Sicherheitsdepartement

Bahnhofstrasse 9
Postfach 1200
6431 Schwyz
Telefon 041 819 20 15
Telefax 041 819 20 19

kantonschwyz

Teilrevision des Gesetzes über die Öffentlichkeit und den Datenschutz
Vernehmlassungsentwurf

1. Ausgangslage

1.1 „Jede Person hat Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten“ (Art. 13 Abs. 2 der Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999, BV, SR 101). Dieser Anspruch auf Datenschutz ist ein eigenständiger Teilgehalt des verfassungsrechtlichen Rechts auf Schutz der Privatsphäre und Persönlichkeit, eines der zentralsten Grundrechte. Das auch als Recht auf informationelle Selbstbestimmung bezeichnete Grundrecht räumt dem eigenverantwortlichen Individuum das vorrangige Recht ein, selber über die Zulässigkeit der Bearbeitung seiner Daten zu entscheiden. Es schützt das Individuum nicht nur gegen den Missbrauch seiner Daten, sondern setzt die in einem demokratischen Rechtsstaat erforderlichen Leitplanken für die Bearbeitung personenbezogener Daten durch den Staat und Private.
Der Datenschutz hat auch eine Querschnittsfunktion, weil er in allen Aufgaben- und Rechtsbereichen zum Tragen kommt, wo schützenswerte Personendaten bearbeitet werden. Er ist mitunter auch eine Prämisse, damit andere Grundrechte und -freiheiten wahrgenommen werden können. Wie andere Grundrechte kann jedoch auch der Datenschutz unter den Voraussetzungen von Art. 36 BV eingeschränkt, nicht aber in seinem Kerngehalt ausgehöhlt werden.

1.2 Es gibt keine besonderen Bestimmungen in der Bundesverfassung, die dem Bund bzw. den Kantonen eine explizite Gesetzgebungskompetenz im Bereich des Datenschutzes einräumen. Der Bund ist aber auf dem Gebiet des Zivilrechts (Art. 122 BV) und der Ausübung privatwirtschaftlicher Erwerbstätigkeiten (Art. 95 BV) zum Erlass von privatrechtlichen wie auch wirtschaftspolizeilichen Datenschutzvorschriften ermächtigt. Die Kompetenz zum Erlass von Datenschutzregelungen für Behörden und Verwaltungsstellen schöpft der Bund aus seiner Organisationsgewalt (vgl. Art. 164 Abs. 1 Bst. g BV). Aufgrund ihrer verfassungsmässig garantierten Organisationsautonomie verfügen die Kantone ihrerseits über eine parallele Kompetenz zum Erlass von Datenschutzrecht in ihrem öffentlich-rechtlichen Bereich.
Auf diesen Grundlagen basieren einerseits das Bundesgesetz über den Datenschutz vom 19. Juni 1992 (DSG, SR 235.1) und andererseits das kantonale Gesetz über die Öffentlichkeit der Verwaltung und den Datenschutz vom 23. Mai 2007 (ÖDSG, SRSZ 140.410), das zusätzlich auch noch das Öffentlichkeitsprinzip gesetzgeberisch verankert hat (vgl. § 45 der Verfassung des Kantons Schwyz vom 24. November 2010, KV, SRSZ 100.100).

1.3 Die Digitalisierung der Gesellschaft und die Weiterentwicklung des europäischen Datenschutzrechts haben direkte oder indirekte Auswirkungen auf die eidgenössische und kantonale Datenschutzgesetzgebung. Der Bund hat inzwischen eine Totalrevision seiner Datenschutzgesetzgebung vorbereitet (BBl 2017 6941 ff.). Der Regierungsrat hat seinerseits

eine Teilrevision des allgemeinen wie auch des polizeilichen Datenschutzrechts in Auftrag gegeben (RRB Nr. 167/2015). Das Vorhaben ist im Gesetzgebungsprogramm enthalten (RRB Nr. 46/2017; RRB Nr. 33/2017).

2. Revisionsbedarf

2.1 Digitalisierung der Gesellschaft

Der virtuelle Raum ist Wirklichkeit geworden. Es gibt kaum noch Lebensbereiche in unserer Zivilgesellschaft, in welche die Digitalisierung noch nicht vorgedrungen ist. Die Entwicklung ist rasend und global. Sie führt dazu, dass in immer kürzerer Zeit riesige Datenseen (Big Data) entstehen, deren Nutzung und Vernetzung nicht nur ein unerschöpfliches Potential, sondern auch grosse Gefahren birgt. Wie verletzbar die Staaten und die Individuen dadurch geworden sind, belegen Internetkriminalität, Hackerangriffe auf private, wirtschaftliche und staatliche Datenverarbeitungssysteme, Verbreitung von Falschmeldungen und Manipulation der demokratischen Auseinandersetzung, terroristische Bedrohungen von Einrichtungen der Grundversorgung sowie Cyberattacken.
Vielen Nutzern fehlt die Sensibilität, oft aber auch das spezifische technische Verständnis für einen sicheren und verantwortungsvollen Umgang mit den eigenen oder fremden Personendaten in einer zunehmend komplexeren und dimensionsloseren digitalen Welt. Staat und Politik müssen Strategien und Antworten für diese Herausforderungen finden. Auch die Rechtsordnungen hinken hinter diesen Entwicklungen her. Dabei ist der Datenschutz eines der zentralsten Themen. Es müssen rechtliche Rahmenbedingungen geschaffen werden, welche in einem digitalisierten Raum die Grundrechte der Informationsfreiheit, der Selbstbestimmung und des Persönlichkeitsschutzes der Bürgerinnen und Bürger wahren, die Datensicherheit gewährleisten und das Funktionieren des Rechtsstaates weiterhin garantieren. Behördliche Zusammenarbeit bedeutet Datenaustausch, Datenaustausch bedingt Datenschutz.

2.2 Europäische Entwicklungen

2.2.1 Datenschutz-Grundverordnung (DSGVO)

Vor diesem Hintergrund hat die EU eine neue Datenschutz-Grundverordnung (EU-Verordnung 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr) erlassen, welche die bisherige EU-Datenschutz-Richtlinie 95/46/EG ablöst und das Datenschutzrecht in allen EU-Mitgliedstaaten harmonisiert. Sie trat am 25. Mai 2018 in Kraft und ist in der gesamten EU unmittelbar anwendbar. Ursprünglich zum Schutz gegen den Überwachungsstaat angelegt, soll das neue europäische Datenschutzrecht die Bürgerinnen und Bürger vor allem auch gegen die digitale Datengier grosser Internetkonzerne schützen, die von Ländern mit einem tieferen Datenschutzniveau aus operieren.
Inhaltlich sieht die DSGVO eine Stärkung der Rechte der von einer Datenbearbeitung betroffenen Person vor: Recht auf Information, Auskunftsrecht, Recht auf Berichtigung, Recht auf Löschung (Recht auf Vergessen), Recht auf Einschränkung der Bearbeitung, Recht auf Mitteilung, Widerspruchsrecht, Recht auf Benachrichtigung über Datenschutzverletzungen.
Die Verordnung sieht auch einen einfacheren und wirksameren Rechtsschutz, griffigere Interventionsinstrumente der Datenschutzbehörden und ein härteres Sanktionensystem bei Datenschutzverletzungen vor.

Die DSGVO ist für die Schweiz nicht verbindlich. Gleichwohl hat sie für die Schweiz eine hohe Relevanz, weil sie auch für Datenverarbeitungen gilt, die zwar von ausserhalb der EU erfolgen, aber Waren und Dienstleistungen an Kunden in der EU betreffen (sog. extraterritoriale Anwendung). Sodann dürfen EU-Mitgliedstaaten einem Nicht-EU-Staat nur dann personenbezogene Daten übermitteln, wenn die EU-Kommission festgestellt hat, dass dieses Drittland über ein angemessenes Datenschutzniveau verfügt. Aus diesem Grund haben die Schweiz und namentlich auch die Schweizer Wirtschaft ein grosses Interesse an der Harmonisierung des schweizerischen Datenschutzrechts mit demjenigen der EU. Dies ist mithin eine Zielsetzung der Totalrevision der Bundesdatenschutzgesetzgebung in deren privatwirtschaftlichem Anwendungsbereich. Für die kantonalen Datenschutzgesetze besteht insoweit aber kein direkter Handlungsbedarf.

2.2.2 Schengener Datenschutzvorschriften

Für die Schweiz von besonderer Bedeutung sind die Datenschutzvorschriften im Rahmen der polizeilichen und justiziellen Zusammenarbeit der Schengen-Staaten und des Schengener Informationssystems (SIS).
Mit dem Schengen-Beitritt und der Aufnahme der operationellen Schengen-Zusammenarbeit im Jahr 2008 hat sich die Schweiz auch zur Übernahme und Anwendung des sogenannten Schengen-Besitzstandes und dessen Weiterentwicklungen verpflichtet. So waren Bund und Kantone gehalten, den seinerzeitigen Rahmenbeschluss Datenschutz 2008/977/JI des EU-Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, im innerstaatlichen Recht umzusetzen. Im Kanton Schwyz erfolgte dies mit dem Erlass des Öffentlichkeits- und Datenschutzgesetzes vom 23. Mai 2007 (GS 21-153) sowie der Teilrevision des Polizeigesetzes vom 17. März 2010 (GS 22-97). Dabei wurde auf eine Differenzierung zwischen inner- und schengenstaatlichem Informationsaustausch und einem unterschiedlichen Datenschutzniveau verzichtet. Es wäre denn auch nicht zu rechtfertigen gewesen, wenn bei einer innerstaatlichen Datenbearbeitung der betroffenen Person weniger Rechte und dem Datenschutzbeauftragten weniger Befugnisse eingeräumt worden wären als bei schengenrelevanten Datenbearbeitungsvorgängen.

Die behördliche Zusammenarbeit im Rahmen von Schengen und Dublin steht auf einem harten Prüfstein. Sie kann aber nur verbessert werden, wenn die Regeln über den Informationsaustausch einerseits vereinfacht und harmonisiert werden und andererseits die Rechtsstaatlichkeit, insbesondere auch der Schutz der Bürgerinnen und Bürger vor unzulässigen Datenbearbeitungen, verstärkt wird. Ein unterschiedliches Datenschutzniveau in den einzelnen Schengen-Staaten setzt der behördlichen Zusammenarbeit Grenzen, während Verbrecher und Terroristen ungehindert grenzüberschreitend agieren können. Es darf nicht sein, dass der Austausch und die Verwertbarkeit von wichtigen Ermittlungserkenntnissen und Beweisen aufgrund von divergierenden Standards bei der Datenbearbeitung verzögert oder verunmöglicht werden. Wenn durch übergeordnete Datenschutzvorgaben sichergestellt wird, dass das Datenschutzniveau in den Schengen-Staaten gleichwertig ist, erweist sich der Informationsaustausch als verantwortbar und macht eine ohnehin schwierige Überprüfung des Datenschutzniveaus im Empfängerstaat entbehrlich. Vor diesem Hintergrund wurde die neue Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr erlassen (nachfolgend DSRL). Sie ersetzt den Rahmenbeschluss Datenschutz 2008/977/JI.

Die neue DSRL stellt eine Schengen-Weiterentwicklung dar. Sie entstand aber ebenfalls unter der Ausrichtung der EU-Datenschutz-Grundverordnung der EU. Die Schweiz hat nach der Notifikation der DSRL am 1. August 2016 an sich zwei Jahre Zeit, diesen Rechtsakt in ihrer Rechtsordnung umzusetzen. Dies gilt auch für die Kantone, da die DSRL den öffentlich-rechtlichen Anwendungsbereich der Datenschutzgesetze betrifft. Diese Zeitvorgabe erweist sich als zu knapp, da sich die Kantone im Interesse einer harmonisierten Auslegung und Umsetzung an der bundesrechtlichen Vorlage zu orientieren haben. Da Rechtsharmonisierungen, die mit einer strengeren und detaillierteren Regulierung verbunden sind, in ihrer Umsetzung und Anwendung häufig nicht zu einer Vereinfachung führen, hat sich der Kanton Schwyz in der Vernehmlassung zur neuen Bundesdatenschutzgesetzgebung für eine der föderalen Ordnung entsprechende, zielführende, auf das Notwendige reduzierte, pragmatische und vollzugstaugliche Umsetzungslösung ausgesprochen, was auch mit der vorliegenden Revision anzustreben ist.
Die Übernahme der DSRL bedingt umfassendere Anpassungen des kantonalen Öffentlichkeits- und Datenschutzgesetzes sowie punktuelle Präzisierungen des Polizeigesetzes vom 22. März 2000 (PolG, SRSZ 520.110). Inhaltlich bedeutet der neue Rechtsakt die Verpflichtung zur Kategorisierung der Personendaten, zur Differenzierung der Bearbeitungsregeln, zur Präzisierung der Datenschutzgrundsätze, zur Verbesserung der Informations- und Kontrollrechte der betroffenen Personen sowie zur stärkeren Verantwortung der Bearbeitungsorgane (Sorgfaltspflichten, Protokollierungspflicht, Datensicherheit, Risikofolgeabschätzungen, Meldepflichten). Bedeutsam ist sodann das neue Beschwerderecht der von einer Datenbearbeitung betroffenen Person, die Erweiterung der Befugnisse des Datenschutzbeauftragten (Beschwerdeinstanz, Verfügungs- und Weisungskompetenzen, zusätzliche Prüf- und Bearbeitungsaufgaben).

