.B. Schutz weiterer betroffener Personen) sind weiterhin zulässig (Abs. 1). Die bisher in

Abs. 2 vorgesehene Regelung, wonach das Auskunftsrecht vom Vorliegen eines schutzwürdigen Interesses des Gesuchstellers abhängig gemacht werden kann, wenn dessen Geltendmachung zu einem unverhältnismässigen Verwaltungsaufwand führen würde, ist demgegenüber nicht mit den europäischen Normen vereinbar. Das Recht, Auskunft über die persönlichen Daten zu erhalten, ist Teil des Persönlichkeitsrechts. Das Vorliegen eines schutzwürdigen Interesses kann daher stets vorausgesetzt werden. Verursacht die Erteilung der Auskunft einen grossen administrativen Aufwand, um berechtigte Interessen Dritter zu schützen, kann eine angemessene Gebühr für die Auskunftserteilung verlangt werden (Art. 18 Abs. 3). Eine weitergehende Einschränkung des Rechts auf Auskunft ist nicht angezeigt.

Art. 20 Berichtigung

Art. 20 Abs. 1

Personendaten, die von öffentlichen Organen bearbeitet werden, müssen richtig sein. Ist dies nicht der Fall, hat die betroffene Person Anspruch auf Berichtigung der Daten. An das Vorliegen eines schutzwürdigen Interesses sind in diesem Zusammenhang geringe Anforderungen zu stellen. Grundsätzlich stellt das Interesse an der Korrektheit der eigenen Daten für sich ein schutzwürdiges Interesse dar.

Berichtigungen müssen kostenlos und innert angemessener Frist vorgenommen werden. Gegenwärtig sind die Kosten für Berichtigungen in der Kantonalen Datenschutzverordnung geregelt. Demnach sind Berichtigungen nur dann kostenlos, wenn dadurch eine Widerrechtlichkeit behoben werden kann (§ 14 Abs. 3 lit. a der kantonalen Datenschutzverordnung). Diesbezüglich ist eine generelle Unentgeltlichkeit auf Gesetzesstufe vorzusehen. Im Rahmen der Totalrevision der kantonalen Datenschutzverordnung ist § 14 entsprechend zu überarbeiten.

Art. 23 Aufsichtsstelle, a) Kanton

Art. 23 Abs. 1^{bis} (neu) und Abs. 2 (geändert), Abs. 3^{bis} (neu)

Der oder die kantonale Datenschutzbeauftragte hat seine oder ihre Aufgaben als kantonales Kontrollorgan unabhängig wahrzunehmen. Die Unabhängigkeit ist auch in institutioneller Hinsicht zu garantieren. Im Sinne einer Unvereinbarkeitsbestimmung ist daher neu festzuhalten, dass der oder die Datenschutzbeauftragte kein anderes öffentliches Amt bekleiden und keine leitende Funktion in einer politischen Partei wahrnehmen darf. Nachdem verschiedene Vernehmlassungsteilnehmer darauf hingewiesen haben, dass die Unabhängigkeit auch durch die Mitgliedschaft in anderen Interessengruppen gefährdet sein könne, wurde im Gesetz eine entsprechende Ergänzung eingefügt.

Ausnahmen dürfen vom Regierungsrat nur bewilligt werden, wenn die Unabhängigkeit des oder der Datenschutzbeauftragten dadurch nicht gefährdet ist. Aufgrund entsprechender Einwände in der Vernehmlassung wird letzteres neu ausdrücklich im Gesetz festgehalten. Ebenfalls angeregt wurde ein gänzliches Absehen von der Möglichkeit Ausnahmen zu bewilligen. Eine solche Regelung würde

den Kandidatenkreis aber zu sehr einschränken. Auch das Bundesrecht kennt im Übrigen die Möglichkeit der Erteilung von Ausnahmebewilligungen für den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (Art. 26b DSG, Art. 41 E-DSG).

Die Unabhängigkeit des oder der Datenschutzbeauftragten ist nur dann garantiert, wenn der Abwahl enge Grenzen gesetzt sind. Bisher erklärte das Gesetz eine Abwahl bei Vorliegen von wichtigen sachlichen Gründen als zulässig. Diese Bestimmung ist dahingehend zu konkretisieren, als wichtige sachliche Gründe einzig in der vorsätzlichen oder grobfährlässigen schweren Verletzung von Amtspflichten oder der dauernden Amtsunfähigkeit erblickt werden dürfen. Ein Vernehmlassungsteilnehmer hat diese Bestimmung als zu eng kritisiert. Die Regelung entspricht aber der auch auf Bundesebene vorgesehenen (Art. 26a DSG, Art. 40 E-DSG).

Der neue Abs. 3bis ermöglicht es dem Regierungsrat, der kantonalen Aufsichtsstelle die Zusammenarbeit mit Aufsichtsstellen anderer Kantone oder die Anstellung von weiterem Fachpersonal zu genehmigen. Damit soll dem Umstand Rechnung getragen werden, dass bei der kantonalen Aufsichtsstelle aufgrund der fortschreitenden Digitalisierung und technologischen Entwicklungen in Zukunft ein erhöhter Bedarf an personellen Ressourcen entstehen kann. Um auf einen allfälligen Mehrbedarf rasch reagieren zu können und so einen effektiven Datenschutz sicherzustellen, liegt die Genehmigungskompetenz bei der Wahlbehörde der Aufsichtsstelle.

Art. 25 Aufgaben

Art. 25 Abs. 1 lit. h - i (neu)

Die Aufgaben der Aufsichtsstelle sind entsprechend Art. 12bis Ziff. 2 lit. e des Übereinkommens SEV 108 und Art. 46 Abs. 1 lit. b und d der Richtlinie (EU) 2016/680 zu erweitern. Die Aufsichtsstelle hat die verantwortlichen öffentlichen Organe und die Öffentlichkeit für Anliegen des Datenschutzes zu sensibilisieren. Sodann hat sie die massgeblichen Entwicklungen in der Informations- und Kommunikationstechnologie zu verfolgen, soweit sie sich auf den Schutz von Personendaten auswirken.

Art. 26b Beschwerde und Anzeigebefugnis

Art. 26b Abs. 1

Der Verweis in Art. 26b Abs. 1 auf Art. 30 des Gesetzes über den Rechtsschutz in Verwaltungssachen vom 20. September 1971 (Verwaltungsrechtspflegegesetz) [8)] ist unvollständig, da er nur die Beschwerde wegen Rechtsverweigerung oder Rechtsverzögerung umfasst. Die Aufsichtsstelle soll aber nicht nur Beschwerde erheben können, wenn eine Behörde in ungerechtfertigter Weise untätig bleibt, sondern generell, wenn Datenschutzvorschriften in grober Weise verletzt werden. Entsprechend ist in Art. 26b Abs. 1 auch auf Art. 31 des Verwaltungsrechtspflegegesetzes zu verweisen.

8) SHR 174.000.

Sehr geehrter Herr Präsident,
Sehr geehrte Damen und Herren

Aufgrund der vorstehenden Ausführungen beantragen wir Ihnen, auf die Vorlage einzutreten und dem im Anhang beigefügten Entwurf für eine Änderung des Kantonalen Datenschutzgesetzes zuzustimmen.

Schaffhausen, 21. Mai 2019

Im Namen des Regierungsrates
Der Präsident:
Ernst Landolt

Der Staatsschreiber:
Dr. Stefan Bilger

Anhang:
- Änderung des Kantonalen Datenschutzgesetzes

Anhang

Gesetz
über den Schutz von Personendaten
(Kantonales Datenschutzgesetz)

Änderung vom …

Der Kantonsrat Schaffhausen,

beschliesst als Gesetz:

I.

Das Datenschutzgesetz vom 7. März 1994 wird wie folgt geändert:

Art. 2 lit. d-h

d) besonders schützenswerte Personendaten:
   1. Daten über die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten,
   2. Daten über die Gesundheit, die Intimsphäre oder die ethnische Herkunft,
   3. Daten über Massnahmen der sozialen Hilfe,
   4. Daten über administrative oder strafrechtliche Verfolgungen und Sanktionen,
   5. genetische Daten,
   6. biometrische Daten;

e) Profiling: die automatisierte Auswertung von Daten, um wesentliche persönliche Merkmale zu analysieren oder persönliche Entwicklungen vorherzusagen;

f) Bearbeiten: jeder Umgang mit Daten, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten;

h) Aufgehoben

Art. 3 Abs. 2 und Abs. 4 (neu)

[2] Während hängigen Verfahren der Zivil-, Straf- und Verwaltungsrechtspflege richten sich die Rechte und Ansprüche der betroffenen Personen sowie die Einsichtsrechte Dritter nach dem anwendbaren Verfahrensrecht.