2.2.3 Übereinkommen des Europarates

Das Übereinkommen des Europarates vom 28. Januar 1981 im Bereich Datenschutz (SEV Nr. 108, inkl. Zusatzprotokoll), dem die Schweiz seinerzeit beigetreten ist, wurde ebenfalls einer Modernisierung unterzogen, um den Schutz der Privatsphäre und der Grundrechte im Zusammenhang mit der Globalisierung, der Digitalisierung und der Zunahme des grenzüberschreitenden Datenverkehrs besser zu gewährleisten. Das revidierte Übereinkommen (nachfolgend E-SEV 108) gilt für Datenbearbeitungen im öffentlichen wie auch privaten Sektor und ist daher sowohl für die Datenschutzgesetzgebung des Bundes wie auch der Kantone relevant. Es ist aber nicht direkt anwendbar und muss folglich ebenfalls im innerstaatlichen Recht umgesetzt werden. Der Bund hat dies in der Vorlage für die Totalrevision des Bundesdatenschutzgesetzes vorgesehen. Auf kantonaler Ebene erfolgt die Berücksichtigung mit dem vorliegenden Rechtsetzungsvorhaben.
Inhaltlich geht das E-SEV 108 nicht über die EU-Datenschutz-Grundverordnung und die Schengener DSRL hinaus und enthält teilweise analoge Bestimmungen. So werden ebenfalls die Pflichten der datenbearbeitenden bzw. verantwortlichen Organe ausgeweitet (Informationspflicht, Risikoabschätzung), die Rechte der betroffenen Personen gestärkt (Anhörungs-, Auskunfts- und Einwilligungsrecht) und das Rechtsmittel- und Sanktionssystem ausgebaut.

2.4 Revision der Bundesdatenschutzgesetzgebung

Mit der Totalrevision des Bundesdatenschutzgesetzes und der Anpassung bereichsspezifischer Datenschutzvorschriften sind im Kontext der Digitalisierung und der grenzüberschreitenden Entwicklungen folgende Zielsetzungen verbunden:

- Wiedererlangung der Selbstkontrolle über die eigenen Personendaten;
- Förderung der Eigenverantwortung der für die Datenbearbeitungen Verantwortlichen;
- Erhalt und Stärkung der schweizerischen Wettbewerbsfähigkeit;
- Umsetzung der Schengener DSRL im innerstaatlichen Recht;
- Annäherung der schweizerischen Datenschutzgesetzgebung an die DSGVO zwecks Anerkennung eines angemessenen Datenschutzniveaus;
- Anpassung des innerstaatlichen Rechts an das E-SEV 108 zwecks Anerkennung eines angemessenen Datenschutzniveaus.

Dabei orientiert sich die DSG-Totalrevision im Wesentlichen an folgenden Leitlinien: Grösstmögliche Minimierung der Gefahren für die Privatsphäre der von der Datenbearbeitung betroffenen Person, technologieneutrale Ausgestaltung der Datenbearbeitungsregeln, Modernisierung und Harmonisierung der Terminologie, Verbesserung des grenzüberschreitenden Datenverkehrs unter der Prämisse eines angemessenen Datenschutzniveaus, Stärkung der Rechte der betroffenen Person und Präzisierung der Pflichten der Datenverantwortlichen, Stärkung der Kontrolle durch den Ausbau der Befugnisse des Datenschutzbeauftragten und ein griffigeres Sanktionensystem. Auf die einzelnen Inhalte der DSG-Totalrevision wird nachfolgend noch einzugehen sein, zumal diese eine gewissen präjudizierenden Charakter für die Auslegung der umzusetzenden Rechtsakte auf die kantonale Datenschutzgesetzgebung hat.

2.5 Nur punktueller Nachführungsbedarf

Dem Datenschutz wird bei der Bearbeitung von Personendaten durch die kantonalen und kommunalen Organe im Kanton Schwyz hohe Beachtung und Sorgfalt beigemessen. Das kantonale Öffentlichkeits- und Datenschutzgesetz hat sich in den rund zehn Jahren seines Bestehens grundsätzlich bewährt. Es erfolgten bislang nur punktuelle Anpassungen im Zusammenhang mit Änderungen anderer Erlasse, so bezüglich der Bekanntgabe von Daten aus dem Einwohnerregister (§ 12 ÖDSG, GS 22-54), der Zuweisung der Wahl des Datenschutzbeauftragten und Oberaufsicht in die Kompetenz des Kantonsrates (§ 28 ÖDSG, GS 24-48) und der Archivierungs- bzw. Löschungspflicht nach dem neuen Archivgesetz (§ 22 ÖDSG, GS 24-57).
Der Bereich des Öffentlichkeitsprinzips als eigenständige Institution des kantonalen Rechts wird von den vorliegend umsetzenden übergeordneten Vorgaben im Bereich des Datenschutzes grundsätzlich nicht tangiert.

3. Regelungsgegenstand

Somit sind die Vorgaben der Schengener DSRL und die Grundsätze des E-SEV 108 unter Berücksichtigung der parallelen Umsetzungsnormierung in der Bundesdatenschutzgesetzgebung in das ÖDSG zu übernehmen. Die spezifisch für die polizeiliche Datenbearbeitung verbindlichen Standards aus dem Schengener Datenschutzrecht werden im Rahmen einer separaten Revision des Polizeigesetzes umgesetzt.
Für die Gesetzgebungsarbeiten der Kantone hat die Konferenz der Kantonsregierungen (KdK) einen Leitfaden vom 2. Februar 2017 ausarbeiten lassen, welcher eine rechtsvergleichende Auslegeordnung zwischen den umzusetzenden Rechtsakten vornimmt und den möglichen Anpassungsbedarf in den kantonalen Datenschutzgesetzgebungen aufzeigt. Die Erhebung des Revisionsgegenstands erfolgte unter Zuhilfenahme dieses Leitfadens.

3.1 Geltungsbereich

Anders als der Rahmenbeschluss Datenschutz 2008/977/JI gilt die neue Schengener DSRL nun auch für innerstaatliche Datenbearbeitungen von Polizei- und Justizbehörden, was aber bereits der geltenden Umsetzungskonzeption im kantonalen Datenschutzrecht entspricht. Sodann muss sichergestellt sein, dass das ÖDSG grundsätzlich für alle Datenbearbeitungen durch kantonale und kommunale Organe zur Anwendung kommt (Art. 2 DSRL, Art. 3 E-SEV 108) und generelle Ausnahmen vom Geltungsbereich an sich nicht mehr zulässig sind, sondern Abgrenzungen bei den Legaldefinitionen bzw. beim Informationszugang vorzunehmen sind. Bei der Überprüfung von § 3 ÖDSG ist weiter Folgendes zu beachten:

- Öffentliche Organe, die privatrechtlich handeln, dürfen insofern der Bundesdatenschutzgesetzgebung unterstellt werden, verbleiben aber in der kantonalen Aufsicht (vgl. Art. 36 E-DSG für Bundesorgane, die privatrechtlich handeln).
- Hängige Verfahren der Zivil-, Straf- und Verwaltungsrechtspflege dürfen nicht mehr generell vom Geltungsbereich des Datenschutzgesetzes ausgenommen werden (Art. 2 DSRL). Im Sinne einer Kollisionsnorm ist aber klarzustellen, dass sich die Rechte und Ansprüche der betroffenen Person während eines hängigen Verfahrens der Zivil-, Straf- und Verwaltungsrechtspflege ausschliesslich nach dem anwendbaren Verfahrensrecht richten und nicht nach den Informationsansprüchen nach dem ÖDSG. Eine entsprechende lex-specialis-Norm sieht auch Art. 2 Abs. 3 E-DSG für die Bearbeitung von Personendaten in Gerichtsverfahren und in Verfahren nach bundesrechtlichen Verfahrensordnungen vor, wobei dort für erstinstanzliche Verwaltungsverfahren die Bestimmungen des E-DSG für massgebend erklärt werden.

3.2 Präzisierung von Legaldefinitionen

Die Begriffsbestimmungen nach § 4 ÖDSG sind nach Massgabe der umzusetzenden Rechtsakte nach den verschiedenen Personen-, Daten- und Bearbeitungskategorien zu differenzieren. Allerdings kommen bestimmte in Art. 3 DSRL bzw. Art. 2 E-SEV 108 definierte Begriffe im allgemeinen oder im spezialgesetzlichen Datenschutzrecht des Kantons bislang nicht vor (z.B. Profiling, Auftragsdatenbearbeiter, Verbot von automatisierten Einzelentscheidungen) und sollen nicht unbesehen übernommen werden. Sie lassen sich teilweise unter bestehende Oberbegriffe subsumieren oder mit gleichbedeutenden Ausdrücken unserer Gesetzessprache ersetzen. Zusätzlicher Präzisierungsbedarf im kantonalen Recht besteht dann, wenn an diese definierten Begriffe der umzusetzenden Rechtsakte spezifische Rechtsfolgen geknüpft werden (z.B. qualifizierte Anforderungen an das Bearbeiten von besonders schützenswerten Personendaten und das Profiling nach Art. 10 DSRL bzw. Art. 6 E-SEV 108).
Anders als die DSRL und das E-SEV 108 schützen die Datenschutzgesetzgebungen von Bund und Kantonen bislang sowohl die natürlichen wie auch die juristischen Personen. Vor dem Hintergrund der praktischen Erfahrungen und Komplikationen der datenschutzrechtlichen Gleichbehandlung juristischer und natürlicher Personen sollen die juristischen Personen künftig vom allgemeinen Bundesdatenschutzgesetz ausgenommen werden (vgl. Art. 4 Bst. a und b E-DSG). Dahinter steht die Überlegung, dass die Datennutzung bei den natürlichen Personen sämtliche Lebensbereiche beschlägt, während sie bei den juristischen Personen auf ihren vorab wirtschaftlichen Zweck ausgerichtet ist. Hierbei würden den juristischen Personen andere Schutzmechanismen (u.a. Persönlichkeitsschutz, Immaterialgüterrechte) zur Verfügung stehen. Zudem würden hinter jeder juristischen Person natürliche Personen stehen, welche an ihrer Stelle Datenschutzrechte ausüben könnten. Allerdings sollen im Regierungs- und Verwaltungsorganisationsgesetz des Bundes (Art. 57r und 57s E-RVOG) allgemeine Rechtsgrundlagen für die Bearbeitung und

die Bekanntgabe von Daten juristischer Personen durch Bundesorgane geschaffen werden. Innerhalb einer Übergangsfrist von fünf Jahren sollen sodann alle bundesrechtlichen Spezialerlasse geprüft und angepasst werden, um allfällige Widersprüche und Lücken zu eliminieren.
Die Kantone sind nicht verpflichtet, ihre Datenschutzgesetzgebung hinsichtlich des Umgangs mit Daten juristischer Personen anzupassen. Die Anlehnung an die bundesrechtliche Umsetzung hätte nämliche zur Folge, dass alle kantonalen Erlasse ebenfalls dahingehend überprüft werden müssten, ob sie auch für die Bearbeitung und den Schutz von Daten juristischer Personen Geltung beanspruchen. Zudem würde die Konzeption einer möglichst einheitlichen Anwendung des Datenschutzes und des Öffentlichkeitsprinzips durchbrochen.

3.3 Grundsätze der Datenbearbeitung

Die Grundsätze der Bearbeitung von Personendaten nach §§ 8 ff. ÖDSG entsprechen im Wesentlichen den umzusetzenden Rechtsakten. Es betrifft dies die Rechtmässigkeit, den Grundsatz von Treu und Glauben (Transparenz), die Zweckbindung, das Verhältnismässigkeitsprinzip (Datensparsamkeit), die Richtigkeit der Personendatenbearbeitungen sowie die Daten- bzw. Informationssicherheit.
Bei der Konkretisierung dieser allgemeinen Datenschutzgrundsätze besteht vorab bei den Verantwortlichkeiten der datenbearbeitenden Organe ein ergänzender Regelungsbedarf. Es betrifft dies insbesondere auch die Konstellation, bei der mehrere öffentliche Organe gemeinsam Personendaten bearbeiten oder wenn bei der Auslagerung oder Übertragung staatlicher Tätigkeiten Dritte mit der Datenbearbeitung beauftragt werden. Für letzteren Fall gelten klare Voraussetzungen und es muss der Nachweis erbracht werden können, dass die beauftragten Dritten die anwendbaren Datenschutzvorschriften einhalten können (Art. 4 Abs. 4 und 22 f. DSRL).

3.4 Rechte der betroffenen Person

3.4.1 Die Transparenz ist Bestandteil der Rechtsstaatlichkeit (§ 3 KV) und ein elementarer Grundsatz des Datenschutzes. Die betroffene Person muss nachvollziehen können, wer was wann und wozu über sie weiss. Dies bedingt, dass das datenbearbeitende öffentliche Organ die betroffene Person über die Datenbearbeitung informiert und diese ihrerseits Auskunft über die Bearbeitung ihrer Personendaten verlangen kann:

- Die umzusetzenden Rechtsakte verpflichten die öffentlichen Organe zu einer aktiven Information über das Bearbeiten von Personendaten aller Kategorien, d.h. nicht nur in Bezug auf die besonders schützenswerten Personendaten, wie dies in § 11 ÖDSG bislang vorgesehen ist. Die Informationspflicht wie auch der Mindestinhalt der Information (verantwortliches öffentliches Organ, bearbeitete Datenkategorie, Rechtsgrundlage, Bearbeitungszweck, Datenempfänger, Rechte der betroffenen Person) müssen im Gesetz verankert sein. Einschränkungen der Informationspflichten haben den in den umzusetzenden Rechtsakten genannten Voraussetzungen zu entsprechen (Art. 13 DSRL, Art. 7^{bis} E-SEV 108).
- Auch beim Auskunftsrecht und dessen Einschränkung nach §§ 24 f. ÖDSG bedarf es analog zur Informationspflicht gewisser Präzisierungen bezüglich des Mindestumfangs der Auskunft (Art. 12 und 14 DSRL), zusätzlich auch Angaben über die Aufbewahrungsdauer und Herkunft der Personendaten.

3.4.2 Personendaten müssen richtig und entsprechend dem Verwendungszweck auch vollständig sein. Dies ist eine grundlegende Entscheidvoraussetzung für das zuständige öffentliche Organ. Dieses muss sich selber vergewissern, dass die zu bearbeitenden Personendaten richtig und vollständig sind. Verletzt es seine Sorgfaltspflicht, riskiert es nicht nur, dass seine Anord-

nungen hinfällig werden, sondern sieht sich unter Umständen auch mit Haftungsfragen konfrontiert.
Zufolge ihres Informations- und Auskunftsrechts kann die betroffene Person ihrerseits überprüfen, ob die über sie bearbeiteten Daten richtig und vollständig sind und gegebenenfalls intervenieren. Der Anspruch auf Berichtigung unrichtiger oder unvollständiger Personendaten sowie auf Unterlassung unbefugter Datenbearbeitungen umfasst auch den Anspruch auf Feststellung der Widerrechtlichkeit einer Bearbeitung, was im kantonalen Recht noch zu ergänzen ist. Zu präzisieren sind auch die Formen der Beseitigung der Folgen widerrechtlicher Bearbeitungen. So ist die Beschränkung einer Datenbearbeitung anstelle der Löschung mit Ausnahme der Datensperrung nach § 13 ÖDSG im kantonalen Datenschutzrecht nicht spezifisch geregelt.

3.4.3 Bei der in den umzusetzenden Rechtsakten vorgesehenen Beschwerdemöglichkeit an den Datenschutzbeauftragten (Art. 17 und 52 f. DSRL, Art. 12bis E-SEV 108) handelt es sich nicht um ein formelles Beschwerderecht, sondern um einen Rechtsbehelf im Sinne einer aufsichtsrechtlichen Anzeige, wie dies im Verfahren vor dem Datenschutzbeauftragten nach §§ 32 ff. ÖDSG bereits heute vorgesehen ist. Allerdings muss die betroffene Person verbindliche Anordnungen des Datenschutzbeauftragten anfechten können (vgl. nachfolgend Ziff. 3.6.4).

3.4.4 Am Grundsatz der Unentgeltlichkeit von Gesuchen, welche die eigenen Personendaten betreffen, muss festgehalten werden (vgl. § 37 Abs. 2 Bst. b ÖDSG). Jedoch darf die Möglichkeit zur Kostenauflage bei offenkundig unbegründeten oder unverhältnismässigen Eingaben betreffend die eigenen Personendaten vorgesehen werden (Art. 12 Abs. 4 und 46 Abs. 3 DSRL, Art. 8 E-SEV 108).

3.5 Verantwortlichkeiten der datenbearbeitenden öffentlichen Organe

3.5.1 Aus dem Ausbau der Rechte der betroffenen Person ergeben sich korrespondierende Pflichten für die datenbearbeitenden öffentlichen Organe, namentlich die bereits behandelte Informationspflicht. Darüber hinaus werden die öffentlichen Organe auch hinsichtlich ihrer Kontrolle stärker in die Pflicht genommen und mit zusätzlichen Schutzmechanismen ausgerüstet.

3.5.2 Erhöhte gesetzliche Anforderungen gelten beim Bearbeitenlassen von Personendaten durch Dritte (Art. 22 f. DSRL). Das öffentliche Organ darf die Bearbeitung solcher Daten nur dann Dritten übertragen, wenn keine rechtlichen oder vertraglichen Vorschriften entgegenstehen und wirksam sichergestellt ist, dass die Personendaten nur so bearbeitet werden, wie es das öffentliche Organ selber tun dürfte. In einem entsprechenden Rechtssatz, Auftrag oder Vertrag müssen Gegenstand, Art und Dauer der Datenbearbeitung, die betroffenen Personen- bzw. Datenkategorien, die Rechte und Pflichten des beauftragten Dritten sowie des weiterhin die Aufsicht ausübenden öffentlichen Organs geregelt werden. Es muss insbesondere sichergestellt sein, dass der Dritte die Personendaten weisungsgemäss bearbeitet, der Verschwiegenheitspflicht unterliegt, die Rechte der betroffenen Personen wahrt, weitere Dritte nur mit Einwilligung des öffentlichen Organs beiziehen darf und die Personendaten nach Beendigung des Auftrages ordnungsgemäss zurückgibt bzw. löscht.

3.5.3 Gemäss Art. 25 DSRL müssen bestimmte Bearbeitungen in IT-Datensystemen protokolliert werden. Die Protokollierung ist wichtig, um die Begründung, den Zeitpunkt und die Identität der datenbearbeitenden Person und damit die Rechtmässigkeit des Datenbearbeitungsvorgangs überprüfen und Datenschutzverletzungen vorbeugen bzw. beseitigen zu können. Die Protokolle dürfen denn auch nur zur Überprüfung der Rechtmässigkeit der Datenbearbeitung, der Eigenüberwachung, der Sicherstellung der Integrität und Sicherheit der Personendaten sowie für

ein allfälliges Strafverfahren verwendet werden. Der Datenschutzbeauftragte soll diese Protokolle auf Verlangen einsehen können.
Allerdings stellt eine solche weitgehende Protokollierungspflicht in praktischer und technischer Hinsicht eine gewisse Herausforderung dar, da noch längst nicht alle Datenbearbeitungssysteme sämtliche verlangten Protokolldaten generieren können.
In der Botschaft zum neuen Bundesdatenschutzgesetz vertritt der Bundesrat die Ansicht, dass die automatisierten Datenbearbeitungssysteme, die von den Bundesorganen in der Schengen-Zusammenarbeit in Strafsachen betrieben werden, den Anforderungen von Art. 25 DSRL genügen (BBl 2017 S. 7181). Er schliesst jedoch nicht aus, dass sich aufgrund einer künftigen Schengen-Evaluation ein zusätzlicher technischer Handlungsbedarf ergeben könnte, der auch mit finanziellen Auswirkungen verbunden wäre. Diese Einschätzung dürfte auch für Datenbearbeitungen in kantonalen IT-(Teil)-Systemen im Rahmen der Schengener Polizeizusammenarbeit gelten, so dass gegenwärtig kein Handlungsbedarf besteht. Im Übrigen ist auf die bestehenden bzw. zu spezifizierenden Instrumente im Bereich der Datensicherheit zu verweisen, namentlich auf die Pflicht zur Registrierung solcher Datensammlungen und das Instrument der Datenschutzfolgeabschätzung.

3.5.4 Die Datenschutzfolgeabschätzung nach Art. 27 DSR, Art. 8bis E-SEV 108) ist dem kantonalen Datenschutzrecht bislang fremd. Sie ist durchzuführen, wenn die Bearbeitung aufgrund ihrer Art (z.B. durch Verwendung neuer Technologien), ihres Umfangs (z.B. Austausch sensibler Daten), ihrer Umstände und ihres Zweckes ein hohes Risiko für die persönlichen Rechte und Freiheiten der betroffenen Personen haben. Die Datenschutzfolgeabschätzung ist an sich eine klassische Risikobewertung eines Vorhabens, mit dem Unterschied, dass sie spezifisch auf den Umgang mit Personendaten ausgerichtet ist. Diese Abschätzung kann bei unbedenklichen Vorhaben formlos erfolgen.
Ergibt sich aus der Datenschutzfolgeabschätzung jedoch, dass die Bearbeitung ein hohes Risiko für die betroffenen Personen zur Folge hätte, muss das zuständige öffentliche Organ das Vorhaben beim Datenschutzbeauftragen in eine Vorabkonsultation nach Art. 28 DSRL geben. In diesem Fall hat die Folgeabschätzung mindestens eine allgemeine Beschreibung der Datenbearbeitungsvorgänge, eine Bewertung in Bezug auf die Risiken für die Grundrechte der betroffenen Person sowie der geplanten Abhilfemassnahmen, Sicherheitsvorkehren und Verfahren zum Schutz dieser Grundrechte und zur Gesetzeskonformität des Vorhabens zu enthalten. Es empfiehlt sich, bei einer solchen Datenschutzfolgeabschätzung auch die IT-Lieferanten und die mit der Datenbearbeitung befassten Stellen einzubeziehen. Die Folgeabschätzung ist nötigenfalls zu überprüfen und anzupassen. Allenfalls ergibt sich daraus auch eine einfachere und bessere Lösung für ein Bearbeitungsproblem.

3.5.5 Der frühzeitige Einbezug des Datenschutzbeauftragten bei allen datenschutzrelevanten Vorhaben ist ein wirksames Mittel des präventiven Datenschutzes. Damit kann verhindert werden, dass unzulängliche Datenbearbeitungssysteme und –vorgänge später mit einem erheblichen Aufwand angepasst oder nicht in Betrieb genommen werden können. Vorabklärungen mit dem Datenschutzbeauftragten im Zusammenhang mit neuen, komplexen Datensystemen sind deshalb geltende Praxis. Nach Art. 28 DSRL muss im kantonalen Recht neu verbindlich die Pflicht zur Vorabkonsultation des Datenschutzbeauftragten bei Rechtsetzungsvorhaben und anderweitigen Vorhaben zur Bearbeitung von Personendaten verankert werden, wenn die Datenschutzfolgeabschätzung oder die vorgesehene Form der Datenbearbeitung ein hohes Risiko für die Grundrechte der betroffenen Person ergeben hat. Ziel solcher Vorabkonsultationen ist es, rechtzeitig sicherzustellen, dass die verfassungs- und datenschutzrechtlichen Vorgaben eingehalten und die Risiken auf ein vernünftiges Mass reduziert oder durch rechtliche, technische sowie organisatorische Massnahmen weiter minimiert werden können.

3.5.6 In Art. 32 ff. DSRL ist die Funktion eines Datenschutzberaters vorgesehen. Dieser Datenschutzberater soll von der vorgesetzten Stelle eingesetzt und damit betraut werden, die datenbearbeitenden Amtsstellen bei allen mit dem Schutz von Personendaten zusammenhängenden Fragen zu beraten. Mit einer solchen internen Fachperson soll der Datenschutzbeauftragte in seiner Beratungsaufgabe entlastet werden.
Gemäss den umzusetzenden Rechtsakten genügt es, die Funktion des Datenschutzberaters nur für polizeiliche und justizielle Datenbearbeitungen vorzusehen und allenfalls bereichsspezifisch zu regeln. Es betrifft dies im Wesentlichen die Polizei, Strafverfolgung und den Strafvollzug. Im Rahmen der verwaltungsinternen Organisationsautonomie sind geeignete Personen, die sich auch mit zunehmend komplexeren Fragestellungen des Datenschutzes und der Digitalisierung zu befassen haben, mit einem entsprechenden Pflichtenheft als Datenschutzberater auszustatten. Die anderen Verwaltungszweige wie auch die Gemeinden und Bezirke sind, auch zufolge der Kantonalisierung der Strafverfolgung, davon nicht betroffen, können aber freiwillig Datenschutzberater einsetzen.

3.5.7 Schliesslich verlangen Art. 30 und 31 DSRL auch die Einführung der Pflicht des verantwortlichen öffentlichen Organs, den Datenschutzbeauftragten bzw. die betroffene Person über Datenschutzverletzungen unverzüglich zu informieren, wenn die Verletzung ein Risiko für deren Grundrechte birgt. Die praktische Schwierigkeit dürfte hier darin bestehen, dass eine Information überhaupt erst dann erfolgen kann, wenn die Datenschutzverletzung sichtbar wird, die Folgen ersichtlich sind und die betroffenen Personen eruiert werden können.

3.6 Befugnisse des Datenschutzbeauftragten

3.6.1 Die behördliche Datenbearbeitung muss durch ein völlig unabhängiges Kontrollorgan überwacht und überprüft werden können (Art. 42 ff. DSRL, Art. 12bis E-SEV 108). Diese institutionellen Garantien müssen mindestens die folgenden Elemente enthalten: Weisungsunabhängigkeit, Ausschluss von unvereinbaren Funktionen, Tätigkeiten oder Beziehungen, Wahl durch Aufsichtsorgan und nicht durch Kontrollierte, mindestens vierjährige Amtsdauer, Amtsenthebung nur bei Amtsunfähigkeit oder schwerer Amtspflichtverletzung, eigenes Budget und Auswahl des eigenen Personals.
Diesen Erfordernissen kommt das geltende Recht bereits nach (§ 28 ÖDSG, vgl. dazu auch Teilrevision der Geschäftsordnung des Kantonsrates vom 21. Oktober 2015 in GS 24-48a sowie RRB Nr. 748/2015 und 929/2015).
Von der Aufsicht des Datenschutzbeauftragten sind aufgrund der Gewaltenteilung (vgl. auch § 7 JG) gewisse Bereiche auszunehmen (so auch Art. 45 Abs. 2 DSRL, Art. 12bis E-SEV 108). Es sind dies:
- die Gerichte;
- andere Justizbehörden sowie der Regierungsrat und weitere Verwaltungsbehörden, soweit sie rechtsprechende Tätigkeiten ausüben;
- der Kantonsrat und seine parlamentarischen Kommissionen.

In diesem Sinne nimmt auch Art. 3 E-DSG die eidgenössischen Gerichte, die Bundesanwaltschaft, weitere rechtsprechende Bundesbehörden, die Bundesversammlung, aber auch den Bundesrat von der Aufsicht des Datenschutzbeauftragten aus.

3.6.2 Der Datenschutzbeauftragte muss über die erforderlichen Qualifikationen, Fachkenntnisse und Erfahrungen in Datenschutzfragen verfügen, um seine gesetzlichen Aufgaben und Befugnisse ausüben zu können (Art. 43 Abs. 2 DSRL). Dies ist ebenfalls ein Aspekt seiner Unabhängigkeit und Wirksamkeit.

3.6.3 Die zu übernehmenden Rechtakte weisen dem Datenschutzbeauftragten zusätzliche Aufgabenbereiche zu:

- So wird von ihm erwartet, dass er die für die Datenbearbeitungen verantwortlichen öffentlichen Organe und die Bevölkerung vermehrt für die Anliegen des Datenschutzes sensibilisiert (Art. 46 Abs. 1 DSRL, Art. 12bis E-SEV 108). Das betrifft im Besonderen auch Sicherheitsaspekte und die Eigenverantwortung. Diese fängt mit einem bewussten, achtsamen und sparsamen Umgang mit den eigenen Daten an.
- Zu diesem Zweck hat er auch die massgeblichen Entwicklungen in der Informations- und Kommunikationstechnologie in ihren Auswirkungen auf den Schutz von Personendaten zu verfolgen (Art. 46 Abs. 1 DSRL).
- Er ist zur Zusammenarbeit mit den Datenschutzbehörden der anderen Kantone, des Bundes und des Auslandes mit gleichwertigem Datenschutzniveau (Schengen-Staaten) verpflichtet und hat diesen Stellen Amtshilfe zu gewähren.

3.6.4 Die zu übernehmenden Rechtsakte statten den Datenschutzbeauftragten auch mit weitergehenden Befugnissen und Pflichten aus (Art. 44 Abs. 2, 47 Abs. 2, 49, 50 und 52 DSRL, Art. 12bis E-SEV 108):

- So muss er über wirksame Einwirkungsmöglichkeiten verfügen. Dazu gehören die bereits genannte Vorabkonsultation sowie förmliche Empfehlungen zu konkreten Datenbearbeitungen.
- Neu ist seine Kompetenz, bei Verstössen gegen das Datenschutzrecht oder nach Ablehnung bzw. Nichtbefolgen einer Empfehlung durch das datenbearbeitende öffentliche Organ verbindliche Anordnungen (in Form einer Verfügung) zu treffen. Die Anordnung ist anfechtbar und es ist der Rechtsweg (Verwaltungsgericht) festzulegen.
- Ihm ist das Recht einzuräumen, bei Verstössen gegen das Datenschutzgesetz bei der vorgesetzten Behörde des datenbearbeitenden öffentlichen Organs eine aufsichtsrechtliche Anzeige einzureichen. Fakultativ kann dem Datenschutzbeauftragten in einem solchen Fall auch das Recht eingeräumt werden, verwaltungsrechtliche Sanktionen, namentlich Bussen, gegen das säumige öffentliche Organ zu ergreifen (Art. 57 DSRL). Auf eine solche Möglichkeit soll aber verzichtet werden, da sie dem hiesigen Verständnis der Behörden- und Verwaltungsorganisation und der Aufsicht über die Verwaltungstätigkeit fremd ist und dafür Steuergelder aufgewendet bzw. auf den Konten der Staatskasse verschoben werden müssten. Im Übrigen soll der Datenschutzbeauftragte wie die öffentlichen Organe weiterhin berechtigt sein, bei bestimmten Datenschutzverletzungen Strafanzeige zu machen (kantonales Nebenstrafrecht gemäss § 38 ÖDSG).
- Er ist verpflichtet, die Eingaben der betroffenen Personen zu behandeln und hat dabei – und auch nach Beendigung seiner Funktion – dieselben Geheimhaltungsvorschriften einzuhalten wie die datenbearbeitenden öffentlichen Organe. Dies resultiert bereits aus §§ 30 und 31 ÖDSG.
- Schliesslich hat er bereits nach geltendem kantonalen Datenschutzrecht gegenüber dem Wahlorgan Rechenschaft abzulegen und dieses wie auch die Öffentlichkeit periodisch und bedarfsweise über wichtige Erkenntnisse seiner Kontrolltätigkeit und die Wirkung der Datenschutzvorschriften zu informieren (§ 29 Abs. 2 Bst. e ÖDSG).

4. Ergebnisse des Vernehmlassungsverfahrens

(…)

5. Erläuterungen zu den einzelnen Bestimmungen

Zur Unterscheidung zwischen dem geltenden Öffentlichkeits- und Datenschutzgesetz werden die nachfolgend kommentierten Bestimmungen des Revisionsentwurfs mit E-ÖDSG bezeichnet.

§ 2 Geltungsbereich

Abs. 2
Aus § 2 Abs. 1 ÖDSG resultiert, dass öffentliche Organe, die nicht hoheitlich, sondern privatrechtlich handeln, nicht dem kantonalen Datenschutzrecht unterstehen. Daran anknüpfend wird im neuen Abs. 2 präzisiert, dass für sie dann die Bestimmungen für die Datenbearbeitung durch private Personen nach dem Bundesdatenschutzgesetz oder anderen Bundeserlassen, die den Umgang mit Personendaten regeln, gelten (vgl. analoge Regelung von Art. 36 E- DSG für Bundesorgane). Weil aber solche öffentlichen Organe dadurch nicht zu Privatpersonen werden, bleibt die kantonale Aufsichtsbehörde zuständig. Für den Geltungsbereich des Öffentlichkeitsprinzips gilt diese Bestimmung selbstredend nicht.
Der bisherige Abs. 2 wird unverändert zu Abs. 3. Demnach bleiben spezielle Bestimmungen anderer Erlasse, nach denen bestimmte Informationen als geheim gelten oder welche den Zugang zu amtlichen Akten oder das Bearbeiten von Personendaten abweichend regeln, vorbehalten (für den Bereich des Öffentlichkeitsprinzips vgl. auch § 6 Abs. 1 ÖDSG). Dieser Vorrang zugunsten von Lex specialis ist vor allem in folgenden Bereichen zu beachten:

- Die (Nicht-)Öffentlichkeit von Sitzungen von öffentlichen Organen und die amtliche Information wird in § 45 KV sowie in den Spezialerlassen normiert.
- In Gerichtsverfahren sowie in Verfahren nach den bundesrechtlichen und den kantonalen Verfahrensordnungen regelt das anwendbare Verfahrensrecht die Bearbeitung von Personendaten und die Rechte der betroffenen Person. Es gilt zu vermeiden, dass auf dem Weg über das allgemeine Datenschutzrecht verfahrensrelevante Handlungen gegenüber der zuständigen Verfahrensbehörde geltend gemacht werden, die nach dem anwendbaren Verfahrensrecht nicht zulässig wären (vgl. BBl 2017 S. 7014). Dies steht im Einklang mit Art. 9 Ziff. 1 Bst. a E-SEV 108. Auf Bundesstufe werden die Verfahrensordnungen mit Ausnahme des erstinstanzlichen Verwaltungsverfahrens explizit vom Geltungsbereich des Datenschutzrechts ausgenommen (Art. 2 Abs. 3 E-DSG). Dabei wird auf das Kriterium der Rechtshängigkeit verzichtet, weil die massgebende Verfahrensordnung auch nach Abschluss des Verfahrens (u.a. bei der Aktenpflege, -einsicht und -aufbewahrung) anwendbar bleibt.
  Auf eine solche Abgrenzung wird mit Blick auf den allgemeinen Vorbehalt von § 2 Abs. 3 E-ÖDSG, der auch für erstinstanzliche Verfahren gilt, verzichtet (vgl. aber § 3 Bst a E-ÖDSG).

– Wie bis anhin in Art. 2 Abs. 2 Bst. d DSG werden in Art. 2 Abs. 4 E-DSG die öffentlichen Register des Privatrechtsverkehrs in der Zuständigkeit des Bundes (z.B. elektronisches Zivilstandsregister, Luftfahrzeugbuch sowie Marken-, Patent- und Designregister) vom Geltungsbereich des Bundesdatenschutzgesetzes ausgenommen, soweit das Spezialrecht den Zugang zu diesen Registern und die Rechte der betroffenen Personen regelt; dies im Bewusstsein, dass Art. 3 E-SEV 108 eine solche Ausnahme an sich nicht vorsieht. Der Bundesrat begründet diese mit dem Zweck der Beweiskraft dieser öffentlichen Register (Art. 9 ZGB), der nicht aus Datenschutzgründen beeinträchtigt werden darf.
  Die öffentlichen Register des Privatrechtsverkehrs in der Zuständigkeit der Kantone (Grundbuch, Schiffsregister, Handelsregister Betreibungs- und Konkursregister, Register der Eigentumsvorbehalte) unterstehen an sich dem kantonalen Datenschutzrecht. Allerdings darf das kantonale Datenschutzrecht die korrekte und einheitliche Anwendung des Bundesprivatrechts und den Grundsatz der Öffentlichkeit der Register nicht behindern. Vor diesem Hintergrund besteht auf kantonaler Stufe kein diesbezüglicher Regelungsbedarf, da der Vorbehalt von § 2 Abs. 3 E-ÖDSG für die öffentlichen Register des Privatrechtsverkehrs in der Zuständigkeit des Kantons – wie übrigens auch für öffentlich-rechtliche Register des kantonalen Rechts (Steuerregister, Einwohnerregister) – sinngemäss das Gleiche besagt wie Art. 2 Abs. 4 E-DSG.

§ 3 Ausnahmen vom Geltungsbereich

Vorbemerkung:
Auch wenn die umzusetzenden Rechtsakte an sich nur den Geltungsbereich des Datenschutzes betreffen, soll vom einheitlichen Konzept des Öffentlichkeits- und Datenschutzgesetzes möglichst nicht abgewichen werden.

Abs. 1
Bst. a
Ausdrücklich ausgenommen sind nach dem Gewaltenteilungsprinzip gemäss dem geltenden § 3 Bst. a die „gerichtlichen Behörden“. Dieser Begriff wird aber weder im ÖDSG noch in anderen kantonalen Erlassen klar definiert. Das Justizgesetz kennt den Begriff „Justizbehörden“, wozu die Gerichte (§ 4 JG), die Strafverfolgungsbehörden (§ 5 JG) sowie die weiteren Justizbehörden (§ 6 JG) zählen. Nicht in dieser Aufzählung enthalten sind jedoch der Regierungsrat und andere Verwaltungsbehörden, soweit ihnen ebenfalls Rechtsprechungskompetenzen zukommen. Es kann deshalb nicht unbesehen die Begriffsbestimmung des Justizgesetzes übernommen werden. Trotz des Vorbehalts von § 2 Abs. 3 E-ÖDSG zugunsten spezialgesetzlicher Vorschriften über das Bearbeiten von Personendaten ist klarzustellen, dass die Strafverfolgungs- und andere Justizbehörden wie auch Verwaltungsbehörden in der Verwaltungsrechtspflege in diesem Umfang vom Geltungsbereich des Öffentlichkeits- und Datenschutzgesetzes ausgenommen sind. Das betrifft im Wesentlichen den Regierungsrat, aber auch die Verwaltungsstrafbehörden und Verwaltungskommissionen (z.B. Schätzungskommission gemäss § 35 des Enteignungsgesetzes, EntG, vom 22. April 2009, SRSZ 470.100).
Die Strafverfolgungsbehörden haben insofern eine besondere Stellung, als vom Anwendungsbereich der vorliegend umzusetzenden DSRL alle Behörden erfasst werden, die zum Zweck der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten sowie zur Strafvollstreckung Personendaten bearbeiten und in Verbindung mit diesen Tätigkeiten öffentliche Gewalt ausüben. Das war grundsätzlich auch bereits nach dem bisherigen EU-Rahmenbeschluss 2008/977/JI sowie nach dem weiterhin geltenden EU-Rahmenbeschluss 2006/960/JI des EU-Rates vom 18. Dezember 2006 über die Vereinfachung des Austausches von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union der Fall. Allerdings unterstehen sie der Aufsicht des Datenschutzbeauftragten nicht,

soweit sie bei ihren Straf- und Bussenbescheiden rechtsprechend tätig sind. Überdies gelten für die Bearbeitung von Personendaten in einem hängigen Strafverfahren nicht die Bestimmungen des Öffentlichkeits- und Datenschutzgesetzes, sondern der Strafprozessordnung sowie des Justizgesetzes. Dies wird im neuen Abs. 2 klargestellt.

Bst. b
Dass die gesetzgebenden Behörden dem geltenden kantonalen Datenschutzrecht nicht unterstehen, geht nicht aus dem geltenden § 3 ÖDSG hervor, sondern lässt sich implizit aus der Aufzählung der öffentlichen Organe nach § 4 Bst. a und § 2 Abs. 1 ÖDSG ableiten. Zudem wurde im seinerzeitigen Bericht zur Gesetzesvorlage (RRB Nr. 104/2007) ausgeführt, dass Kantonsrat, Gemeindeversammlungen und Bezirksgemeinden zwar auch Personendaten bearbeiten, deswegen aber nicht dem Datenschutzrecht unterstellt werden müssen, sondern es genüge, dass die „vorbereitenden" Organe wie die Staatskanzlei und die Verwaltungsstellen diesem unterstehen. Dies soll so bleiben und steht mit den umzusetzenden Rechtsakten im Einklang. Diese Ausnahme wird nun ausdrücklich in die revidierte Bestimmung aufgenommen, um klarzustellen, dass mit den „Behörden" und „Kommissionen" gemäss § 4 Bst. a ÖDSG nicht die gesetzgebenden Behörden und deren Kommissionen gemeint sind. Ausserdem kann der Kantonsrat aus Gründen des Gewaltenteilungsprinzips nicht der Aufsicht des Öffentlichkeits- und Datenschutzbeauftragten unterstehen, wenn er selber die Oberaufsicht über diesen hat. Dass auch die Legislative sich zur Einhaltung der allgemeinen Datenschutzgrundsätze (vgl. § 8 ÖDSG) bekennt, geht aus dem neuen Einleitungssatz von § 3 ÖDSG hervor. Im Übrigen regelt die Spezialgesetzgebung den Umgang des Kantonsrates mit dem Schutz von Personendaten und dem Öffentlichkeitsprinzip (vgl. dazu auch Vernehmlassungsvorlage vom 15. Februar 2018 für eine neue Geschäftsordnung des Kantonsrates, GOKR).
Anders als in Art. 3 Abs. 2 Bst. b E-DSG, wo der Bundesrat von der Aufsicht des Datenschutzbeauftragten ausgenommen wird, soll der Regierungsrat wie bis anhin dem Geltungsbereich des Datenschutzgesetzes unterstehen (vgl. § 4 Bst. a ÖDSG).

Bst. c und d
Der bisherige Bst. c wird inhaltlich unverändert zu Bst. d. Auch Wuhrkorporationen unterstehen weiterhin dem Öffentlichkeits- und Datenschutzgesetz, soweit sie öffentliche Aufgaben erfüllen (vgl. Vernehmlassungsvorlage vom 8. Februar 2018 zur Teilrevision des Wasserrechtsgesetzes).

Abs. 2
Nach Art. 3 E-SEV 108 ist es nicht mehr zulässig, die hängigen Straf-, Zivil- und Verwaltungsverfahren generell vom Datenschutzrecht auszunehmen. Vielmehr gelten die Grundsätze des allgemeinen Datenschutzrechts (z.B. Rechtmässigkeit, Zweckbindung, Treu und Glauben, Datensicherheit) auch für die Datenbearbeitungen in der Zivil-, Straf- und Verwaltungsrechtspflege. Ein Vorbehalt zugunsten der massgeblichen Prozessordnungen und der bereichsspezifischen Datenschutzvorschriften, wie ihn bereits § 2 Abs. 2 ÖDSG bzw. Abs. 3 E-ÖDSG kennt, ist weiterhin zulässig. Demnach wird im neuen Abs. 2 klargestellt, dass die verfahrensrechtlichen Einsichtsrechte der Prozessordnungen, mithin auch im erstinstanzlichen Verwaltungsverfahren, den allgemeinen Informationsansprüchen nach dem Öffentlichkeits- und Datenschutzgesetz vorgehen. Demnach sind sie auch von der Aufsicht des Öffentlichkeits- und Datenschutzbeauftragten ausgenommen. Das übrige Verwaltungshandeln bleibt dem Geltungsbereich des Öffentlichkeits- und Datenschutzgesetzes weiterhin unterstellt.

§ 4 Begriffe

Bst. d
Die Bestimmung wird nach den einzelnen Personendatenkategorien gegliedert und zusätzlich differenziert. Die Aufzählung ist aber weiterhin nicht abschliessend.

Ziff. 1 Diese Kategorie entspricht der bisherigen Umschreibung.

Ziff. 2 Zum persönlichen Geheimbereich gehören auch besonders sensible Daten wie jene über das Erbgut (genetische Daten) oder solche über die sexuelle Orientierung. Es wird verlangt, dass diese Datenkategorien ausdrücklich genannt werden, wenn sie sich nicht zweifellos aus einer nicht abschliessenden Aufzählung ergeben.

Ziff. 3 Der heute überholte und wissenschaftlich nicht mehr haltbare Begriff „Rasse" bzw. „Rassenzugehörigkeit" zur Klassifizierung von Menschen wird durch den Begriff „Ethnie", sozialwissenschaftlich verstanden als Zugehörigkeit zu einer Menschen- bzw. Volksgruppe, ersetzt.

Ziff. 4 Hier bedarf es einer Erweiterung der Definition der besonders schützenswerten Personendaten um die „biometrischen Merkmale". Es sind dies physische, physiologische oder verhaltenstypische Merkmale einer Person, die mit speziellen technischen Verfahren gewonnen werden und ihre eindeutige Identifizierung ermöglichen (z.B. Fingerabdruckdaten, Gesichtsbilder aus Gesichtserkennungsprogrammen, Stimmmuster).

Ziff. 5 Auch Massnahmen des Kindes- und Erwachsenenschutzes gehören in diese Kategorie, soweit sie nicht zum persönlichen Geheimbereich zählen.

Ziff. 6 Diese Kategorie entspricht dem bisherigen Recht.

Bst. f

Die geltende Aufzählung der Formen der Bearbeitung von Personendaten ist zwar nicht abschliessend. Es sollen aber auch die zunehmend gebräuchlicheren Entsprechungen der digitalen Datenbearbeitung wie das Speichern und Löschen Erwähnung finden.
Unter Vernichten wird herkömmlich das physische Zerstören eines konventionellen wie auch elektronischen Datenträgers verstanden, so dass eine Rekonstruktion der Daten ausgeschlossen ist (vgl. § 22 ÖDSG sowie § 4b PolG). Das Überschreiben stellt eine Form des Löschens (sog. sicheres Löschen) dar.

Bst. g

Als besondere und mithin auch „gefährliche" Art des Umgangs mit Personendaten und anderen Daten ist neu explizit auch das „Profiling" aufzunehmen (Art. 3 Ziff. 4 RL 2016/680), da es nicht durch das blosse Verknüpfen von Personendaten abgedeckt ist. Eine einschlägige deutsche Übersetzung dieses Begriffs gibt es nicht. Unter Profiling wird jede Art der automatisierten Bearbeitung von Personendaten verstanden, die darin besteht, dass diese Personendaten dazu verwendet werden, um bestimmte persönliche Aspekte, die sich auf diese Person beziehen, zu bewerten, insbesondere, um deren Arbeitsleistung, finanzielle Situation, Konsumverhalten, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel zu analysieren oder vorherzusagen. Die neue Begriffsbestimmung entspricht im Wesentlichen derjenigen im Bundesdatenschutzgesetz (Art. 3 Bst. f E-DSG).
Es ist wichtig, dass diese Bearbeitungsformen ausdrücklich Erwähnung finden, um zu verdeutlichen, dass für diese höhere Anforderungen gelten als bei anderen Bearbeitungs- und Personendatenkategorien.
Vom „Profiling" zu unterscheiden sind „Persönlichkeitsprofile" als Zusammenstellung von Informationen, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit ermöglichen. Dieser Begriff findet in § 11 Abs. 1 ÖDSG Erwähnung, kann dort aber gestrichen werden, da es sich dabei nur um eine Kategorie von besonders schützenswerten Personendaten handelt, ohne dass eine differenziertere rechtliche Handhabung erfolgt. Ebenfalls nicht deckungsgleich ist „Profiling" mit der Tätigkeit eines polizeilichen „Profilers". Diese Bezeichnung ist in der Praxis geläufig, aber an sich unzutreffend, weil es dabei nicht darum geht, ein psychologisches Täterprofil oder ein charakteristisches Persönlichkeitsbild des Täters anzufertigen. Vielmehr handelt es sich um einen kriminalistischen Fallanalytiker, der zur Aufklärung eines Verbrechens aufgrund von Indizien, Spuren und Umständen auf Merkmale und Muster des Täters schliesst.

§ 8 Bearbeiten von Personendaten im Allgemeinen: Grundsätze

Die Bestimmung von § 8 ÖDSG regelt die zentralen Datenschutzgrundsätze. Es sind dies: Rechtmässigkeit, Zweckmässigkeit, Treu und Glauben, Richtigkeit, Verhältnismässigkeit und Datensicherheit.
Die Sicherheitsmassnahmen gemäss Abs. 4 betreffen nicht nur Vorkehrungen gegen das unbefugte Bearbeiten von Personendaten (zur Legaldefinition der Datenbearbeitungsvorgänge vgl. § 4 Bst. e E-ÖDSG), sondern auch gegen die unbeabsichtigte Beschädigung von Daten und deren Verlust. Konkretisierende Sicherheitsbestimmungen sind gegebenenfalls auf Verordnungs- und Weisungsstufe zu erlassen bzw. bereits vorhanden. Die Verordnung über die Informations- und Kommunikations-Technologie vom 1. September 2015 (IKTV, SRSZ 143.113) gilt allerdings nur für die Kantonsverwaltung sowie die weiteren Nutzer der kantonalen IKT.
Die Pflicht zur Sicherstellung der Datensicherheit ergibt sich auch aus Art. 7 E-SEV 108 sowie Art. 29 DSRL. Es müssen dem jeweiligen Risiko angemessene Sicherheitsvorkehrungen getroffen werden. Dazu gehört auch die Protokollierungspflicht für automatisierte Datenbearbeitungen. Lassen bestehende Datensysteme eine solche umfassende Zugangs-, Benutzer-, Eingabe-, Speicher- bzw. Übertragungskontrolle aus technischen Gründen nicht umfassend zu, wäre es nicht angemessen, wenn diese gänzlich ersetzt werden müssten.
Jedoch hat das verantwortliche öffentliche Organ mit anderen Methoden und Massnahmen die Rechtmässigkeit der Datenbearbeitung sicherzustellen.

§ 9 Rechtsgrundlage

Abs. 2
Neben den besonders schützenswerten Personendaten sind auch beim „Profiling“ (vgl. § 4 Bst. f E-ÖDSG) höhere Anforderungen an die gesetzliche Grundlage zu stellen.

Abs. 3
Bst. a
Diese Ausnahme entspricht im Wesentlichen der bisherigen Regelung von Abs. 3. Sie wurde seinerzeit eingeführt, um kurzfristig auftretenden Datenbearbeitungsnotwendigkeiten auch ohne entsprechende Rechtsgrundlage oder das Einverständnis der betroffenen Person Rechnung tragen zu können, z.B. wenn in einer Schulklasse Masern auftritt und die Mitschüler und Eltern darüber informiert werden müssen (vgl. RRB Nr. 104/2007). Eine analoge Bestimmung findet sich auch in Art. 30 Abs. 4 Bst. a E-DSG. Sie soll beibehalten werden und für alle Kategorien von Personendaten wie auch das Profiling gelten (vgl. Einleitungssatz von Abs. 3). Die Datenbearbeitung bzw. das Profiling muss in diesen Fällen vom Regierungsrat bzw. Bezirks- oder Gemeinderat in deren Zuständigkeitsbereich bewilligt werden und im öffentlichen Interesse liegen. Sodann ist zu gewährleisten, dass die Rechte der betroffenen Person nicht gefährdet sind.
Ohne Rechtsgrundlage und unabhängig vom Einverständnis der betroffenen Person soll eine Datenbearbeitung bzw. ein Profiling im Einzelfall künftig auch bewilligt werden können, wenn gegenüber der betroffenen Person ein begründeter Verdacht auf Rechtmissbrauch besteht, namentlich wenn sie die Erhebung oder Bearbeitung von Daten verhindern will, so dass beispielsweise staatliche Leistungen überprüft werden können. Ein überwiegendes öffentliches Interesse ist hier von vornherein gegeben. Die Rechte der betroffenen Person, vorab die Ansprüche nach §§ 26, 30 sowie 32 ff. E-DSG, werden dadurch nicht tangiert.

Bst. b
Art. 10 Bst. b DSRL erlaubt die ausnahmsweise Datenbearbeitung ohne Rechtsgrundlage zusätzlich, wenn sie notwendig ist, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen und die Einwilligung der betroffenen Person innert ange-

messener Frist nicht möglich ist. Diese Ausnahme wird vorliegend ebenfalls aufgenommen. Sie entspricht der Regelung von Art. 30 Abs. 4 Bst. c E-DSG.

§ 9a Datenschutzfolgeabschätzung

Abs. 1
Die Datenschutzfolgeabschätzung (vgl. Ausführungen unter Ziff. 3.5.4 und 3.5.5 vorstehend) ist an sich nichts anderes, als eine interne Vorbereitungsarbeit, um die Einhaltung der Datenschutzvorschriften belegen zu können. Umfang und Inhalt dieser Folgeabschätzung hängen vom jeweiligen Vorhaben ab und können bei unbedenklichen Vorhaben formlos gehalten werden. Die allgemeinen Anforderungen an Folgeabschätzungen, welche dem Datenschutzbeauftragten zur Vorabkonsultation zu unterbreiten sind, werden auf Verordnungsstufe konkretisiert (vgl. Abs. 3).

Abs. 2
Nach Art. 28 DSRL hat das verantwortliche öffentliche Organ dem Datenschutzbeauftragten Rechtsetzungsvorhaben, die den Datenschutz betreffen, sowie Vorhaben zur Bearbeitung von Personendaten, die ein hohes Risiko in Bezug auf die Grundrechte der betroffenen Person aufweisen, zur Vorkonsultation zu unterbreiten. Diese explizit zu regelnden Verpflichtungen sind zum Teil bereits im geltenden Recht umgesetzt:
- Der Einbezug des Datenschutzbeauftragten bei Rechtsetzungs- und anderweitigen Vorhaben, welche die Bearbeitung von Personendaten vorsehen, wird im Rahmen des Mitberichts- bzw. Vernehmlassungsverfahrens sichergestellt (§ 29 Abs. 1 Bst. b ÖDSG sowie § 27 Abs. 3 des Regierungs- und Verwaltungsorganisationsgesetz, RVOG, SRSZ 143.110, und § 40 KV).
- Sodann regelt § 29 Abs. 2 Bst. b ÖDSG die Aufgabe des Datenschutzbeauftragten, geplante Datenbearbeitung mit hohen Risiken für die Rechte und Freiheiten der betroffenen Person vor Inbetriebnahme zu überprüfen (sog. Vorabkonsultation).

Es geht somit noch darum, vorliegend die Pflichten des verantwortlichen öffentlichen Organs in Bezug auf die Vorabkonsultation und die in diesem Fall erforderlichen Mindestinhalte der Datenschutzfolgeabschätzung festzulegen. Die Vorabkonsultation ist nur erforderlich, wenn die Datenschutzfolgeabschätzung ergeben hat, dass ein hohes Risiko für die Grundrechte der betroffenen Personen durch die geplante Datenbearbeitung besteht.

§ 9b Datenschutzberatung

Abs. 1
Die Bestimmungen von Art. 32 ff. DSRL schreiben für den Bereich der justiziellen und polizeilichen Datenbearbeitungen einen Datenschutzberater vor. Damit soll der Datenschutzbeauftragte entlastet werden. Der Datenschutzberater kann auch für mehrere Behörden gemeinsam ernannt werden. Die Gerichte und andere rechtsprechende Behörden können von dieser Pflicht befreit werden. Dies geschieht durch § 3 ÖDSG und gilt ebenso für die weiteren dort geregelten Ausnahmen. Die Gemeinden und Bezirke sind (nach der Kantonalisierung der Strafverfolgung) nicht verpflichtet, Datenschutzberater einzusetzen, können dies aber auf freiwilliger Basis tun.

Abs. 2
Diese Bestimmung regelt die Mindestaufgaben der Datenschutzberater. Die Zuweisung entsprechender Pflichtenhefte an geeignete verwaltungsinterne Fachpersonen erfolgt im Rahmen der Organisationsautonomie bereichsspezifisch.

§ 11 Informationspflicht

Der Grundsatz, wonach Personendaten bei der betroffenen Person zu beschaffen sind, gilt auch für besonders schützenswerte Personendaten sowie Daten zu Vornahme eines Profilings. Insofern besteht bei § 10 ÖDSG kein Anpassungsbedarf.

In § 11 wird zunächst die Paragrafenüberschrift ersetzt, da es neu um die Informationspflicht bei allen Personendatenkategorien und nicht nur bei den besonders schützenswerten Personendaten geht (vgl. Art. 5 Ziff. 4 E-SEV 108 sowie Art. 13 f. und Art. 24 DSRL).

Abs. 1
Die revidierte Bestimmung regelt die Mindestinhalte der Information. Gestützt auf Art. 8 Abs. 1 Bst. a und Abs. 2 E-SEV 108 sowie Art. 11 DSRL besteht eine Informationspflicht auch dann, wenn eine automatisierte Verfügung bzw. Einzelfallentscheidung erfolgt, die erhebliche Auswirkungen auf die betroffene Person hat. Ihr muss die Möglichkeit eingeräumt werden, sich dazu bzw. den über sie bearbeiteten Personendaten zu äussern. Diese Möglichkeit ist in umfassenderer Weise im Rahmen des rechtlichen Gehörs gewährleistet (vgl. § 21 des Verwaltungsrechtspflegegesetzes, VRP, SRSZ 234.110). Auch gilt es, die datenschutzrechtlichen Spezialnormen der Verfahrensordnungen nicht mit dem allgemeinen Datenschutzrecht zu vermischen.
Sollen künftig in bestimmten Bereichen automatisierte Entscheidverfahren eingeführt werden, die nicht in einer Verfügung bzw. einem Einzelentscheid münden, aber gleichwohl erhebliche Auswirkungen auf die betroffene Person haben können, soll ihr Anhörungsrecht im entsprechenden Spezialgesetz verankert werden.
Um den mit einer individuellen Information verbundenen administrativen Mehraufwand in Grenzen zu halten, empfiehlt es sich in der Praxis, insbesondere bei systematischen Datenerhebungen (Gesuchsformulare, Anmeldungen, Registrierungen etc.) die Angaben zur Erfüllung der Informationspflicht direkt auf dem physischen oder elektronischen Dokument oder auf der entsprechenden Website des zuständigen öffentlichen Organs anzubringen.

Abs. 2
Die Einschränkung der Informationspflicht entspricht im Wesentlichen der bisherigen Regelung, wird jedoch ergänzt um den Fall, dass die betroffene Person bereits anderweitig im Umfang von § 11 Abs. 1 E-ÖDSG über die Datenbeschaffung bzw. -bearbeitung informiert wurde.

Abs. 3
Neu wird analog Art. 7bis Ziff 1bis E-SEV 108 vorgesehen, dass die Information gleichermassen eingeschränkt oder aufgeschoben werden kann wie bei der Einsichtnahme in die eigenen Personendaten (vgl. § 24 E-ÖDSG und § 25 ÖDSG). Sobald der Einschränkungsgrund wegfällt, ist die Information nachzuholen.

§ 16 Abrufverfahren

Den besonders schützenswerten Personendaten werden Profilingdaten gleichgestellt.

§ 17 Veröffentlichung

Den besonders schützenswerten Personendaten werden Profilingdaten gleichgestellt.

§ 20 Besondere Formen der Datenbearbeitung: durch Dritte

Die Bestimmung präzisiert die Anforderungen an die Bearbeitung von Personendaten durch Dritte im Auftrag des zuständigen öffentlichen Organs. Die analoge Bestimmung von Art. 8 E-DSG verwendet hierfür den in den umzusetzenden Rechtsakten verwendeten Begriff des „Auftragsbearbeiters“. Vorliegend wird auf die Einführung dieses Begriffs verzichtet, da im kantonalen Recht bei der Übertragung staatlicher Tätigkeiten an andere öffentliche Organe oder Private allgemein von „Dritten“ die Rede ist und in den für solche Leistungsaufträge geltenden Rechtsgrundlagen (Spezial-, Datenschutz-, Haftungs- oder Personalgesetzgebung) nicht unterschiedliche Bezeichnungen für diese Dritten eingeführt werden sollen. In der Praxis bestehen solche Auftragsverhältnisse, namentlich auch in Bezug auf Datenbearbeitungen, schon lange. Mit der zunehmenden

Digitalisierung gelten jedoch strengere Massstäbe. Der Regierungsrat regelt die weiteren datenschutzrechtlichen Anforderungen an solche Leistungsaufträge auf Verordnungsstufe.
Das öffentliche Organ muss aktiv sicherstellen, dass der beauftragte Dritte die Personendaten ebenso gesetzeskonform bearbeitet, wie er dies selber tun würde. Dies bedingt eine sorgfältige Auswahl, klare Instruktion und bedarfsweise Überwachung dieses Dritten. Um zu verhindern, dass das öffentliche Organ seine Verantwortung nicht mehr wahrnehmen kann, wenn der beauftragte Dritte die Datenbearbeitungen seinerseits noch weiter auslagert, bedarf dies zwingend seiner schriftlichen Zustimmung (Art. 22 Abs. 2 DSRL). Ein solcher Anwendungsfall wäre die Speicherung der Personendaten auf einer Cloud (IT-Infrastruktur über Internet). Befindet sich die Cloud im Ausland, gelten zusätzlich die Anforderungen von § 18 ÖDSG.

§ 22a Wiederherstellung der Datensicherheit

Während es beim Datenschutz in erster Linie um die Frage geht, ob Personendaten erhoben und bearbeitet werden dürfen, geht es bei der Datensicherheit darum, welche organisatorischen, technischen und anderweitigen Massnahmen zum Schutz der erhobenen Personendaten ergriffen werden müssen (vgl. § 8 Abs. 4 ÖDSG).
Art. 30 und 31 DSRL verpflichten das verantwortliche öffentliche Organ, dem Datenschutzbeauftragten die Verletzung der Datensicherheit unter gewissen Umständen zu melden. Die Meldung hat zu erfolgen, sobald das öffentliche Organ die Verletzung der Datensicherheit selber festgestellt hat oder vom beauftragten Dritten darüber orientiert wurde. Die Meldung ist aber nur erforderlich, wenn ein hohes Risiko für die Persönlichkeit oder Grundrechte der betroffenen Person besteht. Geringfügige Verletzungen sind nicht meldepflichtig. Ebenso wenig untersteht jede unbefugte Datenbearbeitung der Meldepflicht. Es ist deshalb zu definieren, was als meldepflichtige Datenschutzverletzung gilt. In Art. 4 Bst. g E-DSG wird der Begriff der Verletzung der Datensicherheit definiert als ein Vorgang, der dazu führt, dass Personendaten verlorengehen, gelöscht oder vernichtet, verändert oder Unbefugten offengelegt oder zugänglich gemacht werden, ungeachtet, ob er absichtlich oder widerrechtlich geschieht. Vorliegend wird eine analoge, nicht abschliessende Begriffsbestimmung vorgenommen.
Auch die betroffene Person bzw. der Datenempfänger sind in solchen Fällen grundsätzlich zu informieren, wenn sie zur Abwendung der Gefahr bzw. des Schadens einen Beitrag leisten können (z.B. durch Mitwirkung an der Rekonstruktion der Daten) oder sicherzustellen ist, dass die richtigen Personendaten weiterbearbeitet werden (vgl. dazu Art. 16 Abs. 5 DSRL). Diese Information erübrigt sich jedoch, wenn sie nicht möglich oder unverhältnismässig ist oder überwiegende öffentliche oder besonders schutzwürdige Interessen Dritter entgegenstehen. Eine analoge Bestimmung findet sich im Übrigen in Art. 22 E-DSG.
Damit die Meldepflicht an den Datenschutzbeauftragten Sinn ergibt und Wirkung entfaltet, müssen diesem auch die fachlichen und personellen Ressourcen (z.B. Informatikexperte) zur Verfügung gestellt werden, um das öffentliche Organ beraten und die Wiederherstellung der Datensicherheit überprüfen zu können. Dies ist aktuell nicht gewährleistet (vgl. dazu nachstehend Ziff. 6).

§ 23 Rechte der betroffenen Person: Register

Art. 24 DSRL sieht vor, dass die Strafverfolgungs- und Polizeibehörden ein Verzeichnis über ihre Datenbearbeitungstätigkeiten zu führen haben. Diese Verpflichtung könnte somit bereichsspezifisch im Polizei- und im Justizgesetz umgesetzt werden. Die Pflicht zur Führung eines solchen Registers gilt nach § 23 ÖDSG jedoch bereits für alle unter den Geltungsbereich des Öffentlichkeits- und Datenschutzgesetzes fallenden Behörden und soll beibehalten werden. Ebenso wird am Begriff „Datensammlungen“ anstelle der in der Richtlinie und in Art. 11 E-DSG verwendeten Bezeichnung der „Datenbearbeitungstätigkeiten“ festgehalten (§ 4 Bst. e ÖDSG).

Somit müssen weiterhin sämtliche von öffentlichen Organen des Kantons, der Bezirke und Gemeinden geführten Datensammlungen, in welchen Personendaten bearbeitet werden, in einem öffentlichen Register aufgeführt werden (vgl. Register der personenbezogenen Datensammlungen des Kantons Schwyz, einsehbar unter http://www.sz.ch/documents/REGISTER_V8.pdf). Das Register der Datensammlungen dient der Ausübung der Kontrollrechte jedes Einzelnen über die ihn betreffenden Personendaten (Recht auf Information, Berichtigung, Löschung oder Sperrung). Selbstredend nicht in das Register aufzunehmen sind Datensammlungen, die keine Personendaten enthalten. Sodann zählt der geltende § 23 Abs. 2 ÖDSG die Ausnahmen auf: Es sind dies Datensammlungen, die nur kurzfristig geführt werden, deren Inhalt bereits rechtmässig veröffentlicht wurde oder die reine Adresslisten darstellen. Der Begriff Adresslisten ist zu eng und soll durch den zutreffenderen Begriff der sogenannten Hilfsdatensammlungen ersetzt werden. Es handelt sich dabei nicht nur um Adresslisten, sondern auch um weitere Datensammlungen, die eine blosse Hilfsfunktion haben oder im Arbeitsprozess ausschliesslich dem persönlichen bzw. internen Gebrauch dienen (vgl. analog § 4 Bst. b ÖDSG für den Bereich des Öffentlichkeitsprinzips). § 23 Abs. 2 Bst. c ÖDSG soll daher allgemeiner umschrieben werden.

§ 24 Einsichtnahme, Auskunft

Das Recht, grundsätzlich kostenlos Auskunft darüber zu erhalten, ob und welche Daten über die eigene Person von einem öffentlichen Organ oder einem beauftragten Dritten bearbeitet werden, ist ein Kernpunkt des Datenschutzrechts und einer der wichtigsten Ausflüsse des verfassungsrechtlichen Persönlichkeitsschutzes. Die geltende Bestimmung entspricht im Wesentlichen den Anforderungen von Art. 8 Ziff. 1 Bst. b E-SEV 108 sowie Art. 12 und 14 DSRL. Sie bedarf aber einer Präzisierung in Bezug auf den Umfang des Auskunfts- bzw. Einsichtsrechts.
Abs. 1 erfährt redaktionelle Anpassungen in Bezug auf den Begriff „kostenlos“ und die Bezeichnung der für die Auskunft zuständigen Stelle. Die Kostenlosigkeit wird im Einleitungssatz sowie in § 37 Abs. 2 E-ÖDSG geregelt.
Abs. 2 wird neu eingefügt und umschreibt den Umfang des Auskunfts- bzw. Einsichtsrechts:
- Mindestangaben, die bei der Informationspflicht nach § 11 Abs. 1 E-ÖDSG gemacht werden müssen;
- Angaben über die Aufbewahrungsdauer der eigenen Personendaten;
- Angaben über die Herkunft der eigenen Personendaten.

§ 26 Weitere Ansprüche

Personendaten, die von einem öffentlichen Organ bearbeitet werden, müssen richtig sein. Die betroffene Person kann schriftlich und kostenlos verlangen, dass unrichtige Daten innert nützlicher Frist berichtigt werden (Art. 8 Ziff. 1 Bst. e E-SEV 108 sowie Art. 12 und 16 DSRL).
Werden Personendaten unbefugterweise, d.h. widerrechtlich bearbeitet, kann die betroffene Person verschiedene Rechtsansprüche geltend machen. Neu ausdrücklich im Gesetz zu regeln ist, dass die betroffene Person einen Anspruch auf Feststellung der Widerrechtlichkeit der Datenbearbeitung hat (Art. 8 E-SEV 108 und Art. 54 DSRL). Sodann kann die betroffene Person nicht nur verlangen, dass die Folgen der unbefugten Datenbearbeitung beseitigt werden, sondern die betreffenden Daten effektiv gelöscht oder deren Weitergabe an Dritte gesperrt wird.
Analog zu § 24 ÖDSG ist auch in dieser Bestimmung der Grundsatz der Kostenlosigkeit, soweit es die eigenen Personendaten betrifft, festzuhalten, um in Bezug auf die Gebührenregelung von § 37 Abs. 2 Bst. b ÖDSG Klarheit zu schaffen.
Weiter ist vorzusehen, dass die Beweislast primär beim verantwortlichen öffentlichen Organ liegt. Dies geschieht in Form einer Begründungspflicht im Bestreitungsfall. Die Folgen der Beweislosigkeit sind hingegen bereits im geltenden Abs. 2 geregelt.

Es ist zulässig, den Anspruch auf Berichtigung bzw. Vernichtung unrechtmässig erhobener Personendaten zu bestimmten Zwecken (z.B. Schutz der öffentlichen Sicherheit, Nichtbehinderung behördlicher oder gerichtlicher Untersuchungen) einzuschränken (Art. 9 E-SEV 108, Art. 16 Abs. 4 DSRL). Diese Ausnahmen werden im neuen Abs. 3 verankert.

§ 27 Zuständigkeit

Die Verantwortung für die Datenbearbeitungen ist im geltenden Recht an sich geregelt. Art. 8 Ziff. 1bis E-SEV 108 sowie Art. 19 und 21 DSRL verlangen jedoch eine klare Zuordnung der Verantwortlichkeiten. Es wird deshalb eine präzisierende Regelung aufgenommen für den Fall von gemeinsamen Datenbearbeitungen durch verschiedene Behörden. Hier gilt es, auch Art. 29 E-DSG zu beachten. Demnach regelt der Bundesrat das Kontrollverfahren und die Verantwortung für den Datenschutz, wenn ein Bundesorgan Personendaten mit anderen Bundesorganen, mit kantonalen Organen oder mit Privaten bearbeitet.
Die Nachweispflicht über die Einhaltung der Datenschutzvorschriften muss neu im Gesetz verankert werden (Art. 8bis Ziff. 1 E-SEV 108 und Art. 4 Abs. 4 DSRL). 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.). Wird auf eine solche Zertifizierung verzichtet, ist festzulegen, welche Dokumente notwendig sind, um diesen Nachweis erbringen zu können (z.B. Datensicherheits- oder Zugriffskonzept). Im Ausführungsrecht ist zu regeln, in welchen Fällen (z.B. nur für besonders schützenswerte Personendaten oder Profiling) ein DSMS obligatorisch sein soll.

§ 28 Beauftragte Person für Öffentlichkeit und Datenschutz: Wahl und Stellung

Gemäss Art. 43 Abs. 2 DSRL muss der Datenschutzbeauftragte über die für die Erfüllung seiner Aufgaben und zur Ausübung seiner Befugnisse entsprechende Sachkunde, Qualifikation und Erfahrung verfügen. Die fachlichen und persönlichen Qualifikationen des Datenschutzbeauftragten sind wesentlich, damit dieser seine Funktion unabhängig und wirksam ausüben kann. Dieses Erfordernis wird nun in Abs. 1 präzisiert.
Ausdruck der Unabhängigkeit des Kontrollorgans ist es auch, dass er unter Vorbehalt seiner Stellvertretung sein Personal im Rahmen des Budgets selber anstellen kann. Schliesslich muss auch sichergestellt sein, dass der Datenschutzbeauftragte nur bei dauernder Amtsunfähigkeit (z.B. aufgrund krankheitsbedingter Abwesenheit) oder bei schwerer Amtspflichtverletzung vorzeitig seines Amtes enthoben werden könnte. Die gesetzliche Verankerung einer solchen Regelung sollte indessen für alle auf Amtszeit gewählten Beamten in der Personalgesetzgebung geprüft werden.

§ 29 Aufgaben

Die geltende Bestimmung regelt die Aufgaben der beauftragten Person für den Bereich des Öffentlichkeitsprinzips und des Datenschutzes.

Abs. 1
Die bisherige Bestimmung von Art. 37 DSG hatte vorgesehen, dass Datenbearbeitungen durch kantonale Organe, die im Rahmen des Vollzugs von Bundesrecht erfolgen, dem Bundesdatenschutzrecht unterstehen, soweit die kantonalen Datenschutzvorschriften keinen angemessenen Schutz der Personendaten gewährleisteten. Sodann hatten die Kantone ein Organ zu bestimmen, das die Einhaltung der Datenschutzvorschriften überwacht. Da alle Kantone über Datenschutzvorschriften verfügen, die einen angemessenen Schutz gewährleisten, und selber auch zur Umsetzung der E-SEV 108 bzw. der DSRL verpflichtet sind, wird Art. 37 DSG nicht in das revidierte

Bundesdatenschutzrecht übernommen. Der Begriff „kantonales Kontrollorgan“ fällt demnach ebenfalls weg. Der Einleitungssatz von § 29 Abs. 1 ÖDSG ist entsprechend anzupassen.

In Bst. e und f werden spezifisch für den Bereich des Datenschutzes neue Aufgaben aufgenommen, die ebenfalls ressourcenrelevant sind (vgl. nachfolgend Ziff. 6):
Nach Art. 12bis Ziff. 2 Bst. e E-SEV 108 sowie Art. 46 Abs. 1 Bst. b und d DSRL gehört es explizit auch zu den Aufgaben des Datenschutzbeauftragen, die öffentlichen Organe und die Bevölkerungen für das Thema Datenschutz zu sensibilisieren. Faktisch ist dies bereits der Fall. Der Sensibilisierungsauftrag wird nun auch im Gesetz verankert.
Mit der zunehmenden Digitalisierung aller Lebensbereiche der Gesellschaft wird es zunehmend anspruchsvoller, die enormen Datenmengen und die dynamischen Datenflüsse in den verschiedensten Systemen zu überblicken und vor Missbräuchen zu schützen. Es ist ein vertieftes Verständnis der massgeblichen Entwicklungen im Bereich der Informations- und Kommunikationstechnologie in Bezug auf die Bearbeitung von Personendaten gefragt.

Abs. 2
Hier werden die Aufgaben des Datenschutzbeauftragten konkretisiert.

Bst. b
Diese Bestimmung wird an die Formulierung von § 9a E-ÖDSG angepasst, indem anstelle von „Rechte und Freiheiten“ der Begriff „Grundrechte“ gesetzt wird.

Bst. d
Nach Art. 48 E-DSG sind die kantonalen Behörden verpflichtet, dem Bundesdatenschutzbeauftragten die Informationen und persönlichen Daten, die er für die Erfüllung seiner gesetzlichen Aufgaben benötigt, zu übermitteln. Der Bundesdatenschutzbeauftragte hat seinerseits gegenüber den kantonalen Datenschutz-, Straf- und Polizeibehörden Amtshilfe zu leisten.
In Bst. d wird der Begriff „Kontrollorgan“ ersetzt. Im Übrigen regelt die Bestimmung bereits heute die Amtshilfe des Datenschutzbeauftragten mit seinen Amtskollegen in den anderen Kantonen, beim Bund und im Ausland.

§ 30 Befugnisse

Nach Art. 12bis Ziff. 2 Bst. a bis d und Ziff. 6 E-SEV 108 sowie Art. 17 und 47 Abs. 1 und 2 und 52 f DSRL muss der Datenschutzbeauftragte mindestens folgende Befugnisse besitzen:
- Er hat sich von Amtes wegen oder auf Anzeige hin mit einer geltend gemachten Datenschutzverletzung zu befassen. Er soll aber bei geringfügigen Beanstandungen auf eine weitere Untersuchung verzichten können (vgl. dazu auch Art. 43 Abs. 1 und 2 E-DSG). Dies regelt bzw. impliziert § 30 Abs. 1 ÖDSG bereits.
- Er muss ungeachtet allfälliger Geheimhaltungspflichten über umfassende Untersuchungsbefugnisse verfügen und Einsicht in alle Personendatenbearbeitungen nehmen können. Dies ist bereits aktuell durch § 30 Abs. 2 ÖDSG sichergestellt.
- Die anzeigende Person hat keine Parteistellung. Ihre Rechte werden sodann durch den Datenschutzbeauftragten wahrgenommen. Wurde die Anzeige von der durch die Datenschutzverletzung selber betroffene Person eingereicht, muss der Datenschutzbeauftragte sie innert nützlicher Frist über die Ergebnisse der Untersuchung informieren, damit sie gegebenenfalls die ihr zustehenden Rechte geltend machen kann (vgl. § 35 ÖDSG). In Art. 52 Ziff. 4 i.V.m. Art. 53 Ziff. 2 DSRL ist von einer Information innerhalb von drei Monaten die Rede, was aber auch mit Blick auf komplexere Untersuchungen als blosse Ordnungsfrist zu interpretieren ist und keine weiteren Rechtsfolgen auslösen kann. Diese spezifische Informationspflicht wird neu in § 30 Abs. 3 E-ÖDSG geregelt (vgl. analoge Bestimmung in Art. 43 Abs. 4 E-DSG). Der bisherige Abs. 3 wird in § 30a E-ÖDSG übernommen.

§ 30a Massnahmen

Mit Verweis auf die vorgenannten Erläuterungen zu § 30 und den umzusetzenden Rechtsakten sind die Interventionsmöglichkeiten des Datenschutzbeauftragten auszubauen. Die Massnahmen und das Verfahren werden daher in einem neuen § 30a E-ÖDSG geregelt.
Die bestehenden Sanktionsmöglichkeiten erweisen sich als ausreichend (vgl. § 38 ÖDSG). Es wäre zwar zulässig, aber systemfremd, dem Datenschutzbeauftragten Bussenkompetenz einzuräumen. Auch auf Bundesstufe soll auf derartige Verwaltungssanktionen verzichtet werden (BBl 2017 S. 7092).

Abs. 1
Der Datenschutzbeauftragte muss wirksame Interventionsinstrumente einsetzen können. Dazu gehört das Recht, sich im Rahmen von Vorabkonsultationen zu Vorhaben mit Bezug zu Personendatenbearbeitungen (Einführung von Datensystemen, Rechtsetzungsprojekte etc.) äussern zu können und zu geplanten oder laufenden Datenbearbeitungen oder Untersuchungsergebnissen Hinweise oder formelle Empfehlungen abgeben zu können. Der bisherige § 30 Abs. 3 wird in Bezug auf die verschiedenen Einwirkungsmöglichkeiten und die Handhabung der Empfehlung, die nicht nur bei Verstössen gegen Datenschutzvorschriften in Betracht kommen kann, angepasst.

Bst. a
Wie bis anhin, kann der Datenschutzbeauftragte das öffentliche Organ auf die Einhaltung der Datenschutzvorschriften oder problematische Bearbeitungsvorgänge hinweisen und Empfehlungen abgeben. Das öffentliche Organ hat dem Datenschutzberater mitzuteilen, ob es die Hinweise und Empfehlungen beachten wird

Bst. b
Dem Datenschutzbeauftragten ist auch eine „Beschwerde- bzw. Klagebefugnis“ einzuräumen. Es ist deshalb weiterhin die Möglichkeit vorzusehen, dass er mittels einer aufsichtsrechtlichen Anzeige an die übergeordnete Behörde gelangen kann.

Bst. c
Neu ist dem Datenschutzbeauftragten Verfügungskompetenz einzuräumen. Wenn das öffentliche Organ bzw. dessen übergeordnete Behörde seine Empfehlung nicht befolgt, kann er diese als Ganzes oder in Teilen als anfechtbare Verfügung erlassen. Auch wenn die umzusetzenden Rechtsakte nur den Datenschutz betreffen, macht es Sinn, die Verfügungskompetenz auch für das Öffentlichkeitsprinzip vorzusehen.

Abs. 2
Der Datenschutzbeauftragte ist neu auch befugt, eine Datenbearbeitung vorsorglich einzuschränken oder zu untersagen, wenn durch diese schutzwürdige Interessen gefährdet oder verletzt wurden.

Abs. 3
Alsdann ist es dem öffentlichen Organ überlassen, eine strittige Anordnung des Datenschutzbeauftragten gerichtlich überprüfen zu lassen. Sinnvollerweise ist hierbei als Rechtsmittel die Verwaltungsgerichtsbeschwerde vorzusehen (§ 51 Bst. b VRP). Die vorsorgliche Anordnung kann ebenfalls vom Verwaltungsgericht überprüft werden.

§§ 33 und 34 Schlichtungsverfahren

Das freiwillige Schlichtungsverfahren nach §§ 33 f. ÖDSG wurde nach seinem Verständnis trotz der systematischen Einbettung dieser Bestimmungen in die gemeinsamen Verfahrensbestimmungen für den Öffentlichkeits- und Datenschutzbereich in übereinstimmender Praxis mit anderen Kantonen stets nur beim Öffentlichkeitsprinzip angewandt. Anlässlich der vorliegenden Revi-

sion soll über diese bewährte und unbestrittene Praxis im Gesetz Klarheit geschaffen werden. Bei der Geltendmachung von Ansprüchen aus dem Öffentlichkeitsprinzip besteht somit weiterhin die Wahl zwischen einer anfechtbaren Verfügung und dem Schlichtungsverfahren.

§ 37 Gebühren und Entgelte

Nach Art. 46 Abs. 3 DSRL dürfen für die Bearbeitung von Gesuchen, welche die eigenen Personendaten betreffen, grundsätzlich keine Gebühren erhoben werden. Der betroffenen Person dürfen somit aufgrund ihrer Gesuche beim zuständigen öffentlichen Organ nach §§ 24 und 26 ÖDSG wie auch der diesbezüglichen Aufgabenerfüllung des Datenschutzbeauftragten grundsätzlich keine Kosten auferlegt werden.
Es ist hingegen unter einem ausdrücklichen Gesetzesvorbehalt zulässig, bei missbräuchlichen Gesuchen (Umgehung des Akteneinsichtsrechts, Ausforschung der Gegenpartei vor einem Prozess, wiederholte Anfragen in querulatorischer Absicht) sowie bei Begehren, die einen ausserordentlichen Aufwand (vgl. auch § 5 Abs. 2 ÖDSG) verursachen, eine angemessene Gebühr zu verlangen. Diese richtet sich nach den Ansätzen der Gebührenordnung für die Verwaltung und die Rechtspflege im Kanton Schwyz (GebO, SRSZ 173.111) und kann sowohl vom öffentlichen Organ als auch vom Datenschutzbeauftragten erhoben werden. Sie sind im Bestreitungsfall begründungspflichtig.
Das Schlichtungsverfahren bleibt jedoch kostenlos (§ 37 Abs. 3 ÖDSG).

§ 39 Übergangsbestimmungen

Abs. 2

Bst. a
Die Informationspflicht bei der Beschaffung von Personendaten gemäss § 11 E-ÖDSG gilt neu nicht mehr nur für besonders schützenswerte Personendaten, sondern allgemein. § 11 E-ÖDSG hat auch Relevanz für das Auskunftsrecht nach § 24 Abs. 2 E-ÖDSG. Die Einführung dieser Neuerung bedingt technische und administrative Vorbereitungen (vgl. Ausführungen zu § 11 E-ÖDSG). Gleiches gilt in Bezug auf das Instrument der Datenschutzfolgeabschätzung und die Vorabkonsultation des Datenschutzbeauftragten nach § 9a E-ÖDSG. Es ist dafür eine angemessene Umsetzungsfrist von zwei Jahren (analog Art. 63 Abs. 1 E-DSG) einzuräumen. Im Anwendungsbereich der DSRL ist eine solche Umsetzungsfrist jedoch nicht möglich. Eine sofortige Umsetzung ist auch bei der Information bei Verletzungen der Datensicherheit angezeigt (§ 22a Abs. 3 E-ÖDSG), zumal hier die Information ausdrücklich unterbleiben kann, wenn sie nur mit einem unverhältnismässigem Aufwand möglich ist.

Bst. b
Hier geht es einerseits um eine verhältnismässige Anpassung der zahlreichen bestehenden Datenbearbeitungen an die Vorgaben des neuen Rechts. Insbesondere kann nicht verlangt werden, dass für bestehende, rechtmässige Datenbearbeitungen, deren Rechtsgrundlagen und Bearbeitungszweck unverändert bleibt, eine Datenschutzfolgeabschätzung und Vorabkonsultation, also Instrumente ,die auf erst geplante Datenbearbeitungen ausgerichtet sind, nachgeholt werden müssten. Das würde eine unzulässige Rückwirkung bedeuten.

Bst. c
Mit einer spezifischen übergangsrechtlichen Bestimmung in Bezug auf hängige Verfahren nach der Datenschutzgesetzgebung, welche dem intertemporalen Recht nach dem Verwaltungsrechtspflegegesetz als subsidiär anwendbares Verfahrensrecht vorgeht, soll Rechtssicherheit geschaffen und der Vertrauensgrundsatz geschützt werden. Die Bestimmung lehnt sich an Art. 65 E-DSG an.

6. Personelle, finanzielle und weitere Auswirkungen

6.1 Die rechtlichen Vorgaben verlangen, dass der Datenschutzbeauftragte seine Aufgaben unabhängig, effektiv und wirksam wahrnehmen kann (Art. 12bis Ziff. 5 E-SEV 108 sowie Art. 47 Abs. 4 DSRL). Er hat zugunsten der Individuen einen Grundrechtsauftrag, namentlich die Wahrung ihrer Persönlichkeitsrechte, zu erfüllen. Gleichzeitig hat er die Behörden zu beraten und zu unterstützen, damit sie die im Rahmen ihrer Aufgabenerfüllung erforderlichen Bearbeitungen von Personendaten gesetzeskonform vornehmen können.
Der Datenschutzbeauftragte kann dies nur gewährleisten, wenn er über die nötigen Befugnisse verfügt, die erforderlichen personellen, fachlichen, technischen und finanziellen Ressourcen zugeteilt erhält und den an ihn gestellten hohen fachlichen Anforderungen, namentlich durch Fachaustausch und Weiterbildung, genügt.

6.2 Aufgrund der neuen, zusätzlichen Aufgaben und Kompetenzen, die der Datenschutzbeauftragte im Kanton Schwyz wie auch in den Kantonen Obwalden und Nidwalden zu erfüllen haben wird, wird er mit zusätzlichen fachlichen, personellen und finanziellen Mitteln auszustatten sein.

- So muss er wirksame Kontrollen darüber machen können, ob die öffentlichen Organe mit den ihnen von den Bürgerinnen und Bürger anvertrauten Personendaten sorgfältig und datenschutzkonform umgehen. Es betrifft dies namentlich die Bearbeitung von besonders schützenswerten Personendaten in organisationsübergreifenden Datensystemen, automatisierte Bearbeitungen von Personendaten zwecks Vornahme von Profilings oder die Auslagerung von Datenbearbeitungen an Dritte (vgl. §§ 9 ff. sowie § 20 E-ÖDSG).
- Die Geschäftslast des Datenschutzbeauftragten ist bereits heute erheblich. Die Anfragen und Gesuche müssen innert nützlicher Frist, zunehmend auch vordringlich bearbeitet werden können, um Datenschutzverletzungen verhindern oder unterbinden zu können.
- Auf das fehlende Spezialwissen in den Bereichen Informatik und Datensicherheit wurde bereits in den Ausführungen zu §§ 22a und 29 E-ÖDSG hingewiesen. Dieses ist auch bei der Vorabkonsultation zu Datenfolgeabschätzungen von erheblicher Bedeutung. Es ist davon auszugehen, dass der Datenschutzbeauftragte vermehrt komplexe Projekte zum Schutz der durch digitale Datenbearbeitungen und autonome Systeme betroffenen Personen zu begleiten haben wird.
- Auch die Formalisierung des Verfahrens, die Einräumung der Verfügungskompetenz, die daraus resultierenden Beschwerdeverfahren und die Vertretung der Interessen der Gesuchsteller werden zusätzliche Ressourcen binden.
- Ein Mehraufwand wird schliesslich auch aus der vermehrten Beratung bei komplexen und sensiblen Datenbearbeitungsfragen, der Verfolgung der datenschutzrelevanten Entwicklungen sowie der behördlichen Zusammenarbeit und Amtshilfe resultieren.

Der Öffentlichkeits- und Datenschutzbeauftragte ist das Datenschutzaufsichtsorgan für die Kantone Schwyz, Obwalden und Nidwalden. Im Kanton Schwyz ist er zusätzlich Öffentlichkeitsbeauftragter. Er verfügt für die Wahrnehmung dieser Funktionen gegenwärtig über personelle Ressourcen im Umfang von 180 Stellenprozenten, wovon 10% für den Bereich des Öffentlichkeitsprinzips im Kanton Schwyz vorgesehen sind. Er übt seine Aufgabe in einem 90%-Pensum aus. Die Stellvertretung ist mit 50 Stellenprozenten dotiert. Auf die Administration entfallen die restlichen 40%.
Unter Vorbehalt der gesetzlichen Ausgestaltung der Kompetenzen und Aufgaben des Öffentlichkeits- und Datenschutzbeauftragten und den Bedürfnisse der Kantone Obwalden und Nidwalden ist von einer Aufstockung der datenschutzrechtlichen Ressourcen um rund 50 zusätzliche Stellenprozente auszugehen. Dabei ist zu berücksichtigen, dass Spezialwissen im Bereich Informatik

und Datensicherheit einer rasanten technologischen Entwicklung unterliegt und es je nach Sachgebiet und Themenkomplex zweckmässiger und kostengünstiger sein kann, wenn eine spezifische datenschutzrechtliche bzw. technische Fragestellung von einem externen Experten geklärt wird.

6.3 Im Zeitalter der evolutionären Digitalisierung und von Big Data werden die organisatorischen, personellen und technischen Massnahmen zur Kontrolle von sich verselbständigenden Datenflüssen an ihre Grenzen stossen. Auch verfügen bestehende Datenverarbeitungssysteme noch nicht über alle Funktionalitäten (u.a. Protokollierungspflichten), um den detaillierten Sicherheitsanforderungen auf praktischer und technischer Ebene in umfassender Weise nachkommen zu können, sei es, weil sie unter einem anderen Fokus entwickelt wurden oder weil sie technologisch nicht dazu im Stande sind. Ein zusätzlicher technischer Handlungsbedarf wird mit finanziellen und personellen Auswirkungen verbunden sein, der heute noch nicht abschätzbar ist.