[4] Richterliche Behörden unterstehen nicht der Aufsichtsstelle gemäss Art. 23 ff.

Art. 4 Abs. 1

[1] Personendaten dürfen bearbeitet werden, wenn

a) dafür eine gesetzliche Grundlage besteht, oder

b) dies zur Erfüllung der gesetzlich umschriebenen Aufgaben geeignet und erforderlich ist oder

c) die betroffene Person ausdrücklich zustimmt oder ihre Zustimmung nach den Umständen unzweifelhaft vorausgesetzt werden darf.

Art. 5 Ingress

Besonders schützenswerte Personendaten dürfen nur bearbeitet werden oder ein Profiling darf nur vorgenommen werden, wenn:

Art. 5a

Informationspflicht beim Beschaffen von Personendaten

[1] Das öffentliche Organ ist verpflichtet, die betroffene Person über die Beschaffung von Personendaten zu informieren; diese Informationspflicht gilt auch dann, wenn die Daten bei Dritten beschafft werden.

[2] Der betroffenen Person sind mindestens mitzuteilen:

a) der Inhaber der Datensammlung das verantwortliche öffentliche Organ samt Kontaktdaten;

b) die Rechtsgrundlage und der Zweck des Bearbeitens;

c) die Kategorien der Datenempfänger, wenn eine Datenbekanntgabe vorgesehen ist;

d) die bearbeiteten Daten oder die Kategorien der bearbeiteten Daten;

e) die Rechte der betroffenen Person.

[3] Die Übermittlung der Informationen kann unter denselben Voraussetzungen eingeschränkt werden wie die Auskunft über die eigenen Daten (Art. 19).

[4] Die Informationspflicht entfällt, wenn:

a) das Bearbeiten der Daten ausdrücklich durch das Gesetz vorgesehen ist oder

b) die Information nicht oder nur mit unverhältnismässigem Aufwand möglich ist oder

c) die betroffene Person bereits über die Informationen nach Abs. 2 verfügt.

Art. 6

[1] Für den Datenschutz ist jenes öffentliche Organ verantwortlich, das - alleine oder zusammen mit anderen - über den Zweck und die Mittel der Bearbeitung von Daten entscheidet.

[2] Bearbeiten mehrere öffentliche Organe Personendaten aus einem gemeinsamen Informationsbestand, ist ein öffentliches Organ zu bezeichnen, das die Hauptverantwortung für den Datenschutz trägt.

Art. 7 Abs. 2

Aufgehoben

Art. 8 Abs. 3 (neu)

[3] Die Bekanntgabe von besonders schützenswerten Personendaten und Resultaten eines Profilings richtet sich nach Art. 5.

Art. 11a

Für die Bekanntgabe von Personendaten an ausländische Stellen der Europäischen Union sowie Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum und des Übereinkommens des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung von personenbezogenen Daten (SEV Nr. 108) gelten neben dem übergeordneten Recht und dem Staatsvertragsrecht die Bestimmungengemäss Art. 8 ff. sinngemäss.

Art. 11b Abs. 1 und 2

[1] An Drittstaaten dürfen Personendaten unter Vorbehalt von Art. 8 ff. nur bekannt gegeben werden, sofern diese ein angemessenes Datenschutzniveau gemäss Übereinkommen des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung von personenbezogenen Daten (SEV Nr. 108) gewährleisten.

[2] Die Angemessenheit des Datenschutzniveaus wird in Anlehnung an die Vorgaben des Bundes und unter Berücksichtigung aller Umstände beurteilt, die für die Datenübermittlung von Bedeutung sind.

Art. 13

[1] Das verantwortliche öffentliche Organ kann ein anderes öffentliches Organ oder Dritte mit dem Bearbeiten von Personendaten beauftragen, wenn

a) der Übertragung keine rechtliche Bestimmung oder vertragliche Vereinbarung entgegensteht und

b) sichergestellt wird, dass die Daten nur so bearbeitet werden, wie es das verantwortliche öffentliche Organ tun dürfte.

[2] Der Datenschutz ist durch Vereinbarung, Auflagen oder auf andere Weise sicherzustellen. Der Regierungsrat regelt das Nähere durch Verordnung.

(neu)
[3] Die beauftragte Stelle darf ohne vorgängige schriftliche Zustimmung des auftraggebenden öffentlichen Organs die Datenbearbeitung keiner weiteren Stelle übertragen.

(neu)
[4] Das auftraggebende öffentliche Organ bleibt für den Umgang mit den Daten nach diesem Gesetz verantwortlich.

Art. 14 Marginalie und Abs. 2

[2] Das öffentliche Organ muss nachweisen können, dass es die Datenschutzbestimmungen einhält. Der Regierungsrat regelt das Nähere durch Verordnung.

Informationssicherheit

Art. 14a (neu)

[1] Das öffentliche Organ meldet der Aufsichtsstelle ohne unangemessene Verzögerung eine Datenschutzverletzung, die zu einem hohen Risiko für die Grundrechte der betroffenen Person führt.

Meldung von Datenschutzverletzungen

[2] Werden Daten von einer dritten Stelle im Auftrag bearbeitet, hat diese das öffentliche Organ unverzüglich über Datenschutzverletzungen zu informieren.

[3] Das öffentliche Organ informiert ausserdem die betroffene Person, wenn es zu deren Schutz erforderlich ist oder die Aufsichtsstelle dies verlangt.

[4] Die Information der betroffenen Person kann unter Benachrichtigung der Aufsichtsstelle eingeschränkt oder aufgehoben werden, wenn überwiegende öffentliche oder private Geheimhaltungsinteressen dies erfordern.

[5] Eine Datenschutzverletzung liegt vor, wenn bearbeitete Personendaten unbeabsichtigt vernichtet werden oder verloren gehen, unbeabsichtigt oder unrechtmässig verändert oder bekannt gegeben werden oder wenn Unbefugte Zugang zu solchen Daten erhalten.

Art. 14b (neu)

[1] Beabsichtigt das öffentliche Organ eine Bearbeitung von Personendaten, die voraussichtlich ein erhöhtes Risiko für die Grundrechte der betroffenen Person mit sich bringt, führt es eine Datenschutz-Folgenabschätzung durch.

Datenschutz-Folgenabschätzung

[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 vermeiden.

Art. 14c (neu)

Vorabkonsultation

[1] Ergibt sich aus der Datenschutz-Folgenabschätzung, dass die geplante Bearbeitung ein hohes Risiko für die Grundrechte der betroffenen Person zur Folge hat, so holt das öffentliche Organ vorgängig die Stellungnahme der Aufsichtsstelle ein.

[2] Die Aufsichtsstelle teilt dem öffentlichen Organ innert angemessener Frist allfällige Einwände gegen die geplante Bearbeitung mit. Sie kann Massnahmen nach Art. 26 ergreifen.

III. Datensammlung

Titel aufgehoben

Art. 15

Aufgehoben

Art. 16

Aufgehoben

Art. 16a

Aufgehoben

Art. 17 Abs. 1

[1] Nicht mehr benötigte Personendaten sind zu vernichten. Vorbehalten bleiben die Vorschriften über die Archivierung.

Art. 17a (neu)

Information der Empfänger von Personendaten

[1] Das öffentliche Organ informiert die Empfängerinnen und Empfänger von Personendaten über jede Berichtigung, Löschung oder Vernichtung von Personendaten sowie über Vermerke gemäss Art. 20 Abs. 3, sofern anzunehmen ist, dass sie Daten durch die Empfängerinnen und Empfänger noch bearbeitet werden.

[2] Von der Mitteilung kann abgesehen werden, soweit sie nur mit unverhältnismässigem Aufwand möglich ist.

Art. 17b (neu)

Strafverfolgung und Justizvollzug
a) Register

[1] Die Polizei, die Staatsanwaltschaft und die Justizvollzugsbehörde führen öffentliche Register über die Datenbearbeitungstätigkeiten in ihren Zuständigkeitsbereichen.

[2] Die Register enthalten Angaben über die Rechtsgrundlage, den Zweck und die Mittel der Bearbeitung sowie die Art, Herkunft und regelmässigen Empfänger der Personendaten.

Art. 17c (neu)

b) Datenschutzberatung

[1] Die Polizei, die Staatsanwaltschaft und die Justizvollzugsbehörde benennen innerhalb ihrer Organisation eine für den Datenschutz zuständige Person.

[2] Diese hat folgende Aufgaben:

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

b) sie nimmt Datenschutz-Folgenabschätzungen gemäss Art. 14b vor;

c) sie ist Ansprechperson der Aufsichtsstelle gemäss Art. 23 ff..

Art. 18

[1] Aufgehoben

[2] Jede Person erhält auf Verlangen in allgemein verständlicher Form Auskunft darüber, ob und wenn ja welche Daten über sie von einem öffentlichen Organ bearbeitet werden. Die Auskunft erfolgt in der Regel schriftlich in Form eines Ausdrucks oder einer Fotokopie. Sie enthält mindestens die Angaben nach Art. 5a Abs. 2 sowie Angaben über die Aufbewahrungsdauer und Herkunft der Daten.

[2bis] Von der Auskunftspflicht ausgenommen sind Daten, die ausschliesslich als persönliche Arbeitsmittel dienen, namentlich persönliche Notizen.

[3] Die Auskunft erfolgt in der Regel kostenlos. Eine angemessene Gebühr kann verlangt werden, wenn:

a) zum Schutz berechtigter Interessen Dritter administrativ aufwendige Massnahmen zu treffen sind;

b) der Antrag rechtsmissbräuchlich ist, namentlich bei exzessiven Anträgen in derselben Angelegenheit oder bei offensichtlicher Unbegründetheit.

Art. 19 Abs. 2

Aufgehoben

Art. 20 Abs. 1

[1] Wer ein schutzwürdiges Interesse darlegt, kann vom öffentlichen Organ verlangen, dass unrichtige Personendaten kostenlos und innert angemessener Frist berichtigt werden.

Art. 23 Abs. 1bis (neu), Abs. 2 und Abs. 3bis (neu)

[1bis] Der oder die kantonale Datenschutzbeauftragte darf kein anderes öffentliches Amt und keine leitende Funktion in einer politischen Partei ausüben oder Mitglied in einer anderen Interessengruppe sein, die Zielkonflikte befürchten lässt. Der Regierungsrat kann Ausnahmen bewilligen, sofern die Unabhängigkeit dadurch nicht gefährdet ist.

[2] Eine Abwahl ist nur zulässig bei:

a) vorsätzlicher oder grobfährlässiger Verletzung der Amtspflichten in schwerer Weise; oder

b) dauerndem Verlust der Amtsfähigkeit.

[3bis] Die Wahlbehörde kann bei Bedarf Kooperationen mit Aufsichtsstellen anderer Kantone oder die Anstellung von Fachpersonal genehmigen.

Art. 25 Abs. 1 lit. h - i (neu)

[1] Die Aufsichtsstelle

h) sensibilisiert die öffentlichen Organe für ihre datenschutzrechtlichen Pflichten und die Öffentlichkeit für die Anliegen des Datenschutzes;

i) verfolgt die für den Schutz von Personendaten massgeblichen Entwicklungen.

Art. 26b Abs. 1

[1] Stellt die Aufsichtsstelle grobe Verletzungen von Datenschutzvorschriften durch ein öffentliches Organ fest, so erhebt sie Aufsichtsbeschwerde gemäss Art. 30 f. des Verwaltungsrechtspflegegesetzes.

II.

[1] Dieses Gesetz untersteht dem Referendum.

[2] Der Regierungsrat bestimmt das Inkrafttreten.

[3] Dieses Gesetz ist im Amtsblatt zu veröffentlichen und in die kantonale Gesetzessammlung aufzunehmen.

Schaffhausen, …

Im Namen des Kantonsrates

Der Präsident:

Die Sekretärin: