Entwurf der Justizverwaltung
1. Mai 2007/ab

Bericht des Sicherheits- und Gesundheitsdepartements zum Entwurf eines Gesetzes über den Datenschutz

vom ...

Herr Präsident
Sehr geehrte Damen und Herren Kantonsräte

Wir unterbreiten Ihnen mit dieser Botschaft den Entwurf eines Gesetzes über den Datenschutz (Datenschutzgesetz; DSG) mit dem Antrag, auf die Vorlage einzutreten.

Sarnen, ...

Im Namen des Regierungsrats

Landammann: Hans Wallimann

Landschreiber: Urs Wallimann

Inhaltsverzeichnis

1. Übersicht

Aufgrund der internationalen Bestrebungen, den grenzüberschreitenden Datentransfer, der letztlich keine Grenzen kennt, sowie den wachsenden Einsatz der modernen Informations- und Kommunikationstechnologien in fast allen Lebensbereichen bzw. die enorme Intensivierung der Datenverarbeitung und -verbreitung in Gesellschaft, Wirtschaft und Staat zu regeln, wurden auf internationaler und nationaler Ebene gesetzliche Grundlagen geschaffen. Diese bezwecken, die Hindernisse für die notwendigen Datenbearbeitungen wie auch für den freien Datenverkehr aus dem Weg zu räumen, ohne den Schutz von personenbezogenen Daten zu beeinträchtigen. Mit dieser Zielsetzung entwickelte sich der Datenschutz seit zwei Jahrzehnten stetig.

Mit dem Beitritt zu verschiedenen internationalen Vereinbarungen verpflichteten sich Bund und Kantone, einen entsprechenden datenschutzrechtlichen Standard einzuführen. Als letzte Schritte in dieser Entwicklung sind die Assoziierungsabkommen betreffend die Besitzstände von Schengen und Dublin sowie das Zusatzprotokoll des Europarats betreffend das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten zu nennen.

Speziell die Assoziierungsabkommen werden erst in Kraft gesetzt, nachdem die Vertreter der EU sich aufgrund einer Evaluation vor Ort davon überzeugt haben, dass die schweizerische Gesetzgebung – auf eidgenössischer wie auch kantonaler Stufe – dem Schengen/Dublin-Standard entspricht.

Der Kanton Obwalden blieb von der obgenannten Entwicklung weitgehend unberührt. Die neuen internationalen und nationalen Rechtsgrundlagen im Datenschutzbereich fordern nun aber auch von ihm, sich an den entsprechenden Standard anzupassen. Allein er kann sich hiezu nicht auf eine bereits bestehende, umfassende und abschliessende Gesetzgebung stützen. Deshalb ist die datenschutzrechtliche Materie im Rahmen eines Datenschutzgesetzes völlig neu zu regeln; freilich wird darin das bisherige Datenschutzrecht eingearbeitet.

Der minimal einzuführende Datenschutzstandard, den die öffentlichen Organe zukünftig zu beachten haben, wurde u.a. durch die Konferenz der Kantonsregierungen (KdK) in einer Wegleitung festgehalten. Er betrifft insbesondere folgende Bereiche:

- *Qualität der Daten;*
- *Zulässigkeit der Verarbeitung von Daten;*
- *besondere Kategorien der Verarbeitung;*
- *Information der von der Datenverarbeitung betroffenen Personen;*
- *Auskunftsrecht der betroffenen Personen und Ausnahmen;*
- *Vertraulichkeit und Sicherheit der Verarbeitung;*
- *Meldepflicht der Verarbeitungen, Vorabkontrolle, Register;*
- *Rechtsmittel, Haftung, Sanktionen;*
- *Transfer von Personendaten aus einem Mitgliedstaat in ein Drittland;*
- *Behörden (Stellung, Aufgaben, Befugnisse).*

Der internationale Standard verpflichtet die Kantone, eine Kontrollbehörde mit weitreichenden Aufgaben und Befugnissen einzurichten. Die Kontrollbehörde muss in völliger Unabhängigkeit und mit effektiver Wirksamkeit arbeiten können. Dies bedingt einerseits die notwendigen institutionellen Garantien wie auch die erforderlichen personellen und finanziellen Ressourcen.

Dabei ist vorliegend zu unterscheiden zwischen der Schaffung einer entsprechenden gesetzlichen Grundlage sowie der Einsetzung eines solchen Organs. In Bezug auf Letzteres sieht der Entwurf eine Kompetenzdelegation an den Regierungsrat vor, die Zusammenarbeit mit anderen Kantonen mittels Vereinbarung zu regeln. Als Pendant dazu initiierte die Zentralschweizerische Regierungsratskonferenz (ZRK) ein Projekt betreffend eines gemeinsamen Kontrollorgans.

2. Auftrag

In der integrierten Aufgaben- und Finanzplanung (IAFP) 2007 – 2010 der Justizverwaltung ist für das Jahr 2007 unter Projekte aufgeführt:

– Umsetzung der internationalen Datenschutzbestimmungen (Schengen/Dublin, Zusatzprotokoll vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bzgl. Aufsichtsbehörden und grenzüberschreitender Datenübermittlung)
– Umsetzung der nationalen Datenschutzbestimmungen.

Dies entspricht dem Ziel Nr. 7 der Amtsdauerplanung des Regierungsrats 2006 bis 2010.

Mit Beschluss vom 7. November 2006 (Nr. 237, Ziff. 2.2.3) entschied der Regierungsrat, am Zusammenarbeitsprojekt der Zentralschweizerischen Regierungskonferenz (ZRK) betreffend eines gemeinsamen, unabhängigen Datenschutzkontrollorgans teilzunehmen (vgl. Anstoss des ZRK-Ausschusses vom 18. September 2006, Antrag 4). Der kantonale Datenschutzbeauftragte wurde als Mitglied der eingesetzten Arbeitsgruppe zur Erarbeitung der notwendigen Grundlagen bestimmt.

3. Projektorganisation

3.1 Zeitplan

Mit dem Beitritt zu internationalen Vereinbarungen verpflichteten sich Bund und Kantone, ihre datenschutzrechtlichen Bestimmungen entsprechend umzusetzen.

Im Speziellen die Assoziierungsabkommen betreffend die Besitzstände von Schengen und Dublin werden erst in Kraft gesetzt, nachdem die Vertreter der EU sich davon überzeugt haben, dass die schweizerische Gesetzgebung – auf eidgenössischer wie auch kantonaler Stufe – dem Schengen/Dublin-Standard entspricht. Die Evaluation ist zweistufig (Beantwortung des Fragebogens/Prüfung der praktischen Umsetzung vor Ort).

Der momentan gültige Zeitplan des Bundes stellt sich wie folgt dar:

– erste Hälfte 2007:
    – Erstellung eines detaillierten "Action Plans" durch den Bund;
    – Information betreffend Evaluationsplanung durch die EU;
– Spätsommer/Herbst 2007 (ca.):
    – Ratifizierung der Assoziierungsabkommen durch die EU;
    – Inkrafttreten[1] der Assoziierungsabkommen;
    – "declaration of readiness“ durch die Schweiz (Start des Evaluationsprozesses);
    – Vorbereitung der Evaluierung durch die Schengen Staaten (insb. Erstellung des zu beantwortenden Fragebogens, erste Programm-Planung betreffend die Evaluationen vor Ort);
– Herbst 2007 (ca.):
    – Beantwortung des Fragebogens durch die Schweiz;
    – Vorbereitung der Evaluationen vor Ort;
        – in der Arbeitsgruppe SCH-EVAL (insbesondere Besprechung der Antworten auf den Fragebogen, Präsentation der Organisationsstrukturen, geltenden Normen und aktuellen Zahlen, Erstellung des definitiven Evaluationsprogramms sowie Zusammenstellung der Expertenteams);
        – in der Schweiz (insbesondere Vorbereitung der Infrastruktur, Ausbildung des Personals);
– Winter/Frühling 2008 (ca.):

[1] Unterscheidung zwischen „Inkrafttreten“ und „Inkraftsetzung“. Inkrafttreten meint, dass die Schweiz das weiterentwickelte Schengenrecht übernimmt. Inkraftsetzung meint, dass die Verträge in der Schweiz effektiv anwendbar sind (Herbst 2008).

  - Durchführung der Evaluationen vor Ort;
- Frühsommer 2008 (ca.):
  - Inkraftsetzungsbeschluss durch EU-Rat (Feststellung der Erfüllung des Schengen/Dublin-Standards);
- bis Herbst 2008:
  - Durchführung allenfalls notwendiger Nachbesserungen;
  - Evaluation SIS;
- Herbst 2008:
  - Inkraftsetzung der Assoziierungsabkommen (auf den Flugplanwechsel).

Wenn die Schweiz voraussichtlich im Spätsommer 2007 die "declaration of readiness" verkündet, muss der Gesetzgebungsprozess in den Kantonen soweit fortgeschritten sein, dass für die EU ersichtlich ist, welches Recht bei der Inkraftsetzung von Schengen/Dublin gelten wird und welche Ressourcen für den Datenschutz zur Verfügung stehen. Konkret heisst dies, dass entsprechende gesetzliche Regelungen im Entwurf von der Regierung spätestens im August 2007 zuhanden des Kantonsparlaments verabschiedet sein müssen.

3.2 Projektressourcen

Auf den 1. Juli 1997, d.h. auf den Zeitpunkt der Inkraftsetzung der heute geltenden Datenschutzbestimmungen im StVG[2] wurde erstmals ein Datenschutzorgan einsetzt, dem allerdings aufgrund des damals anfallenden Aufwands im Datenschutzbereich kein zusätzliches Pensum geäufnet wurde.

Der kantonale, interkantonale sowie internationale Informationsaustausch hat sich in den letzten Jahren stark gewandelt. Heute wird der Informationsaustausch – vor allem aus Gründen der staatlichen Leistungsoptimierung – vermehrt über elektronische Datenübermittlungs- und Datenbanksysteme abgewickelt, was einen höheren und komplexeren Datendurchfluss zur Folge hat. Für das Datenschutzorgan ist es unmöglich geworden, unter den Bedingungen und Voraussetzungen von damals die vermehrten Bedürfnisse von Bevölkerung und Verwaltung nach Beratung und Klärung zu bearbeiten.

Folgerichtig hat der Regierungsrat im Staatsvoranschlag 2007– auf Antrag des Sicherheits- und Gesundheitsdepartements – für die Umsetzung der Verträge von Schengen/Dublin, welche eine ausserordentliche Aufgabe des Datenschutzorgans darstellen, ein Projektbudget gesprochen.

4. Ausgangslage

4.1 Entwicklung im Bereich des Datenschutzes

Angesichts des Informationsflusses, der letztlich keine Grenzen kennt, drängte sich schon früh eine internationale Zusammenarbeit auf, um ein möglichst hohes Datenschutzniveau bei gleichzeitiger Gewährleistung des freien grenzüberschreitenden Informationsaustausches sicherzustellen. Mit dieser Zielsetzung hat der Europarat das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981 beschlossen (Europarats-Konvention 108 [nachfolgend ER-Konv 108]; SR 0.235.1). Dieses Übereinkommen trat für die Schweiz am 1. Februar 1998 in Kraft.

Aufgrund der internationalen Bestrebungen, den grenzüberschreitenden Datentransfer zu regeln sowie des wachsenden Einsatzes der modernen Informations- und Kommunikationstechnologien in fast allen Lebensbereichen bzw. der enormen Intensivierung der Datenverarbeitung und -verbreitung in Gesellschaft, Wirtschaft und Staat wurde auf eidgenössischer Ebene das Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG),

---

[2] Regierungsratsbeschluss (Nr. 128) vom 10. Juni 1997.

in Kraft seit dem 1. Juli 1993, erlassen; es gilt für das Bearbeiten von Daten natürlicher und juristischer Personen durch Privatpersonen und Bundesorgane, nicht aber für die Datenbearbeitung durch kantonale Organe (BBl 1988 II 413 ff.).

In der Folge wurden in der Schweiz die meisten kantonalen Datenschutzregelungen geschaffen, welche die elektronische Datenverarbeitung durch öffentliche Organe regelten. So stammen auch die Datenschutzbestimmungen des Kantons Obwalden aus dieser Zeit; vereinzelte Datenschutzbestimmungen bestanden bereits im kantonalen Recht.[3]

Die bilateralen Abkommen zwischen der Schweiz und der EU über die Assoziierung an Schengen und Dublin wurden am 26. Oktober 2004 vom Bundesrat unterzeichnet und am 5. Juni 2005 von den Schweizer Stimmberechtigten angenommen. Die Abkommen sehen u.a. im Rahmen der Zusammenarbeit zur Stärkung der inneren Sicherheit den grenzüberschreitenden Austausch von Personendaten vor. Als Gegengewicht ist deshalb die Verstärkung des Datenschutzes ein Hauptanliegen der Schengener Gesetzgebung. Die Schweiz hat mit den erwähnten bilateralen Abkommen sich, d.h. Bund und Kantone, verpflichtet, diesen Standard ins landesinterne Recht zu übernehmen (BBl 2004 5965 ff.).

Am 8. November 2001 wurde das Zusatzprotokoll des Europarats zur ER-Konv 108 (ZP zur ER-Konv 108) [4] geschaffen. Das Zusatzprotokoll enthält Grundsätze bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung. Das Zusatzprotokoll wurde vom Bundesrat am 17. Oktober 2002 unterzeichnet und vom Parlament mit Beschluss vom 24. März 2006 genehmigt. Es ist beabsichtigt, das Zusatzprotokoll per Ende 2007 zu ratifizieren, so dass es auf den 1. April 2008 in Kraft treten kann.

Gleichzeitig mit dem Zusatzprotokoll beantragte der Bundesrat dem Parlament eine Revision des DSG, welche am 24. März 2006 beschlossen wurde.[5] Es ist beabsichtigt, die Revision Mitte 2007 in Kraft zu setzen.

4.2 Die Assoziierung der Besitzstände[6] von Schengen und Dublin (Datenschutz)

4.2.1 Inhalt

Im Rahmen der Schengener und der Dubliner Zusammenarbeit werden zwischen den Behörden der beteiligten Staaten regelmässig Daten über Personen und Sachen ausgetauscht. Im Bereich von Schengen geschieht dies primär im Rahmen des sogenannten Schengener Informationssystems (SIS), einem elektronischen Fahndungssystem für gesuchte oder unerwünschte Personen sowie für gesuchte Gegenstände (Fahrzeuge, Waffen und dergleichen). Im Bereich von Dublin betrifft dies insbesondere die computergestützte zentrale Datenbank Eurodac, in welcher die Fingerabdruckdaten aller Asylbewerber und illegal anwesenden Personen aus Drittländern erfasst werden.

In diesem Zusammenhang stellen sich Fragen des Datenschutzes. Ziel ist es, bei der Verarbeitung persönlicher Daten die Grundrechte und insbesondere die Privatsphäre der Betroffenen durch klare rechtliche Vorgaben zu schützen. Die Schengen/Dublin Zusammenarbeit untersteht einem strengen Datenschutzrecht. Sowohl das Schengener Durchführungsübereinkommen (SDÜ) als auch die Dubliner Verordnung (Dublin II) und die Verordnung zu Eurodac enthalten spezielle Datenschutzvorschriften. Diese regeln den Datentransfer. In weiten Teilen von Schengen/Dublin kommt daneben auch die allgemei-

---

[3] Der Entwurf des Regierungsrates betreffend eines Datenschutzgesetzes vom 18./25. Januar 1994 wurde anschliessend an das Vernehmlassungsverfahren stark gekürzt und in Art. 8 ff. Staatsverwaltungsgesetz vom 8. Juni 1997 (StVG; GDB 130.1) eingegliedert.

[4] Vgl. die Botschaft des Bundesrates in: BBl 2003 2101 ff. sowie den Wortlaut des Zusatzprotokolls in: BBl 2006 3649.

[5] Vgl. die Botschaft des Bundesrates in: BBl 2003 2101 ff. sowie den Gesetzestext in: BBl 2006 3547.

[6] Die zu Schengen oder Dublin gehörenden Rechtsakte und Massnahmen nennt man Schengen–Besitzstand bzw. Dublin–Besitzstand.

ne EU-DSRL[7] zur Anwendung. Mit der Assoziierung an Schengen und Dublin entfalten diese Vorschriften auch für die Schweiz Wirkung.

4.2.2 Schengen-Besitzstand

Im Rahmen von Schengen besteht eine Vielzahl zum Teil sehr detaillierter Datenschutzbestimmungen. Je nach Bereich der Zusammenarbeit sind unterschiedliche Vorschriften zu beachten:

– In den Bereichen, die unter den ersten Pfeiler[8] der EU fallen (Grenzkontrollen, Visa, Feuerwaffen sowie teilweise Betäubungsmittel), kommt die EU-DSRL zur Anwendung.
– In den Bereichen, die unter den dritten Pfeiler der EU fallen (polizeiliche Zusammenarbeit und justizielle Kooperation in Strafsachen), gelten für den Datenaustausch im Rahmen des SIS die Art. 102 – 118 SDÜ und für den Datenaustausch ausserhalb des SIS die Art. 126 – 130 SDÜ.

4.2.3 Dublin-Besitzstand

Der Dublin-Besitzstand regelt den Asylbereich (erster Pfeiler der EU). Der entsprechende Datenschutz in diesem Bereich wird durch die Dublin-Verordnung, die Eurodac-Verordnung sowie die EU–DSRL geregelt.

Die Dublin-Verordnung regelt den Datenaustausch im Asylwesen. Die Datenschutzbestimmungen befassen sich mit folgenden Bereichen :

– Bekanntgabe der Daten;
– Zweck des Datenaustauschs;
– Grundsatz der Richtigkeit der Daten;
– Auskunftsrecht der betroffenen Personen;
– Recht auf Berichtigung, Löschung und Sperrung;
– Protokollierung des Datenaustauschs;
– Aufbewahrungsdauer der Daten.

Die Eurodac-Verordnung enthält spezifische Datenschutzregelungen betreffend die Fingerabdruckabnahme. Neben dem eigentlichen Fingerabdruck werden in Eurodac mithin nur diejenigen Daten gespeichert, die für die Identifikation absolut notwendig sind. Die Datenschutzbestimmungen der Eurodac-Verordnung regeln insbesondere:

– Grundsatz der Fingerabdruckabnahme;
– Einrichtung der zentralen Datenbank Eurodac, zur Speicherung und zum Vergleich der Fingerabdrücke;
– Katalog der an Eurodac zu übermittelnden Daten;
– Zugriff auf die Daten;
– Aufbewahrung und Löschung der Daten;
– dazugehörige Sicherheitsvorschriften

---

[7] Richtlinie 95/46 EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (EU-DSRL).

[8] Die EU besteht seit dem Vertrag von Maastricht aus drei Pfeilern: Der erste Pfeiler bildet die EG (Vertrag zur Gründung der Europäischen Gemeinschaft, EGV), der zweite Pfeiler enthält die Bestimmungen zur gemeinsamen Aussen- und Sicherheitspolitik (Art. 11–28 des Vertrags über die Europäische Union, EUV) und der dritte Pfeiler umfasst die polizeiliche und justizielle Zusammenarbeit in Strafsachen (Art. 29–42 EUV). Die Bereiche Grenzkontrollen, Visa, Feuerwaffen sowie teilweise Betäubungsmittel wurden dem ersten Pfeiler der EU zugeordnet; diese Bereiche gehören mithin zum eigentlichen Gemeinschaftsrecht. Die polizeiliche Kooperation und die justizielle Zusammenarbeit in Strafsachen fallen hingegen unter den dritten Pfeiler der EU (BBl 2004 6067 f.).

Neben diesen datenschutzrechtlichen Regelungen wird auf die EU-DSRL verwiesen.

4.2.4 Die EU-DSRL im Speziellen

Die Datenschutzrichtlinie regelt ganz allgemein den Datenschutz im Bereich des Gemeinschaftsrechts und der Schengener Zusammenarbeit. Die Datenschutzrichtlinie bezieht sich auf die Verarbeitung aller personenbezogenen Daten in ihrem Anwendungsbereich. Sie konkretisieret und erweitert die in der ER-Konv 108 enthaltenen Grundsätze.

Inhaltlich zielt die Datenschutzrichtlinie darauf ab, die Hindernisse für den freien Datenverkehr aus dem Weg zu räumen, ohne den Schutz von personenbezogenen Daten zu beeinträchtigen. In diesem Zusammenhang regelt sie Folgendes:

– Qualität der Daten (Art. 6);
– Zulässigkeit der Verarbeitung von Daten (Art. 7);
– besondere Kategorien der Verarbeitung (Art. 8 f.);
– Information der von der Datenverarbeitung betroffenen Personen (Art. 10 f.);
– Auskunftsrecht der betroffenen Personen und Ausnahmen (Art. 12 f.);
– Widerspruchsrecht/Automatisierte Einzelentscheidungen (Art. 14 f.);
– Vertraulichkeit und Sicherheit der Verarbeitung (Art. 16 f.);
– Meldepflicht der Verarbeitungen, Vorabkontrolle, Register (Art. 18 ff.);
– Rechtsmittel, Haftung, Sanktionen (Art. 22 ff.);
– Transfer von Personendaten aus einem Mitgliedstaat in ein Drittland (Art. 25 f.);
– Behörden (Kontrollstellen, Datenschutzgruppe, Kommission; Art. 28 ff.).

4.3 ER-Konv 108 und Zusatzprotokoll

4.3.1 ER-Konv 108

Zweck des Übereinkommens ist es, im privaten und im öffentlichen Sektor den Rechtsschutz des Einzelnen gegenüber der automatischen Verarbeitung der ihn betreffenden personenbezogenen Daten zu verstärken. In allen Mitgliedstaaten soll ein Minimum an Persönlichkeitsschutz bei der Verarbeitung von Personendaten und eine gewisse Harmonisierung des Schutzsystems sichergestellt werden. Andererseits gewährleistet das Übereinkommen den internationalen Datenverkehr dadurch, dass keine Vertragspartei den Transfer von Informationen an eine andere Vertragspartei, welche den vom Übereinkommen vorgesehen Mindestschutz gewährleistet, untersagen darf.

Das Abkommen regelt konkret Folgendes:

– Qualität der Daten (Art. 5);
– besondere Arten von Daten (Art. 6);
– Datensicherung (Art. 7);
– zusätzlicher Schutz für den Betroffenen (Art. 8);
– Ausnahmen und Einschränkungen (Art. 9);
– Sanktionen und Rechtsmittel (Art. 10);
– weitergehender Schutz (Art. 11);
– grenzüberschreitender Verkehr personenbezogener Daten (Art. 12).

Die Grundsätze des Übereinkommens wurden von der EU-DSRL übernommen und konkretisiert (BBl 2003 2113 ff.).

Das Übereinkommen vervollständigt und konkretisiert im Bereich der automatisierten Bearbeitung von Personendaten die Art. 8 (Recht auf Privatsphäre) und 10 (Meinungsäusserungsfreiheit) der Konvention vom 4. November 1950 zum Schutze der Menschenrechte und Grundfreiheiten (EMRK). Das eidgenössische Recht genügt bereits heute den Anforderungen der ER-Konv 108.

Das Ministerkomitee hat mehrere Empfehlungen im Datenschutzbereich angenommen. Diese sehen generell vor, dass, wer Personendaten erhebt, die Betroffenen angemessen zu informieren hat. Die Revision des DSG hat diese Empfehlungen aufgenommen – auch aufgrund der parlamentarischen Motion „Erhöhte Transparenz“ (2000 M 00.3000) – und eine detaillierte Informationspflicht für die Erhebung von besonders schützenswerten Daten und Persönlichkeitsprofilen sowie einer weniger weit gehenden Informationspflicht (vgl. Erkennbarkeit der Datenbearbeitung) für die übrigen Datenkategorien eingeführt (BBl 2003 2113).

4.3.2 Zusatzprotokoll zur ER-Konv 108

Das Zusatzprotokoll ergänzt die ER-Konv 108 und soll die Umsetzung der darin enthaltenen Grundsätze verbessern in Bezug auf zwei Aspekte:

– Harmonisierung der Zuständigkeiten der Kontrollbehörden;
– Vermeidung der Umgehung der Gesetzgebung eines Vertragsstaates durch Datentransfers in Drittstaaten oder an Drittorganisationen.

Als Massnahmen sieht das Zusatzprotokoll Folgendes vor:

– Einsetzung von Kontrollbehörden, die Untersuchungsbefugnisse und Klagerechte besitzen, zur Durchsetzung der im Übereinkommen stipulierten Grundsätze (Art. 1).
– Transfer von personenbezogenen Daten an einen Datenempfänger, der vom Übereinkommen nicht erfasst ist, nur dann, wenn der Empfängerstaat oder die Empfängerorganisation ein angemessenes Schutzniveau garantiert, z.B. mit entsprechend ausgestalteten Vertragsklauseln (Art. 2).

Die vom Zusatzprotokoll vorgesehenen Anforderungen bezüglich der Aufsichtsbehörden und des grenzüberschreitenden Datenverkehrs sind jenen der EU-DSRL sehr ähnlich.

4.4 Revision des DSG[9]

Auslöser der Revision waren:

– zwei im Jahre 1999 bzw. 2000 von den Eidgenössischen Räten angenommene Motionen zum Datenschutz;[10]
– der Beitritt der Schweiz zum Zusatzprotokoll der ER-Konv 108.

Die Revisionsarbeiten waren vom Bemühen getragen, den Persönlichkeitsschutz zu verstärken und Transparenz bei der Bearbeitung von Personendaten herbeizuführen, ohne indessen die Tätigkeiten der Inhaber der Datensammlungen unnötig zu erschweren.

Die Änderungen des DSG vom 24. März 2006 bezwecken in erster Linie die (eingehendere) Regelung folgender, hier relevanter Bereiche:

– Generell: Annäherung des schweizerischen Rechts an das Recht der Europäischen Union;[11]
– Beschaffung und Bekanntgabe von Personendaten;
– Information und Rechte der Personen, deren Daten bearbeitet werden;
– Verantwortlichkeiten und Kontrolle bei der Delegation der Bearbeitung an Dritte;

---

[9] Vgl. BBl 2003 2101 ff.

[10] 2000 M 00.3000 (Erhöhte Transparenz bei der Erhebung von Personendaten [S 7.3. 00, Kommission für Rechtsfragen; SR 99.067; N 5.10.00]) und 1999 M 98.3529 (Erhöhter Schutz für Personendaten bei Online-Verbindungen [S 16.3. 99, Geschäftsprüfungskommission SR; N 21.12.99]): Die Motionen verlangen einerseits eine Verstärkung der Transparenz beim Beschaffen von Daten und andererseits eine formelle gesetzliche Grundlage für Online-Verbindungen zu Datenbanken des Bundes sowie einen Mindestschutz bei der Bearbeitung von Daten durch die Kantone beim Vollzug von Bundesrecht.

[11] Vgl. Zusammenhang Revision DSG/Assoziierungsabkommen: BBl 2003 2110 und 2004 6175.

- Kontrolle der Einhaltung des Datenschutzes;
- Festlegung eines minimalen Schutzstandards bei der Verarbeitung von Daten durch kantonale Behörden beim Vollzug von Bundesrecht.

5. Regelungsnotwendigkeit und Regelungsbedarf

5.1 Regelungsnotwendigkeit

Im internationalen Bereich werden die Kantone durch vom Bund abgeschlossene Staatsverträge auch in ihren eigenen Kompetenzbereichen verpflichtet. Jeder Kanton muss allerdings selber für die nötigen Datenschutzregelungen sorgen, da dem Bund mangels einer verfassungsrechtlichen Kompetenz keine Regelungsbefugnis für das Datenbearbeiten durch kantonale und kommunale Organe zukommt.

Die Regelungsnotwendigkeit ergibt sich aus folgenden Gründen:

- Beitritt der Schweiz zur ER-Konv 108 (inkl. Zusatzprotokoll)
- Assoziierung der Besitzstände von Schengen und Dublin durch die Schweiz;
- Revision des DSG (insbesondere Art. 37 Abs. 1);
- Projekt ZRK betreffend eines gemeinsamen Datenschutzorgans.

Ein darüber hinausgehender Regelungsbedarf besteht aus kantonaler Sicht nicht.

5.2 Regelungsbedarf aufgrund des internationalen Rechts[12]

Der Beitritt der Schweiz zur ER-Konv 108 und zum ZP wie auch eine Teilnahme an Schengen/Dublin hat sowohl rechtliche als auch faktische Auswirkungen auf die Kantone.

Insbesondere die Besitzstände von Schengen und Dublin kennen einen hohen, rechtlich verbindlichen Datenschutzstandard. Die zum Teil sehr detaillierten Datenschutzregelungen müssen im kantonalen Kompetenzbereich auch von unseren Behörden angewendet werden, wobei die Einhaltung der Datenschutzvorschriften zwingend durch eine (unabhängige) kantonale Behörde zu kontrollieren ist.

Aufgrund der neuen Ausgangslage im Kanton Obwalden – ungenügende und lückenhafte Datenschutzgesetzgebung – besteht ein erheblicher kantonaler Umsetzungsbedarf.

Jede Bearbeitung von Personendaten im kantonalen Bereich, bei:

- der nicht spezifische Vorschriften der Besitzstände von Schengen oder Dublin zur Anwendung gelangen[13] ;
- bei dem die kantonalen Behörden nicht im Rahmen des Vollzugs von Bundesrecht tätig werden (vgl. nachstehend Kap. 4.3)

hat folgenden Datenschutzstandard einzuhalten:

- ER-Konv 108;
- ZP zur ER-Konv 108.
- Grundsätze der Empfehlung des Ministerkomitees des Europarats vom 17. September 1987 über die Nutzung personenbezogener Daten im Polizeibereich (Europaratsempfehlung R [87] 15);
- EU-DSRL.

---

[12] Zum Ganzen: BBl 2003 2148, 2004 6089, 6098, 6176 f., 6181 ff.

[13] Z.B. Bei der Bearbeitung von Personendaten im Rahmen der polizeilichen Zusammenarbeit (dritter Pfeiler der EU), gelangen primär die Art. 102 – 118 SDÜ und Art. 126 – 130 zur Anwendung. Soweit die Bestimmungen des SDÜ den Datenschutz in den Bereichen des SIS und der allgemeinen Polizeizusammenarbeit nicht abschliessend regeln, sind die Datenschutzbestimmungen des nationalen Rechts anwendbar, die einem definierten Mindeststandard entsprechen müssen (Art. 117 Abs. 1, 126 Abs. 1 und 129 SDÜ).

Das kantonale Recht ist deshalb an die europäischen Grundlagen anzupassen.

5.3 Regelungsbedarf aufgrund des DSG

Früher fand das Bundesrecht anstelle des kantonalen Rechts nur Anwendung, wenn im kantonalen Recht keine eigenen Datenschutzbestimmungen bestanden. Der neue Art. 37 Abs. 1 DSG geht weiter und legt ergänzend einen Mindestschutzstandard fest. Das DSG findet somit künftig nicht nur dann Anwendung, wenn kantonale Datenschutzvorschriften beim Vollzug von Bundesrecht fehlen, sondern auch, wenn diese kantonalen Bestimmungen kein angemessenes Schutzniveau gewährleisten.

Unter einem "angemessenen Schutzniveau" versteht man die Einhaltung folgender Standards:

– ER-Konv 108 sowie ZP;
– Standards im Rahmen der Schengener und der Dubliner Zusammenarbeit.

Die Sicherheit eines Informatiksystems und der Schutz der darin enthaltenen Daten wird durch das schwächste Glied der Kette bestimmt. Das Niveau des Datenschutzes variiert heute von einem Kanton zum anderen erheblich (BBl 2003 2146 f., 2148).

5.4 Regelungsbedarf auf kommunaler Ebene

Freilich gelten die europäischen Datenschutzstandards auch auf kommunaler Ebene. Da jedoch die meisten Anwendungsfälle das kantonale Recht betreffen, besteht auf kommunaler Ebene kein Regelungsbedarf, zumal der Geltungsbereich des kantonalen Datenschutzrechts – wie bisher – alle Ebenen des Kantons einbezieht. Die Gemeinden bleiben dadurch auch von nachfolgenden Änderungen des eidgenössischen oder internationalen Rechts verschont.

Unter Umständen kann sich ein kommunaler Regelungsbedarf bei der Schaffung einer Datenschutzstelle auf Gemeindeebene ergeben (Art. 33).

5.5 Wegleitung der KdK[14] zur Umsetzung Schengen/Dublin in den Kantonen

In Absprache mit der Konferenz der kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) und gestützt auf einen Zirkulationsbeschluss des leitenden Ausschusses der Konferenz der Kantone (KdK) wurde ein externer Experte (Verfasser Dr. Beat Rudin, Lehrbeauftragter an der Universität Basel) damit beauftragt, zuhanden der Kantone eine Wegleitung zur Umsetzung der mit Schengen und Dublin übernommenen Datenschutzvorschriften auszuarbeiten.

Namentlich nennt die Wegleitung den kantonalrechtlichen Mindeststandard. Mit diesem Hilfsmittel sollen die Kantone die Vollständigkeit ihrer Datenschutzgesetzgebung überprüfen und den noch bestehenden Handlungsbedarf im Hinblick auf das geforderte Schutzniveau feststellen können.

Vorliegend diente die Wegleitung als Grundlage für den Entwurf eines Datenschutzgesetzes.

6. Konzept des kantonalen Gesetzesentwurfs

6.1 Gesetzestechnisch

Ein Erlass muss dem Gesetzmässigkeitsprinzip entsprechen. Weiter muss er adressatengerecht sein. Wesentlich ist dabei die Praktikabilität und Verständlichkeit, was wiederum von der Systematik und der Sprache abhängt. Die staatliche Regelung soll widerspruchsfrei und in sich inhärent sein. Schliesslich soll sie vollzugtauglich und wirksam

[14] Konferenz der Kantonsregierungen.

sein.

6.1.1 Erfordernis der formell-gesetzlichen Regelung

Aus Gründen der Rechtsicherheit ist eine Regelung auf (formell-)gesetzlicher Stufe erforderlich.

Nach der bundesgerichtlichen Praxis gelten als Gesetze im formellen Sinn vorab die einem obligatorischen oder fakultativen Referendum unterworfenen kantonalen Erlasse. Doch können auch vom Parlament allein beschlossene Erlasse die Funktion des formellen Gesetzes erfüllen, wenn die kantonale Verfassung selber für die betreffende Materie die abschliessende Zuständigkeit des Parlaments vorsieht oder aber Raum dafür lässt, dass der Gesetzgeber die betreffende Rechtsetzungskompetenz an das Parlament delegiert (BGE 132 I 157 Erw. 2.2).

Nach Art. 60 der Kantonsverfassung vom 19. Mai 1968 (KV; GDB 101) sind diejenigen generellen Bestimmungen in Form des Gesetzes zu kleiden, die Rechte und Pflichten der natürlichen und juristischen Personen sowie die Organisation von Kanton und Gemeinden allgemein gültig festlegen. Ein Gesetz im formellen Sinn wird vom Kantonsrat erlassen und unterliegt im Kanton dem fakultativen Referendum (Art. 59 Abs. 1 Bst. a KV). Keine Gesetze im formellen Sinn sind die Verordnungen.

Demnach ist vorliegend die Form des "Gesetzes" im Sinne von Art. 60 KV zu wählen, um den datenschutzrechtlichen Anpassungsbedarf gesetzgeberisch umzusetzen.

(Wo im Entwurf der Begriff "Gesetz" verwendet wird, ist ein Gesetz im formellen Sinne gemeint, wo der Entwurf lediglich von "Gesetzgebung" spricht, kann formell auch eine tiefere Gesetzesstufe möglich sein.)

6.1.2 Systematische und inhaltliche Eingliederung ins kantonale Recht

Das heute geltende Datenschutzrecht des Kantons Obwalden ist primär in Art. 8 – 14 StVG geregelt.

Eine blosse Ergänzung des StVG ist nicht möglich; der Umfang des Anpassungsbedarfes würde den Rahmen des StVG sprengen. Daher ist ein eigenständiges Datenschutzgesetz zu schaffen, das ausschliesslich und abschliessend die datenschutzrechtliche Materie regelt.

6.1.3 Ausführungsbestimmungen

Im Rahmen des Datenschutzgesetzes soll der Regierungsrat die Kompetenz erhalten, auf dem Weg der Ausführungsbestimmungen bestimmte Bereiche näher zu regeln.

Damit kann insbesondere dem sich entwickelnden Bedürfnis der Bevölkerung nach Transparenz, Einsicht und Auskunft im Zusammenhang mit Datenbearbeitungen durch öffentliche Organe organisatorisch und administrativ Rechnung getragen werden.

6.1.4 Gesetzliche Grundlage einer Auslagerung der Datenschutzaufgaben

Mit der Assoziierung der Besitzstände von Schengen und Dublin ist die behördliche Datenbearbeitung durch eine unabhängige Stelle zu kontrollieren; jeder Kanton muss eine Datenschutzstelle vorsehen.

Die Form der Datenschutzstelle ist nicht vorgeschrieben. Die rechtlichen Vorgaben verlangen aber eine Stelle, die ihre Aufgabe "in völliger Unabhängigkeit" wahrnehmen kann. Weiter verlangen die rechtlichen Vorgaben eine wirksame aktive Kontrolle. Dies bedingt, dass die Datenschutzstelle:

– die nötigen Befugnisse besitzt;
– die erforderlichen personellen und finanziellen Ressourcen zugeteilt erhält;
– die hohen fachlichen Anforderungen erfüllt.

In Bezug auf die Sicherstellung der letzten beiden Anforderungen hat die Zentralschweizerische Regierungskonferenz (ZRK) den Anstoss zu einem Zusammenarbeitsprojekt betreffend einer gemeinsamen, unabhängigen Datenschutzstelle gegeben (der Kanton Luzern nimmt nicht am Projekt teil).

Die Leistung der gemeinsamen Datenschutzstelle soll durch Abschluss einer Verwaltungsvereinbarung eingekauft werden, ohne rechtsetzendes Konkordat. Damit soll eine Teilung der notwendigen Ressourcen bezweckt und die fachlichen Anforderungen auf eine Stelle konzentriert werden. Ausserdem würde mit einem vollen Pensum die Frage der Zulässigkeit einer Nebenerwerbstätigkeit (Unabhängigkeit) nicht aktuell. Im Vergleich zu einer kantonalen Datenschutzaufsicht sind allerdings eine geringere Nähe zu den Bürgern und Verwaltungen sowie grössere Reisewege in Kauf zu nehmen.

Eine entsprechende Vereinbarung betreffend der Auslagerung einer hoheitlichen Aufgabe setzt innerkantonal voraus, dass:[15]

– eine Auslagerung rechtlich zulässig ist;
– eine genügende gesetzliche Grundlage besteht;
– die Auslagerung dem öffentlichen Interesse entspricht;
– die Auslagerung verhältnismässig ist.

Die Frage, ob eine Auslagerung, insbesondere mit Blick auf die geforderte völlige institutionelle Unabhängigkeit rechtlich zulässig ist, kann noch nicht abschliessend beantwortet werden; sie ist im Augenblick Gegenstand der Abklärungen im Rahmen des Zusammenarbeitsprojekts. Voraussichtlich übernimmt die Datenschutzstelle des Kantons Zug die Aufgabe der zentralschweizerischen Datenschutzstelle.

Jedenfalls aber sieht der hier diskutierte Entwurf vorsorglich eine entsprechende gesetzliche Grundlage vor, die den Regierungsrat ermächtigt, die Zusammenarbeit mit anderen Kantonen mittels Vereinbarung zu regeln.

6.2. Inhaltlich

Vorbemerkung: Die Regelungsnotwendigkeit sowie der Regelungsbedarf, der sich aus dem übergeordneten nationalen und internationalen Recht ergibt, wird jeweils eingangs der Erläuterung eines einzelnen Artikels mit Hinweis auf die massgebenden Gesetzesbestimmungen angegeben.

6.2.1. Primäre Anlehnung an das DSG und die Wegleitung der KdK

Der vorliegende Entwurf lehnt sich systematisch wie auch inhaltlich primär an das revidierte eidgenössische Datenschutzgesetz an, freilich nur für den Bereich der öffentlichen Organe.

Gründe dafür sind:

– die Umsetzung des europäischen Minimalstandards ist im eidgenössischen Datenschutzgesetz grossmehrheitlich bereits erfolgt;
– das DSG findet ohnehin für die Kantone Anwendung, wenn kantonale Datenschutzvorschriften beim Vollzug von Bundesrecht kein angemessenes Schutzniveau gewährleisten (Mindestschutzstandard; Art. 37 Abs. 1 DSG);
– die Gesetzgebung zwischen Bund und Kanton ist kohärent (Auslegung, Definitionen, nachfolgender Anpassungsbedarf etc.);
– fehlende Übereinstimmen der zentralschweizerischen Datenschutzgesetzgebungen im konkreten Wortlaut wie auch teilweise in der Systematik.

Für die Festlegung des Minimalstandards wurde auch auf die Wegleitung der KdK abgestellt.

---

[15] Vgl. die von der ZRK zur Verfügung gestellte "Mustervereinbarung interkantonaler Zusammenarbeit mittels Kauf von Leistungen bei einer externen Stelle".

6.2.2 Weitere Einflüsse

Wo die Bundeslösung für den kantonalen Entwurf keinen befriedigenden Weg aufzeigen konnte, was zahlreich vorkam, wurden eigenständige Lösungen für den Kanton Obwalden entworfen.

Dabei wurden mitberücksichtigt:

– die geltenden Datenschutzbestimmungen des StVG;
– die geltenden oder im Entwurf bestehenden zentralschweizerischen Datenschutzgesetzgebungen, soweit eine gewisse zentralschweizerische Homogenität erkennbar war. Dies war vor allem dann der Fall wenn, wenn es um den Geltungsbereich, die zu regelnde Materie oder um die Systematik. Im konkreten Wortlaut aber weisen die fünf zentralschweizerischen Datenschutzgesetzgebungen völlig unterschiedliche Lösungen auf.

7. Vernehmlassungsverfahren

...

8. Erläuterungen zu den einzelnen Artikeln des Datenschutzgesetzes

8.1 Zweck, Geltungsbereich und Begriffe

Art. 1 *Zweck*

Der erste Artikel des Entwurfs verweist auf die Bezugspunkte und Quellen allen Datenschutzrechts. Es sind dies die Grundrechte und insbesondere der Persönlichkeitsschutz (vgl. Art. 13 Abs. 2 BV; Art. 10 KV), welche bei der Datenbearbeitung durch staatliche Behörden zu beachten sind. Zweck des Erlasses ist es, die Gewährleistung dieser Rechtsgüter im Zusammenhang mit der Informationsbearbeitung verbindlich zu regeln. Der Zweckartikel soll auch als Leitlinie für die Auslegung der einzelnen Datenschutzbestimmungen dienen.

Art. 2 *Geltungsbereich*

(Art. 2 Abs. 1 DSG
Art. 2 Abs. 2 Bst. a und c DSG
Art. 23 Abs. 1 DSG
Art. 3 ER-Konv 108
Art. 3 f. EU-DSRL)

Abs. 1: Der Geltungsbereich des Erlasses soll sich grundsätzlich auf jedes Bearbeiten von Personendaten in öffentlich-rechtlichen Körperschaften und Anstalten auf kantonaler und kommunaler Ebene beziehen. Auf die Bearbeitung von Personendaten durch private Personen ist das eidgenössische Datenschutzgesetz anwendbar.

Abs. 2: Das übergeordnete Recht lässt verschiedene Ausnahmen zu:

– Bst. a: Es ist zulässig, eine Ausnahme für privatrechtlich handelnde Organe des öffentlichen Rechts (wie z.B. die Obwaldner Kantonalbank) vorzusehen. In einem solchen Fall gelangt das Bundesdatenschutzgesetz zur Anwendung.
– Bst. b: Es ist zulässig, eine Ausnahme für hängige Verfahren der Zivil- und Strafrechtspflege vorzusehen, da die dadurch zur Anwendung gelangenden Zivil- und Strafprozessordnungen ihrerseits die nötigen Regelungen (insb. zur Beschaffung und Bekanntgabe von Personendaten sowie zu den Rechten der betroffenen Personen und zur Aufsicht) enthalten.
– Bst. c: Gleiches ist zulässig – unter den Voraussetzungen von Bst. b – für hängige Verfahren der Verfassungs- und Verwaltungsgerichtsbarkeit. Jedoch ist es unzulässig, das erstinstanzliche Verwaltungsverfahren sowie das verwaltungsinterne Rechtsmittelverfahren im Sinne von Art. 67 Abs. 1 StVG aus dem Geltungsbereich auszunehmen.

- Bst. d: Ausgenommen vom Geltungsbereich des Datenschutzgesetzes sind auch die Geschäfte des Kantonsrats (inkl. Kommissionen). Dieser könnte seine verfassungsrechtlich vorgesehene Oberaufsicht über die Staatsverwaltung und Rechtspflege (Art. 70 Ziff. 3 KV) nicht richtig wahrnehmen, wenn er in jedem Fall die Datenschutzgrundsätze, insbesondere die Bestimmung über die Weitergabe von Personendaten, beachten müsste. Die übrigen kommunalen und kantonalen Wahl- und Abstimmungsgeschäfte unterstehen dem Datenschutzrecht; immerhin können sich die öffentlichen Organe dabei auf Art. 17 Abs. 2 stützen.
- Bst. e: Ähnliche Überlegungen wie bei den Gesetzesvorschriften über die hängigen Rechtsprechungsverfahren haben auch zu einer Ausnahmeklausel für die öffentlichen Register des privatrechtlichen Rechtverkehrs geführt. Zu diesen Registern gehören u.a. das Grundbuch, das Zivilstandsregister, das Handelsregister und die Register für Schuldbetreibung und Konkurs. Diese Register stellen im Grunde genommen staatlich getragene und gesicherte "Informationssysteme" dar, die bestimmte Angaben über die Begründung, den Bestand, die Änderung oder die Ausübung von privaten Rechten enthalten. Die Datenbearbeitung im Rahmen dieser Register läuft meist nach sehr detaillierten und formellen Vorschriften ab. Diese sollen und können nicht durch das Datenschutzgesetz modifiziert werden.
- Bst. f: Die gesetzlichen Pflichten, die beim Umgang mit Personendaten zu beachten sind, wie auch die Rechte der betroffenen Personen müssen eine Grenze finden, wo Daten ausschliesslich zum persönlichen Gebrauch bearbeitet werden. Nicht unter das Gesetz fallen somit Notizen, die als Gedankenstützen oder Arbeitshilfen ausschliesslich zum persönlichen Gebrauch erstellt werden. Sobald aber solche Teil der offiziellen Verfahrensakten bilden, sie also Grundlage einer Entscheidung bilden, unterstehen sie dem Geltungsbereich dieses Gesetzes (vgl. BGE 121 I 227 [Akteneinsicht]). Ebenso wenig handelt es sich um ein persönliches Arbeitsmittel, wenn die Daten innerhalb der Verwaltung z.B. der Stellvertretung, der Nachfolge oder der übergeordneten Stelle weiter gegeben werden.

Abs. 3: Vorbehalten bleiben Sonderreglungen des kantonalen Rechts, die den Datenschutz für einen konkreten Bereich regeln. Es sind dies insbesondere:

- Archivierung der Gerichtsakten;
- Patientenrechte;
- Einwohnerkontrolle.

Art. 3 *Begriffe*

(Art. 3 Bst. c DSG
Art. 6 ER-Konv 108
Art. 8 Abs. 1 EU-DSRL)

Voraussetzung für den Schutz von Personendaten, insbesondere schützenswerter (sensitiver, besonderer) Daten ist eine Begriffsdefinition. Es versteht sich von selbst, dass diese in Übereinstimmung mit den Begriffsbestimmungen des übergeordneten Rechts zu definieren ist.

Die im vorliegenden Entwurf verwendeten Begriffe stehen – mit Ausnahme des Begriffs der "öffentlichen Organe", der je nach rechtstaatlicher Struktur eines Kantones massgeblich den Geltungsbereich bestimmt – im Einklang mit den Definitionen des CH-DSG. Es ist daher sinnvollerweise auf diese zu verweisen.

Datenschutzerlasse anderer Kantone haben die Begriffsdefinitionen des DSG-CH mit mehr oder weniger grossen Abänderungen wörtlich übernommen.

8.2 Bearbeiten von Personendaten

8.2.1 Allgemeine Bestimmungen

Art. 4 *Grundsätze*

(Art. 4 i.V.m. Art. 37 Abs. 1 DSG
Art. 5 Bst. a - c ER-Konv 108
Art. 6 Abs. 1 Bst. a - c EU-DSRL)

Abs. 1: Das Bearbeiten von Personendaten muss rechtmässig sein. Bezüglich des behördlichen Datenbearbeitens heisst das insbesondere, dass Daten nur gestützt auf eine Rechtsgrundlage bearbeitet werden dürfen. Eine solche Rechtsgrundlage kann als ausdrückliche Verpflichtung oder Ermächtigung zu einer bestimmten Datenbearbeitung vorliegen oder als gesetzliche Aufgabe, zu deren Erfüllung bestimmte Datenbearbeitungen erforderlich sind.

Der Grundsatz der rechtmässigen Bearbeitung wird konkretisiert insbesondere in:
– Art. 7 Rechtsgrundlage
– Art. 8 Datenbearbeitung durch Dritte
– Art. 17 Datenbekanntgabe im Allgemeinen
– Art. 19 Abrufverfahren
– Art. 20 Automatisierte Informations- und Kommunikationsdienste
– Art. 22 Bearbeitung für nicht personenbezogene Zwecke
– Art. 23 Überwachungsgeräte
– Art. 24 Abs. 4 Bst. b Register der Datensammlungen
– Art. 25 Abs. 2 Bst. b Auskunftsrecht

Abs. 2: Das Bearbeiten von Personendaten muss nach Treu und Glauben erfolgen. Ausfluss dieses Grundsatzes ist insbesondere das Verbot der verdeckten Datenerhebung. Deshalb ist minimal festzuschreiben, dass Personendaten, wenn immer möglich, bei der betroffenen Person zu erheben sind, und dass die Beschaffung und der Zweck der Bearbeitung für die betroffene Person erkennbar sein müssen.

Der Grundsatz der Bearbeitung von Personendaten nach Treu und Glauben wird konkretisiert insbesondere in:
– Art. 13 Datenquellen
– Art. 14 Erkennbarkeit der Beschaffung
– Art. 15 Informationspflicht bei systematischen Erhebungen
– Art. 16 Informationspflicht bei besonders schützenswerten Personendaten und Persönlichkeitsprofilen
– Art. 23 Abs. 1 Bst. a Überwachungsgeräte

Abs. 3: Die Zweckbindung (oder das Zweckänderungsverbot) ist eines der Kernelemente des Datenschutzrechts. Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich ist oder gesetzlich vorgesehen ist, wobei im öffentlich-rechtlichen Bereich die Zweckbestimmung durch das Gesetz im Vordergrund steht.

Der Grundsatz der Zweckbindung wird konkretisiert insbesondere in:
– Art. 11 Archivieren und Vernichten
– Art. 15 Informationspflicht bei systematischen Erhebungen
– Art. 16 Abs. 2 Bst. b Informationspflicht bei besonders schützenswerten Personendaten und Persönlichkeitsprofilen
– Art. 20 Abs. 2 Automatisierte Informations- und Kommunikationsdienste
– Art. 22 Bearbeitung für nicht personenbezogene Zwecke
– Art. 25 Abs. 2 Bst. b Auskunftsrecht

Abs. 4: Das Bearbeiten von Personendaten muss – wie jedes behördliche Handeln – verhältnismässig sein. Dies ist unter folgenden Voraussetzungen der Fall:

– die bearbeiteten Daten müssen zur Zweckerreichung geeignet sein;
– die Datenbearbeitung muss das mildeste Mittel sein, mit welchem der Zweck erreicht werden kann;
– Zweck (Aufgabe) und Eingriff (Datenbearbeitung) in die informationelle Selbstbestimmung (Art. 13 BV) müssen in einem vernünftigen Verhältnis zueinander stehen (Verhältnismässigkeit i.e.S.).

Der Grundsatz der Verhältnismässigkeit wird konkretisiert insbesondere in:

– Art. 12 Archivieren und Vernichten
– Art. 17 Abs. 1 Bst. a und Abs. 2 Bst. b Datenbekanntgabe im Allgemeinen
– Art. Art. 18 Bekanntgabe ins Ausland
– Art. 20 Abs. 2 Automatisierte Informations- und Kommunikationsdienste
– Art. 21 Bst. a Ablehnung der Bekanntgabe
– Art. 23 Abs. 1 Bst. b Überwachungsgeräte
– Art. 26 Abs. 1 Einschränkung des Auskunftsrechts
– Art. 27 Abs. 2 Sperrung der Bekanntgabe

Art. 5 *Einwilligung*

(Art. 4 Abs. 5 i.V.m. Art. 37 Abs. 1 DSG
Art. 7 Bst. a und Art. 8 Abs. 2 Bst. a EU-DSRL)

Hier geht es um die Voraussetzungen, unter denen die Einwilligung einer betroffenen Person gültig ist (z.B. im Fall von Art. 7 Abs. 2 lit. c). Es geht somit nicht darum, die Einwilligung zur Bedingung für jede Datenbearbeitung zu erheben.

Die betroffene Person muss über alle Informationen im konkreten Fall verfügen, die erforderlich sind, damit sie eine freie Entscheidung treffen kann. Der Begriff "freiwillig" entspricht im Übrigen auch der im Gemeinschaftsrecht verwendeten Terminologie. Das bedeutet insbesondere, dass die betroffene Person über mögliche negative Folgen oder Nachteile informiert sein muss, die sich aus der Verweigerung ihrer Zustimmung ergeben können. Die alleinige Tatsache, dass eine Verweigerung einen Nachteil für die betroffene Person nach sich zieht, kann dagegen die Gültigkeit der Zustimmung nicht beeinträchtigen.

Beispielsweise erteilt ein Mitarbeiter die Einwilligung nicht freiwillig, der gezwungen ist, einer nicht im Arbeitsvertrag vorgesehenen Datenbearbeitung zuzustimmen, weil ihm die Entlassung angedroht wird.

Die Einwilligung ist nicht an eine bestimmte Form gebunden und kann stillschweigend bzw. durch konkludentes Handeln erfolgen, sofern es nicht um die Bearbeitung von besonders schützenswerten Daten oder Persönlichkeitsprofilen geht.

Art. 6 *Vorabkontrolle*

(Art. 31 Abs. 1 Bst. b i.V.m. Art. 37 Abs. 1 DSG
Art. 20 EU-DSRL)

Wenn Bearbeitungen von Personendaten aufgrund der Art der Bearbeitung oder der zu bearbeitenden Daten besondere Risiken für die Rechte und Freiheit der betroffenen Personen mit sich bringen können, müssen sie vor ihrem Beginn durch das Kontrollorgan geprüft werden. Kriterien für die Beurteilung der Risiken sind etwa die Zahl der erfassten Personen, die Zahl der beteiligten öffentlichen Organe, die Sensitivität der Daten usw.. Objekt der Vorabkontrolle können insbesondere Projekte für IT-Systeme, für Datenbanken, für Register sein.

Art. 6 statuiert den Grundsatz der Vorabkontrolle sowie die Pflicht der öffentlichen Organe, heikle Bearbeitungen durch die beauftragte Person für Datenschutz prüfen zu lassen. Die Vorabkontrolle als eine Aufgabe der beauftragten Person für Datenschutz ist in Art. 31 Abs. 3 Bst. b des Entwurfs geregelt.

Art. 7 *Rechtsgrundlage*

(Art. 17 i.V.m. Art. 37 Abs. 1 DSG
Art. 5 Bst. a und b ER-Konv 108
Art. 6 Abs. 1 Bst. a Art. 8 Abs. 4 EU-DSRL)

Abs. 1: Die Datenbearbeitung durch öffentliche Organe bedarf wie jedes Verwaltungshandeln einer gesetzlichen Grundlage; dies ist ein Ausfluss des Grundsatzes der rechtmässigen Bearbeitung von Personendaten. Dies gilt für alle Formen und Phasen der Informationsbearbeitung, sofern das Gesetz nicht ausdrücklich eine Ausnahme vorsieht. Als gesetzliche Grundlage kommen alle Erlassformen infrage; mithin kann es sich auch um Ausführungsbestimmungen des Regierungsrates handeln.

Grundsätzlich müssen in der Rechtsgrundlage Zweck, beteiligte Organe und Ausmass der Datenbearbeitung in den Grundzügen festgelegt sein. Der Detaillierungsgrad bestimmt sich nach dem Eingriff der Datenbearbeitung in die Freiheitsrechte der Bürger, der Art der bearbeiteten Daten, dem Kreis der betroffenen Personen, aber auch der Organisation des Informationssystems. Angesichts der unendlichen Vielfalt von Datenbearbeitungsvorgängen in der Verwaltung dürfen aber keine allzu strengen Anforderungen an die gesetzliche Grundlage gestellt werden. Vielfach muss es genügen, dass eine Informationsbearbeitung in einem einsichtigen sachlichen Zusammenhang mit der Aufgabe des betreffenden Bundesorgans steht. Immerhin aber sind von den öffentlichen Organen die Grundsätze in Art. 4 zu beachten.

Art. 7 Abs. 1 entspricht dem allgemeinen Grundsatz in Art. 8 StVG.

Abs. 2: An das Bearbeiten von besonders schützenswerten Personendaten und von Persönlichkeitsprofilen sind qualifizierte Anforderungen zu stellen. Da es aber kaum je möglich sein wird, für jegliche Bearbeitung sensitiver Daten die nötige Bestimmung in einem formellen Gesetz zu schaffen, sollen derartige Daten auch bearbeitet werden dürfen, wenn:

– die Bearbeitung für eine in einem formellen Gesetz klar umschriebene Aufgabe unentbehrlich ist;[16]
– der Regierungsrat unter bestimmten Voraussetzungen im Einzelfall die Bearbeitung bewilligt, um kurzfristig auftretenden Bedürfnissen Rechnung tragen zu können;[17]
– die betroffene Person eingewilligt (vgl. Art. 5 des Entwurfes) oder ihre Daten allgemein zugänglich gemacht hat und sich einer Bearbeitung nicht widersetzt (Bst. c).

Art. 8 *Datenbearbeitung durch Dritte*

(Art. 7 ER-Konv 108
Art. Art. 17 Abs. 2 – 4 EU-DSRL)

Die Bestimmung steht im Zusammenhang mit der Datensicherheit (Art. 11). Hier ist sie eine Adaption von Art. 14 DSG, der zwar für die Bearbeitung von Personendaten durch private Personen geschaffen wurde, vorliegend aber auf öffentliche Organe angewendet werden soll.

Denn das Datenschutzgesetz soll auch für Dritte gelten, die im Auftrag eines Organs eine öffentliche Aufgabe erfüllen. Das öffentliche Organ, welches den Auftrag erteilt hat, bleibt zwar im externen Verhältnis verantwortlich (vgl. aber die Strafbestimmungen in Art. 40). Es ist aber wichtig, dass bei der Auftragserteilung sichergestellt wird, dass der Datenschutz durch den beauftragten Dritten in gleicher Weise gewährleistet wird, wie wenn das öffentliche Organ selbst die Daten bearbeiten würde, namentlich durch:

– Sorgfalt bei der Auswahl des Auftragnehmers;
– Anordnung von Sicherheitsvorkehren (Auflagen, Weisungen etc.)

---

[16] Hingegen rechtfertigt der Umstand, dass eine Aufgabe durch Verwendung von besonders schützenswerten Daten oder Persönlichkeitsprofilen noch besser erfüllt werden kann, für sich allein die Bearbeitung dieser Daten noch nicht.

[17] Die Delegationsklausel erlaubt aber nicht, eine unbestimmte Anzahl von Fällen zu bewilligen.

– organisatorische Massnahmen;
– Kontrolle der Einhaltung der Vereinbarung.

Art. 9 *Verantwortlichkeit*

(z.B. Art. 6 Abs. 2 EU-DSRL)

Abs. 1: Die öffentlichen Organe tragen im Rahmen ihrer durch Gesetz und Verordnung eingeräumten Zuständigkeiten auch die datenschutzrechtliche Verantwortung. Sie sind es, die namentlich Einblick in die Datensammlungen geben, die Weitergaberegeln beachten und Sicherheitsmassnahmen ergreifen müssen.

Abs. 2: Namentlich bei automatisierten Datenverarbeitungssystemen oder Abrufverfahren verwenden oft mehrere Organe, eventuell zusammen mit Dritten, Daten aus ein und derselben Datensammlung. Abs. 2 weist für solche Fälle die Verantwortung zu.

In dem die beteiligten Organe für ihren Bereich verantwortlich bleiben, soll einerseits vermieden werden, dass eine betroffene Person von einer Verwaltungsstelle zur anderen gesandt wird, weil sich jede nur für einen Teil verantwortlich erklärt, und andererseits, dass das hauptverantwortliche Organ der Datensammlung für die Weiterbearbeitung eines beteiligten Organs verantwortlich gemacht wird.

Der Regierungsrat kann die Verantwortlichkeit bei gemeinsamer Datenbearbeitung mehrerer öffentlicher Organe über Ausführungsbestimmungen regeln.

Art. 10 *Datenrichtigkeit*

(Art. Art. 5 Abs. 1 i.V.m. Art. 37 Abs. 1
Art. 5 Bst. d ER-Konv 108
Art. 6 Abs. d EU-DSRL)

Personendaten, die von öffentlichen Organen bearbeitet werden, müssen richtig sein, weil es:
– das Recht auf informationelle Selbstbestimmung (Art. 13 BV) es gebietet;
– die Bearbeitung unrichtiger Daten zur behördlichen Aufgabenerfüllung nicht verhältnismässig sein kann.

Dementsprechend wurde das Erfordernis der Richtigkeit und Vollständigkeit, soweit es der Bearbeitungszweck verlangt, im Gesetz als Grundsatz verankert. An diesen knüpft der Berichtigungsanspruch der betroffenen Personen (vgl. Art. 29 des Entwurfs).

Art. 11 *Datensicherheit*

(Art. 7 i.V.m. Art. 37 Abs. 1 DSG
Art. 7 ER-Konv 108
Art. 17 EU-DSRL)

Personendaten müssen durch technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt sein, insbesondere gegen:
– zufällige oder unbefugte Zerstörung;
– gegen zufälligen Verlust;
– unbefugten Zugang;
– unbefugte Veränderung unbefugtes Bekanntgeben.

Es bestehen bereits Bestimmungen über die Mindestanforderungen an die Datensicherheit. Zu erwähnen sind hier die regierungsrätlichen Weisungen über die Nutzung von Informatikmitteln (Informatikweisungen) vom 14. November 2005.

Art. 12 *Archivieren und Vernichten*

(Art. 21 DSG
Art. 5 Bst. e ER-Konv 108
Art. 6 Abs. 1 Bst. e EU–DSRL)

Abs. 1 und 2: Ein Ausfluss des Verhältnismässigkeitsprinzips ist die zeitliche Begrenzung

der Aufbewahrung von Personendaten: Sollten diese zur Aufgabenerfüllung nicht mehr erforderlich sein, sind sie – vorbehältlich gesetzlicher Archivierungsregelungen – zu vernichten (oder zu anonymisieren, so dass kein Rückschluss mehr auf die betroffene Person möglich ist).

Der Entwurf lässt Raum für spezielle Archivierungsregelungen (vgl. Art. 3), z.B. in Bezug auf:

– Gerichtsakten;
– Akten des Betreibungs- und Konkursamtes;
– Grundbuchakten;
– elektronische Unterlagen.

Abs. 3: Da Art. 5 der Verordnung über das Staatsarchiv lediglich auf kantonale Organe Anwendung findet, ist die Bestimmung für kommunale Organe sinngemäss anwendbar.

8.2.2 Beschaffung von Personendaten

Der Abschnitt über das Beschaffen von Personendaten stellt eine Ergänzung zu den Grundsätzen von Art. 4 und dem vorangehenden Abschnitt über die allgemeinen Bearbeitungsvorschriften dar. Die Bestimmungen sollen Gewähr bieten, dass in einer Zeit, in welcher die Verwaltung auf immer mehr Informationen und namentlich auch auf Personendaten angewiesen ist, diese so beschafft werden, dass der Betroffene allenfalls dazu Stellung nehmen und sich gegen eine unzulässige Bearbeitung wehren kann.

Wichtigste Voraussetzung hierfür ist die Transparenz bezüglich der Bearbeitung von Personendaten. Transparenz bedingt, dass die betroffene Person:

– weiss, welche Datenbearbeitungen erfolgen oder welche Datensammlungen bestehen (Erkennbarkeit durch die betroffene Person);
– vom öffentlichen Organ über bestimmte behördliche Datenbearbeitungen informiert wird (Informationspflicht des Datenbearbeiters).

Besteht Transparenz über die Bearbeitung von Personendaten, kann die betroffene Person – gegebenenfalls nach Einsicht in das Register der öffentlichen Datensammlungen – ihre Rechte wahrnehmen und sich allenfalls gegen eine unzulässige Bearbeitung wehren.

Art. 13 *Datenquellen*

(Art. 4 Abs. 2 i.V.m. Art. 37 Abs. 1 DSG
Art. 6 Abs. 1 Bst. a [aber auch Art. 10 und 11 Abs. 1] EU-DSRL
Art. 5 Bst. a ER-Konv 108)

Abs. 1: Daten müssen so beschafft werden, dass dies für die betroffene Person erkennbar ist. Diesem Gebot wird am besten nachgelebt, wenn die Daten bei der betroffenen Person selber erhoben werden.

Abs. 2: Aber auch eine Erhebung bei Dritten ist zulässig, sofern die betroffene Person ausreichend darüber informiert wird. Denn die Erhebung bei Dritten, die bereits über die benötigten Daten verfügen, stellt eine wichtige Rationalisierungsmöglichkeit für die Verwaltung dar, welche nicht grundsätzlich in Frage gestellt werden soll. Auch ist es zum Teil im Interesse des Bürgers, wenn er die gleichen Angaben nicht gegenüber verschiedenen Verwaltungsstellen wiederholen muss.

Art. 14 *Erkennbarkeit*

(Art. 4 Abs. 4 i.V.m. Art. 37 Abs. 1 DSG
Art.
im Übrigen vgl. Art. 13)

Die Erkennbarkeit der Datenbearbeitung stellt ein Kernelement des Datenschutzrechts dar und ist Ausfluss des Grundsatzes, dass öffentliche Organe nach Treu und Glauben zu handeln haben.

In Art. 18 Abs. 2 aDSG statuierte der Bundesgesetzgeber noch lediglich die Erkennbar-

keit bei der Bearbeitung besonders schützenswerter Personendaten oder Persönlichkeitsprofilen. Im revidierten Art. 4 Abs. 4 DSG wird die Erkennbarkeit grundsätzlich und für jede Datenbearbeitung verlangt.

Zur Systematik: Art. 14 stellt eine Konkretisierung des Grundsatzes in Art. 4 Abs. 2 des Entwurfs dar. Die Pflicht, Daten primär bei der betroffenen Person zu erheben (Art. 13), wurde dem Grundsatz der Erkennbarkeit (Art. 14) vorangestellt. Dies, weil der Entscheid der öffentlichen Organe, welche Datenquellen heran gezogen werden sollen, vor der tatsächlichen Bekanntgabe der Datenerhebung erfolgt. Die Systematik entspricht hier somit dem chronologischen Ablauf der Datenerhebung.

Art. 15 *Informationspflicht bei systematischen Erhebung*

(Art. 18 i.V.m. Art. 37 Abs. 1 DSG
Art. 8 Bst. a ER-Konv 108
Art. 10 EU-DSRL)

Die Bestimmungen von Art. 15 und 16 gehen bezüglich des Grundsatzes der Erkennbarkeit der Datenbeschaffung weiter als Art. 4 Abs. 2 und Art. 15, konkretisieren sie doch den Grundsatz in dem Sinne, als sie eine Pflicht zur aktiven Information vorsehen.

Für systematische Erhebungen obliegt dem öffentlichen Organ eine besondere Orientierungspflicht, da in solchen Fällen in grossem Umfang Daten beschafft werden. Wenn auch aufgrund einer Befragung nicht notwendigerweise eine Datensammlung entstehen muss, so sollen doch die Betroffenen in ähnlicher Weise orientiert werden wie bei Datensammlungen (Art. 16).

Art. 16 *Informationspflicht bei schützenswerten Personendaten und Persönlichkeitsprofilen*

(Art. 7a i.V.m. Art. 37 Abs. 1
Art. 6 i.V.m. Art. 8 Bst. a ER-Konv 108
Art. 10 und 11 EU-DSRL)

Abs. 1: Der Inhaber der Datensammlung, der besonders schützenswerte Daten oder Persönlichkeitsprofile beschafft, ist verpflichtet, von sich aus die betroffene Person zu informieren.

– im Gegensatz zum Auskunftsrecht nach Art. 25.

Die Bestimmung geht weiter als der Grundsatz der allgemeinen Erkennbarkeit, denn sie sieht eine Pflicht zur aktiven Information vor. Der verstärkte Schutz rechtfertigt sich insofern, als die Bearbeitung von besonders schützenswerten Daten und Persönlichkeitsprofile in Datensammlungen zu systematischen Diskriminierungen führen kann. Im Übrigen wird der Inhaber der Datensammlung bestrebt sein, keine entsprechenden Daten zu beschaffen, die er für seine Tätigkeit nicht unbedingt benötigt, wenn er die betroffene Person stets aktiv informieren muss.

Die Information ist keinem Formerfordernis unterworfen.

Abs. 2: Der Inhaber der Datensammlung muss der betroffenen Person alle Informationen zukommen lassen, die für eine Bearbeitung nach dem Grundsatz von Treu und Glauben erforderlich sind (vgl. Art. 10 und 11 EU-DSRL). Gemäss Bst. c sind lediglich die Kategorien allfälliger Datenempfänger, nicht aber die Identität jedes einzelnen Datenempfängers anzugeben.

Abs. 3: Die gesamte Bestimmung lehnt sich an Art. 7a nDSG, die allerdings im parlamentarischen Verfahren des Bundes eine starke Änderung erfahren hat (vgl. BBl 2003 2132 und AB 2005 N 1443 / BO 2005 N 1443). Aus diesem Grund wurden die beiden letzten Absätze nicht wortgetreu übernommen. Abs. 3 enthält nunmehr übersichtlich alle Ausnahmen der Informationspflicht. Sie gelten unabhängig davon, ob eine Beschaffung bei der betroffenen Person oder eine Drittbeschaffung stattgefunden hat.

Die Informationspflicht des öffentlichen Organs entfällt in folgenden Fällen:

– Bst. a: Die betroffene Person ist bereits informiert, evtl. durch Dritte.
– Bst. b: Das Gesetz sieht die Datenbeschaffung oder weitere Datenbearbeitungsschrit-

te ausdrücklich vor. Im Gegensatz zur Bundeslösung entfällt hier die Informationspflicht nicht nur dann, wenn die Daten bei Dritten beschafft wurden, sondern generell, wenn das Gesetz die entsprechende Regelung vorsieht. Denn gerade bei Drittbeschaffungen müsste aufgrund der fehlenden Erkennbarkeit der Datenbeschaffung die Informationspflicht aus datenschutzrechtlicher Sicht eigentlich strenger sein als bei Beschaffungen bei der betroffenen Person.

– Bst. c: Die Information der betroffenen Person erweist sich als sehr schwierig oder unmöglich. Es ist jedoch alles zu unternehmen, was nach den Umständen vernünftigerweise verlangt werden kann, um der Informationspflicht nachzukommen. Es versteht sich von selbst, dass dies nur für Drittbeschaffungen gilt.
– Bst. d: Das Auskunftsrecht kann eingeschränkt werden (Art. 26).

Abs. 4: Die betroffene Person muss möglichst dann informiert werden, wenn der Inhaber der Datensammlung die Daten beschafft, spätestens jedoch beim nächsten Bearbeitungsschritt, d.h. bei jeder sich an die Beschaffung anschliessenden Tätigkeit, die eine weitere Verwertung der Daten vorbereitet (z.B. Speicherung oder Bekanntgabe an Dritte).

Exkurs: Automatisierte Einzelentscheidung: Gemäss Art. 15 EU–DSRL dürfen Personen nur unter bestimmten Voraussetzungen einem Entscheid unterworfen sein, der für sie rechtliche Folgen hat oder sie sonst wesentlich betrifft und ausschliesslich auf einer automatisierten Datenbearbeitung beruht, welche die Bewertung einzelner Aspekte ihrer Persönlichkeit bezweckt (z.B. Bewertung von Merkmalen wie der Kreditwürdigkeit, der Zuverlässigkeit, des Verhaltens oder von spezifischen [Versicherungs-]Risiken).

Der Entwurf des Bundesrats (BBl 2003 2134) enthielt in diesem Zusammenhang eine Informationspflicht: Die betroffene Person sollte ausdrücklich darüber informiert werden, wenn ein Entscheid auf einer automatisierten Datenbearbeitung beruht. Allerdings wurde diese Bestimmung in der parlamentarischen Beratung ersatzlos gestrichen (AB 2005 N 1447 / BO 2005 N 1447). Die Nachbarkantone haben ebenfalls keine derartige Bestimmung in ihr Datenschutzrecht aufgenommen

8.2.3 Bekanntgabe von Personendaten

Art. 17 *Im Allgemeinen*

(Art. 19 Abs. 1 – 2 i.V.m. Art. 37 Abs. 1 DSG)

Die Erfahrung zeigt, dass die Regelungen über die Bekanntgabe von Personendaten die wichtigste Rolle im öffentlich-rechtlichen Persönlichkeitsschutz spielen. Es besteht ein Spannungsfeld zwischen den Erfordernissen einer koordinierten und rationellen Verwaltungstätigkeit und den Anliegen des Persönlichkeitsschutzes. Die vorliegende Bestimmung stellt eine Art allgemeine Amts- und Rechtshilferegelung dar und konkretisiert das Amtsgeheimnis.

Mit der vorliegenden Bestimmung werden die Art. 9 und 10 StVG in den vorliegenden Entwurf übernommen und vereint; auf die Unterscheidung der Bekanntgabe an öffentliche Organe oder an private Personen und Organisationen wird verzichtet.

Die nachfolgenden Bestimmungen Art. 18 – 20 des Entwurfs ergänzen die Allgemeinen Regelungen im Hinblick auf spezielle Fälle.

Abs. 1: Daten dürfen grundsätzlich weitergegeben werden, wenn dafür eine Rechtsgrundlage besteht, das heisst wenn die Weitergabe in einem Gesetz, in einer Verordnung, in Ausführungsbestimmungen oder in einem Vertrag vorgesehen ist.

Fehlt es an einer Rechtsgrundlage, so können Personendaten dennoch weitergegeben werden in folgenden Fällen:

– Bst. a: Wenn der Empfänger im Einzelfall sonst seine gesetzliche Aufgabe überhaupt nicht erfüllen könnte. Die Beweislastregel in Art. 9 Bst. b StVG "glaubhaft macht" wurde hier nicht mehr aufgenommen, sondern der Praxis überlassen. Im "Einzelfall" bedeutet dies, dass ohne gesetzliche Grundlage kein dauernder Zugriff auf eine Datensammlung gewährt werden darf.

– Bst. b und c: Wenn die betroffene Person eingewilligt hat. Der Passus in Art. 9 Bst. c und Art. 10 Abs. 1 Bst. b StVG "oder die Einwilligung nach den Umständen vorausgesetzt werden darf" wurde im vorliegenden Entwurf nicht mehr aufgenommen, da einerseits die Definition einer gültig erteilten Einwilligung in Art. 5 geregelt ist, andererseits weil Art. 17 Abs. 1 Bst. c den entsprechenden Passus teilweise ausschreibt.
– Bst. d: Wenn die betroffene Person in rechtsmissbräuchlicher Art Angaben über sich selber verweigern will (z.B. Geltendmachung familienrechtlicher Ansprüche, Auskunft des Arbeitnehmers über vom Arbeitgeber einbezahlten Beträge an den Sozialversicherer).
  Das öffentliche Organ kann auf die Einholung einer Stellungnahme verzichten, wenn die Gefahr besteht, dass Rechtsansprüche oder wichtige Interessen von Dritten beeinträchtigt würden, oder wenn der Betroffene innert Frist nicht reagiert oder nicht auffindbar ist.

Abs. 2: Die Personalien (Name, Vorname), die Adresse sowie das Geburtsdatum einer Person dürfen auf Anfrage einem anderen öffentlichen Organ oder einer interessierten Privatpersonen bekannt gegeben werden. Mangels Bekanntgabepflicht muss auch bei dieser Art von Datenweitergabe allfälligen Schutzbedürfnissen einer betroffenen Person Rechnung getragen werden (vgl. Art. 21 des Entwurfes).

Abs. 3: Damit wird – im Spannungsfeld von Datenschutz-, Informations- und Transparenzanliegen – die notwendige Rechtsgrundlage für Fälle der behördlichen Informationstätigkeit in Bezug auf Personendaten geschaffen (vgl. auch Art. 7 der Organisationsverordnung). Welche Informationen veröffentlicht werden können, ist aufgrund einer Interessenabwägung im Einzelfall zu ermitteln (BBl 2003 2033). Diesbezüglich wird die Bestimmung durch Art. 2 der Ausführungsbestimmungen über die Information der Öffentlichkeit durch den Regierungsrat und die kantonale Verwaltung vom 28. Januar 1992 (Informationsrichtlinien; GDB 131.111) konkretisiert.

Abs. 2 und 3 beinhalten im Weitesten Sinne Art. 10 Abs. 2 und 3 StVG.

Art. 18 *Bekanntgabe ins Ausland*

(Art. 6 i.V.m. Art. 37 Abs. 1 DSG
Art. 12 ER-Konv 108 und Art. 2 ZP zur ER-Konv 108
Art. 25 f. EU-DSRL)

Die Bestimmung soll verhindern, dass Daten an Staaten weitergegeben werden, welche die Grund- und Menschenrechte nicht einhalten oder die über keinen, dem europäischen Niveau gleichwertigen, Datenschutz verfügen. Denn Datenbearbeitungen, die im Inland und in den Nachbarstaaten problemlos sind, können für die betroffene Person im Ausland mit erhöhten Risiken einer Persönlichkeitsverletzung verbunden sein, wenn sie ohne spezielle Vorkehrungen ins Ausland transferiert werden. Diesen Grundsatz gilt es in das kantonale Recht aufzunehmen und zu konkretisieren.

Abs. 1: Die öffentlichen Organe trifft eine Sorgfaltspflicht. Die Datenübermittlung ins Ausland verlangt – zusätzlich zu den allgemeinen Bekanntgabevoraussetzungen – dass namentlich die Gesetzgebung oder hinreichende Garantien im Bestimmungsland einen angemessenen Schutz gewährleisten. Dies ist dann gegeben, wenn die Anforderungen der ER-Konv 108 erfüllt sind. Im Falle einer Datenbekanntgabe an einen Empfänger, für den die ER-Konv 108 nicht gilt, muss ein adäquates Datenschutzniveau sichergestellt sein.

Abs. 2: Die beauftragte Person für Datenschutz prüft – analog Art. 8b Abs. 2 Bst. b StPO – ob ein angemessener Schutz gewährleistet ist. Es handelt sich um eine Konkretisierung von Art. 6 des Entwurfs. Die Angemessenheit des Datenschutzniveaus wird unter Berücksichtigung aller Umstände beurteilt, die für die Datenübermittlung von Bedeutung sind.

Abs.3: Gewährleistet ein Drittstaat kein angemessenes Datenschutzniveau, so können Personendaten im Einzelfall trotzdem bekannt gegeben werden, wenn:

– die betroffene Person im Sinne von Art. 5 des Entwurfs eingewilligt hat;
– die Bekanntgabe erforderlich ist, um das Leben oder die körperliche Integrität der betroffenen Person zu schützen;

- die Bekanntgabe entweder für die Wahrung eines überwiegenden öffentlichen Interesses oder für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht unerlässlich ist;
- die betroffene Person die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat.

Abs. 4: Wurde generell ein angemessenes Datenschutzniveau durch die beauftragte Person für Datenschutz festgestellt, wie beispielsweise bei den EU-Staaten, welche die EU-DSRL im innerstaatlichen Recht umgesetzt haben, sind in der Regel lediglich die allgemeinen Bekanntgabevoraussetzungen im Sinne von Art. 17 des Entwurfs zu prüfen. Freilich sind diese auch im Falle von Abs. 3 zu prüfen, wie die systematische Anreihung zeigt.

Art. 19 *Bekanntgabe im Abrufverfahren*

(Art. 19 Abs. 3 i.V.m.
Art. 37 Abs. 1 DSG)

Nach Abs. 1 dieser Bestimmung dürfen öffentliche Organe Personendaten durch ein Abrufverfahren zugänglich machen, wenn dies von der Gesetzgebung ausdrücklich vorgesehen ist. Gemäss Abs. 2 ist bei besonders schützenswerten Personendaten als Grundlage für ein solches Abrufverfahren ein formelles Gesetz erforderlich. Zudem ist eine Vorabkontrolle im Sinne von Art. 6 des Entwurfs durchzuführen.

Unter einem Abrufverfahren versteht man jedes automatisierte Verfahren, welches einem Dritten ermöglicht, über die Daten ohne Intervention des bekannt gebenden Organs zu verfügen. Es erlaubt dem informationssuchenden Organ, sich seine Informationen anhand des Datenbestands einer anderen staatlichen Stelle selber, zielgerichtet und fristgerecht zu beschaffen (z.B. ViCLAS [Violent Crime Linkage Analysis System]; vgl. auch Art. 111m Verordnung vom 22. Februar 1910 betreffend das Grundbuch [GBV; SR 211.432.1] i.V.m. Art. 17b Verordnung über das Grundbuch vom 29. Februar 1980 [GDB 213.41])

Ausdrücklich bedeutet, dass die gesetzliche Grundlage das öffentliche Organ bezeichnen muss, welches die Daten bearbeitet. Weiter muss sie den Zweck nennen, dem die Bearbeitung dienen soll sowie den Umfang der Bearbeitungsberechtigung umreissen. Sie genügt nicht, wenn sie einzig die für die Bearbeitung erforderlich machenden Aufgaben statuiert. Als typisches Beispiel einer gesetzlichen Grundlage sei Art. 8b StPO erwähnt.

Art. 20 *Automatisierte Informations- und Kommunikationsdienste*

(Art. 19 3bis i.V.m.
Art. 37 Abs. 1 DSG)

Die Bestimmung schafft eine Grundlage für die Veröffentlichung von Personendaten auf dem Internet durch die öffentlichen Organe zu Informationszwecken. Dabei ist allerdings der Grundsatz der Verhältnismässigkeit (Art. 4 Abs. 4 des Entwurfs) zu beachten. Es sind Fälle denkbar, in denen eine Veröffentlichung von Personendaten unverhältnismässig sein könnte (z.B. wenn der Personenkreis, an den sich die Information richtet, klein und von vornherein genau bestimmbar ist).

Die Bestimmung knüpft an Art. 17 Abs. 3 des Entwurfs, welcher vorgängig eine Interessenabwägung verlangt.

Schliesslich sind die Informationen, die Personendaten enthalten, wieder zu löschen bzw. vom Netz zu nehmen, wenn durch den Zeitablauf das öffentliche Interesse an ihrer Publikation erloschen ist.

Art. 21 *Ablehnung der Bekanntgabe*

(Art. 19 Abs. 4 i.V.m.
Art. 37 Abs. 1 DSG)

Die Bestimmung – die Art. 12 Abs. 1 StVG entspricht – hält fest, unter welchen Umständen das Ersuchen um eine an und für sich zulässige Bekanntgabe im Einzelfall abgelehnt werden kann. Erscheint eine Verweigerung der Datenbekanntgabe als unverhältnismäs-

sig, kann sie unter Auflagen erteilt oder eingeschränkt gewährt werden. Vorbehalten bleiben besondere Geheimhaltungsvorschriften, die als Spezialrecht den kantonalen Datenschutzbestimmungen vorgehen.

8.2.4 Besondere Formen der Personendatenbearbeitung

Art. 22 *Bearbeitung für nicht personenbezogene Zwecke*

(Art. 22 i.V.m. Art. 37 Abs. 1 DSG
Art. 9 Ziff. 3 ER-Konv 108
Art. 6 Abs. 1 Bst. b und e und Art. 11 Abs. 2 EU-DSRL)

Abs. 1: Personendaten können zu nicht personenbezogenen Zwecken bearbeitet werden, wenn zwar Daten über bestimmte oder bestimmbare Personen bearbeitet werden, nicht jedoch diese, sondern Statistik, Planung oder Forschung, sogenannte wissenschaftliche Zwecke, im Fokus stehen.

Solche Bearbeitungen werden privilegiert, insbesondere vom Vorliegen einer spezifischen gesetzlichen Grundlage für die Bearbeitung befreit, wenn sichergestellt wird, dass die Daten anonymisiert werden, sobald es der Bearbeitungszweck zulässt und die Ergebnisse so veröffentlicht werden, dass es unmöglich ist, auf die betroffenen Personen zurück zu schliessen.

Abs. 2: Für die Bekanntgabe von Personendaten an Dritte, d.h. an Empfänger ausserhalb der Verwaltung erscheint es sinnvoll, die Gewährleistung von Abs. 1 über zusätzliche Auflagen vorzusehen (Garantien, Weitergabeverbot, Verstärkung mit Konventionalstrafe u.ä.).

Art. 23 *Überwachungsgeräte*

Die Aufzeichnungen und deren Aufbewahrung während 100 Tagen stellen eine präventive Massnahme zur Verhütung von Straftaten dar. Es sollen Beweise sichergestellt und damit eine effiziente Aufdeckung von Straftaten ermöglicht werden. Mit dem damit verbundenen Abschreckungseffekt soll im Dienste der Wahrung der öffentlichen Sicherheit und Ordnung und der Gewährleistung der Sicherheit von Benützern öffentlicher Strassen und Plätze Straftaten begegnet werden. Es steht ausser Frage, dass diese Zielsetzung im heutigen Zeitpunkt einem öffentlichen Interesse entspricht.

Die Wirksamkeit der Strafverfolgung steht in Beziehung zur Dauer der Aufbewahrung der Aufzeichnungen. Bei Straftaten – auf öffentlichem Grund, an abgelegenen Orten, zu nächtlicher Stunde oder aber auch an stark frequentierten Stellen – bilden solche Aufzeichnungen häufig das einzig aussagekräftige Beweismaterial. Eine äusserst kurze Aufbewahrungsdauer birgt die Gefahr, dass im Falle einer erst späteren Entdeckung einer Straftat oder später eingereichten Anzeige die Aufzeichnungen bereits gelöscht sind und darauf als Beweismittel nicht mehr zurückgegriffen werden kann. Eine gewisse Aufbewahrungsdauer ist damit erforderlich, um die durch eine wirksame Strafverfolgung erhoffte Abschreckungswirkung sicherzustellen. Dies um so mehr, als das Anzeigeverhalten der Betroffenen weitgehend von persönlichen Umständen abhängt. Es ist nachvollziehbar, dass zum Beispiel bei Straftaten gegen die sexuelle Integrität oder gegen Jugendliche aus Furcht oder Scham oder mannigfaltigen anderen Gründen mit einer Anzeige oder einem Strafantrag eine gewisse Zeit zugewartet wird.

Die Dauer von 100 Tagen erscheint zudem, im Vergleich mit anderen Regelungen, als lang (vgl. Verordnung über die Videoüberwachung durch die Schweizerischen Bundesbahnen SBB [SR 742.147.2]; Verordnung über die Geländeüberwachung mit Videogeräten [SR 631.09]; Verordnung über Glücksspiele und Spielbanken [SR 935.521]).Das Bundesgericht hat jedoch unlängst entschieden, dass eine Aufbewahrungsdauer von 100 Tagen für die Verwendung im strafrechtliche Ermittlungsverfahren zulässig ist (BGE 133 I 77).

Immerhin ist die missbräuchliche Verwendung des Bildmaterials durch geeignete technische und organisatorische Massnahmen auszuschliessen (Art. 11 des Entwurfs). Zudem ist die Öffentlichkeit mit Hinweistafeln auf den Einsatz von Überwachungsmassnahmen

aufmerksam zu machen (Art. 23 Abs. 1 Bst. a des Entwurfs)

8.3 Rechte der betroffenen Personen

Art. 24 *Register der Datensammlungen*

(Art. 11a i.V.m. Art. 37 Abs. 1 DSG
Art. 8 Bst. a ER-Konv 108
Art. 18 f. und 21 EU-DSRL)

Abs. 1: Die Datensammlungen der öffentlichen Organe müssen in einem öffentlichen Register angemeldet werden. Minimale Angaben sind:

– die Rechtsgrundlage der Bearbeitung;
– der Zweck und die Mittel der Bearbeitung;
– die Art und Herkunft der bearbeiteten Personendaten;
– die an der Datensammlung beteiligten Stellen und die regelmässigen Datenempfänger.

Die Registrierung der Datensammlungen bezweckt:

– Transparenz für die betroffenen Personen (wo werden welche Personendaten bearbeitet) als Grundlage für die Geltendmachung ihrer Rechte;
– Bewusstmachen der bearbeitenden öffentlichen Organe, die sich auf die Rechtsgrundlage ihrer Datenbearbeiten besinnen müssen;
– Schaffung einer Grundlage für die Kontrolltätigkeit des Kontrollorgans.

Abs. 2: Ausnahmen von der Registrierungspflicht sind zulässig für Datensammlungen, die:

– nur kurzfristig verwendet werden;
– rechtmässig veröffentlicht sind;
– reine Hilfsdatensammlungen[18] sind.

Um den Zweck der Datensammlung sicherzustellen, muss sie öffentlich und von jedermann einsehbar sein. Die organisatorische Abwicklung des Zugangs kann durch den Regierungsrat in Ausführungsbestimmungen näher geregelt werden.

Art. 25 *Auskunftsrecht*

(Art. 8 i.V.m. Art. 37 Abs. 1 DSG
Art. 8 Bst. b ER-Konv 108
Art. 12 Abs. a EU-DSRL)

Abs. 1: Das Recht jeder Person, Auskunft zu erhalten, ob und wenn ja, welche Daten über sie von einem öffentlichen Organ in einer bestimmten Datensammlung bearbeitet werden, und zwar unabhängig davon, ob das öffentliche Organ die Daten selber bearbeitet oder bearbeiten lässt, ist einer der Kernpunkte des Datenschutzrechts (vgl. schon heute Art. 13 Abs. 1 StVG). Es ist der Ausgangspunkt für die weiteren Rechte und Ansprüche der betroffenen Person. Nur wer weiss, ob und welche Daten über ihn bearbeitet werden, kann diese nötigenfalls berichtigen oder vernichten lassen oder wenigstens deren Richtigkeit bestreiten (Art. 27 ff. des Entwurfs).

Beim Auskunftsrecht handelt es sich um ein subjektives, höchstpersönliches Recht, das auch von einer urteilsfähigen unmündigen oder entmündigten Person direkt ausgeübt werden kann; deshalb kann vorab auch nicht darauf verzichtet werden (Abs. 3).

Adressat des Auskunftsbegehrens ist nicht jeder, der Daten bearbeitet – dies wäre nicht praktikabel – sondern nur der Inhaber einer Datensammlung. Dies weil die Möglichkeiten einer Persönlichkeitsverletzung bei ihm wesentlich grösser sind als bei jemandem, dessen Daten nicht nach den betroffenen Personen systematisch erschlossen sind.

Abs. 2: Die Auskunft muss vollständig und richtig sein. Die Verpflichtung, Auskunft betref-

[18] Kopien und Bearbeitungsmittel oder ausschliesslich persönliche Arbeitsmittel sind.

fend die Herkunft der Daten zu geben, besteht nur insoweit, als diese Information verfügbar ist.

Zu regeln sind aber auch die Modalitäten des Auskunftsrechts (Initiierung durch ein Begehren der betroffenen Person, Form der Auskunftserteilung. Diesbezüglich ist es zur Vereinfachung des Verfahrens zulässig vorzusehen, dass auf Begehren der betroffenen Person auch direkt Einsicht in die relevanten Daten gewährt werden kann). Der Regierungsrat kann in Ausführungsbestimmungen das Nähere regeln.

Art. 26 *Einschränkung des Auskunftsrechts*

(Art. 9 und 10 i.V.m. Art. 37 Abs. 1 DSG
Art. 9 Abs. 2 ER-Konv 108
Art. 13 EU-DSRL)

Abs. 1: So wichtig und unabdingbar das Auskunftsrecht für den Persönlichkeits- und Datenschutz auch ist, so kann es doch nicht uneingeschränkt beansprucht werden. Das Recht auf Auskunft darf aber nicht ohne Weiteres eingeschränkt (verweigert, eingeschränkt oder aufgeschoben) werden, sondern das Gesetz muss abschliessend festlegen, wann die Auskunft höchstens eingeschränkt werden darf (vgl. schon heute Art. 13 Abs. 2 StVG).

Das Auskunftsrecht darf eingeschränkt werden, wenn:

– Bst. a: ein formelles Gesetz dies vorsieht;
– Bst. b: ein überwiegendes öffentliches Interesse des Staates (innere oder äussere Sicherheit) vorliegt oder die gesuchstellende Person beim Einblick in ihre Daten zugleich auch Informationen über Drittpersonen erhalten könnte und dadurch die Interessen derselben verletzt würden; oder
– Bst. c: der Zweck einer Strafuntersuchung[19] oder eines anderen amtlichen Untersuchungsverfahrens (z. B. eines Disziplinarverfahrens) in Frage gestellt würde.

Der Inhaber der Datensammlung muss der gesuchstellenden Person angeben, aus welchen Gründen er die Auskunft einschränkt (vgl. Art. 35 des Entwurfs).

Abs. 2: Zum Selbstschutz der betroffenen Person ist ein besonderes Verfahren vorgesehen, ohne dass die Auskunftserteilung verweigert wird (z.B. kann die Auskunft betreffend Patientendaten über einen Vertrauensarzt erteilt werden).

Art. 27 Anspruch auf Massnahmen:
a. Sperrung der Bekanntgabe

(Art. 20 i.V.m. Art. 37 Abs. 1 DSG
Art. 12 Bst. b EU-DSRL)

Art. 27 – 29: Die öffentlichen Organe dürfen Personendaten nur rechtmässig, nach Treu und Glauben sowie unter Beachtung des Verhältnismässigkeitsprinzips bearbeiten (Art. 4 des Entwurfs). Vor diesem Hintergrund räumt der Entwurf den betroffenen einen Anspruch auf folgende Massnahmen ein:

– Sperrung der Bekanntgabe;
– Unterlassung, Beseitigung oder Feststellung des widerrechtlichen Bearbeitens;
– Berichtigung, Vernichtung, Bestreitung oder Sperrung der Bekanntgabe unrichtiger Daten.

Abs. 1: Die von behördlicher Datenbearbeitung betroffene Person kann vom verantwortlichen Organ verlangen, dass es die an sich zulässige Bekanntgabe von bestimmten Personendaten sperrt. Das verantwortliche Organ kann nicht alle möglichen negativen Auswirkungen voraussehen, weshalb die betroffene Person ihre Interessen direkt geltend machen kann. Die Sperre gilt grundsätzlich aber auch für Bekanntgaben gegenüber an-

[19] Die Bestimmung dürfte keine allzu grosse Bedeutung erlangen, da ja das Gesetz insgesamt keine Anwendung auf Verfahren findet, die in Prozessgesetzen geregelt sind. Immerhin ist vorstellbar, dass Auskünfte ausserhalb eines Untersuchungsverfahrens dieses negativ beeinflussen.

deren Behörden (vgl. aber Abs. 2).

Das Sperrrecht kann nicht in pauschaler Weise geltend gemacht werden; die betroffene Person muss sich vielmehr an die zuständigen Organe wenden und die Daten, welche der Sperrung unterliegen sollen, genau bezeichnen.

Eine Sperrung der Bekanntgabe kann nicht jedermann verlangen, sondern nur eine betroffene Person, die ein schutzwürdiges Interesse glaubhaft macht (z.B. wenn durch die Datenbekanntgabe das Risiko von Belästigungen, Repressionen oder gar Verfolgungen resultieren würde).

Abs. 2: Das Gesetz legt auch fest, unter welchen Voraussetzungen die Sperrung durchbrochen werden darf.

Art. 28 *b. Wiederrechtliches Bearbeiten*

Art. 25 Abs. 1-3 i.V.m. Art. 37 Abs. 1 DSG
Art. 8 Bst. c ER-Konv 108
Art. 12 Bst. b EU-DSRL)

Personendaten dürfen nur rechtmässig bearbeitet werden (Art. 4 Abs.1 des Entwurfs). Werden Daten unrechtmässig bearbeitet, kann die betroffene Person verschiedene Ansprüche dagegen geltend machen: Die Ansprüche können von jedem, der sich über ein schutzwürdiges Interesse ausweist, geltend gemacht werden. Damit sind unter Umständen auch Dritte, deren eigene Personendaten nicht zur Diskussion stehen, legitimiert (z.B. im Fall der Abwesenheit oder Versterbens der betroffenen Person). Die Legitimation der Verbände richtet sich nach allgemeinen verwaltungsrechtlichen Grundsätzen (zum Ganzen vgl. BBl 1988 II II 476 f.).

Folgende Ansprüche können geltend gemacht werden:

– Unterlassung der widerrechtlichen Datenbearbeitung (z.B. durch Löschung, Sperre der Bekanntgabe);
– Beseitigung der Folgen der widerrechtlichen Bearbeitung (z.B. durch Mitteilung an Datenempfänger, Veröffentlichung, Schadenersatz, Genugtuung);
– Feststellung der Widerrechtlichkeit der Bearbeitung.

Allenfalls kann ein Feststellungsanspruch an das Vorliegen eines speziellen schutzwürdigen Interesse geknüpft werden. Bei den anderen Ansprüchen muss die Gefahr einer weiteren Bearbeitung zur Begründung genügen.

Art. 29 *Unrichtige Personendaten*

(Art. 5 Abs. 2 i.V.m. Art. 37 Abs. 1 DSG
Art.8 Bst. c ER-Konv 108
Art. 12 Bst. b und c EU-DSRL)

Abs. 1: Personendaten, die von öffentlichen Organen bearbeitet werden, müssen richtig sein, weil:

– es das Recht auf informationelle Selbstbestimmung es gebietet;
– die Bearbeitung unrichtiger Daten zur behördlichen Aufgabenerfüllung nicht verhältnismässig ist.

Dementsprechend ist die Pflicht der Datenbearbeiter, sich über die Richtigkeit und Vollständigkeit (soweit es der Bearbeitungszweck verlangt) zu vergewissern (Art. 10 des Entwurfs), ebenso wie der Anspruch der betroffenen Person auf die Berichtigung unrichtiger Daten im Gesetz verankert (bisher in Art. 13 Abs. 3 StVG).

Für die Legitimation wird auf die Ausführungen betreffend der widerrechtlichen Bearbeitung von Personendaten verwiesen.

Abs. 2: Die Bestimmung zählt – nicht abschliessend – die Ansprüche der gesuchstellenden Person auf.

Zu erwähnen ist insbesondere die Möglichkeit eines Bestreitungsvermerks (Bst. b). Dieser stellt eine besondere Art von Beweislastregel dar. Da im Verwaltungsrecht die Offi-

zialmaxime gilt, muss das öffentliche Organ, das sich mit einem datenschutzrechtlichen Begehren konfrontiert sieht, den Sachverhalt von Amtes wegen abklären (vgl. Art. 34 des Entwurfes). Dabei trifft die Parteien allerdings eine Mitwirkungspflicht. Kann die Richtigkeit von Daten nicht eindeutig festgestellt werden, die Behörde auf diese jedoch nicht einfach verzichten, besteht die Möglichkeit, einen Bestreitungsvermerk anzubringen. Damit wird dargetan, dass der Betroffene mit der Darstellung eines Sachverhalts in behördlichen Akten nicht einverstanden ist.

Wie der Bestreitungsvermerk genau auszugestalten ist (Kennzeichnung, Gegendarstellung usw.), wird die Praxis entscheiden müssen. Immerhin kann der Regierungsrat das Nähere in Ausführungsbestimmungen regeln (Art. 38 Bst. f des Entwurfes).

8.4 Organisation, Verfahren und ergänzendes Recht

Art. 30 *Beauftrage Person für Datenschutz:*
a. Wahl und Stellung

(Art. 37 Abs. 2 DSG
Präambel Abs. 2 und Art. 1 ZP zur ER-Konv 108
Art. 28 EU-DSRL)

Art. 30 – 33: Mit Verhaltensnormen allein kann kein wirkungsvoller Datenschutz geschaffen werden. Damit die datenschutzrechtlichen Grundsätze in der Rechtswirklichkeit tatsächlich beachtet werden, ist eine Aufsicht und auch eine Beratung durch ein kompetentes Organ im Gesetz ausdrücklich vorzusehen.

Abs. 1 – 3: Die rechtlichen Vorgaben verlangen ein Kontrollorgan, das seine Aufgabe "in völliger Unabhängigkeit" wahrnehmen kann.[20] Weiter verlangen sie eine wirksame und aktive Kontrolle.

Das bedingt, dass (vgl. Wegleitung KdK, Ziff. 7.5 ff. sowie Anhang, S. 23 f.):

- die Unabhängigkeit ausdrücklich im Gesetz festgehalten ist;
- die Unabhängigkeit mit institutionellen Sicherungen garantiert wird;
- das Kontrollorgan die nötigen Befugnisse besitzt;

Um die verlangte völlige Unabhängigkeit des Kontrollorgans zu gewährleisten, sind die folgenden institutionellen Garantien unabdingbar:[21]

- Budget: Das Kontrollorgan muss ein eigenes Budget für Personal- und Sachressourcen haben (inkl. der Möglichkeit, im Falle von Kapazitätsproblemen weiteres Personal oder externe Fachspezialisten anzustellen bzw. beizuziehen):
  - Die Erstellung des Budgets geschieht durch das Kontrollorgan.
  - Die Unterbreitung des Budgets dem Parlament zu Entscheid darf keine Regierungsintervention zulassen.
- Planung und Durchführung der Kontrolltätigkeit:
  - Eine wirksame, aktive Kontrolle muss anlassfrei möglich sein und aufgrund eines autonomen, aufgrund einer Risikobeurteilung erstellten Prüfprogramms erfolgen können.[22]

---

[20] Unabhängigkeit ist z.B. nicht gegeben, wenn die Exekutive das Kontrollorgan mit einem jederzeit kündbaren Arbeitsvertrag anstellt, über die Zuteilung von personellen und finanziellen Ressourcen entscheidet oder die Planung und Durchführung der Kontrolltätigkeit beeinflussen kann (vgl. die heute bestehende Regelung aufgrund von Art. 14 StVG).

[21] Zum Vergleich: Die meisten Kontrollorgane in den europäischen Staaten werden vom Parlament auf eine feste Amtsdauer gewählt, verfügen über ein eigenes Budget, das ohne Regierungsintervention vom Parlament beschlossen wird, und legen ihr Prüfungsprogramm autonom fest.

[22] Eine effektive Kontrolle ist z.B. in keiner Weise sichergestellt werden, wenn ein kantonales Kontrollorgan aufgrund seines Pensums (z.B. 20%) faktisch höchstens reaktiv tätig werden kann, wenn ein Anliegen an es herangetragen wird, wie dies heute im Kanton Obwalden der Fall ist.

  - Es bestehen umfassende Untersuchungsbefugnisse (ungeachtet allfälliger Geheimhaltungspflichten), effektive Einwirkungs-, Anzeige- und Rechtsmittelbefugnisse.
  - Kompetenz des Kontrollorgans zur Ablehnung von Sonderaufträgen, wenn diese die Realisierung des Prüfprogramms gefährden.
- Sicherung der persönlichen Unabhängigkeit:
  - Die Fachkompetenz ist Wahlvoraussetzung und Pflicht zur Erhaltung durch Fortbildung.
  - Anforderungsprofil: Persönliche Integrität.
  - Pflicht zur Offenlegung von Interessenbindungen der leitenden Person und der weiteren mit Kontrollaufgaben betrauten Mitarbeitenden zur Vermeidung von Interessenkonflikten. Nebenerwerbstätigkeiten – die zu Interessenkollisionen führen können – unterliegen einer Genehmigungspflicht.
- Wahl der leitenden Person: Eine Wahl ausschliesslich durch die Exekutive stellt eine Wahl der Kontrollierenden durch die Kontrollierten dar. Sie kann unter dem Aspekt der verlangten völligen Unabhängigkeit allerhöchstens dann genügen, wenn dieses offensichtliche Manko durch andere Sicherungen in höchster Qualität kompensiert werden kann:
  - durch ein Maximum bei den übrigen institutionellen Sicherungen (Amtsdauer und Stellung/Zuordnung des Kontrollorgans);
  - durch ein Maximum an Einwirkungsbefugnissen des Kontrollorgans;
  - durch eine Ausstattung mit entsprechenden finanziellen und personellen Ressourcen.
- Anstellungsverhältnis der leitenden Person:
  - Die leitenden Person ist auf eine feste Amtsdauer (ohne eine vorgängige ordentlichen Kündigungsmöglichkeit) anzustellen.
  - Eine Auflösung ist ausschliesslich bei schwerwiegenden Amtspflichtverletzungen in Betracht zu ziehen.
  - Die Auflösung ist gerichtlich anfechtbar zu machen.
- Aufsicht/Kontrolle:
  - Rechenschaftsablage des administrativ-finanziellen Gebarens wie durch die Gerichte.
  - Qualitätskontrollen sind nicht durch Audits der Exekutive, sondern durch parlamentarische Organe vorzunehmen, zumal eine öffentliche Kontrolle durch Veröffentlichung der Tätigkeitsberichte des Kontrollorgans stattfindet.
- Stellung: Die Zuordnung des Kontrollorgans zu einer Verwaltungseinheit kann lediglich eine organisatorische sein.

Die Form des Kontrollorgans (beauftragte Person, Kommission oder eine Kombination der beiden Formen) ist nicht vorgeschrieben, jedoch muss sich die gewählte Form an den Anforderungen an die Unabhängigkeit und Wirksamkeit der Kontrolle messen lassen.

Vorliegende Lösung sieht die Wahl einer beauftragten Person für Datenschutz vor. Wahlorgan ist der Regierungsrat. Dies insbesondere auch deshalb, weil ihm aufgrund des von der ZRK initiierten Projekts eines gemeinsamen Wahlorgans, die Kompetenz zur Zusammenarbeit mit anderen Kantonen zukommen soll (eine entsprechende Bestimmung wird nun – unabhängig des Ausgangs des Projekts – in Abs. 6 vorgesehen). Wie in den meisten Kantonen und im Bund ist die beauftragte Person für Datenschutz organisatorisch der Staatskanzlei anzugliedern (vgl. auch die Finanzkontrolle). Die Aufsicht hingegen übt der Kantonsrat aus. Zusätzlich garantiert der Verweis auf die Bestimmungen im Gerichtsorganisationsgesetz über die Gerichtsverwaltung die geforderte institutionelle Unabhängigkeit. Die Stellung der beauftragten Person (garantierte Unabhängigkeit) kann mit jener des Gerichts verglichen werden. Betreffend des personellen Aufwands geben die Ausführungen zu den "Auswirkungen" eines neuen Datenschutzgesetzes Auskunft. Diese Lösung entspricht am ehesten dem Rechtssystem des Kantons Obwalden.

Abs. 4: Das Berufsgeheimnis passt sich der Geheimhaltungsstufe der zu kontrollierenden

Daten an (vgl. auch Art. 28 Abs. 7 EU-DSRL).

Abs. 5: Es versteht sich von selbst, dass eine ausserkantonale Datenschutzstelle die Anwendung dieses Gesetzes zur Aufgabe hat. Mit Blick auf die institutionelle Unabhängigkeit müsste ein entsprechender Vertrag zumindest auf eine bestimmte Dauer unkündbar sein. Wie die geforderte aktive Datenschutzkontrolle, die Beratung oder Registerführung durch eine ausserkantonale Stelle bewerkstelligt wird und auf welche Akzeptanz sie bei den Bürgern und öffentlichen Organen innerkantonal stossen wird, wird die Praxis zeigen müssen (vgl. auch die Ausführungen zu Kapitel 5.1.4).

Art. 31 *b. Aufgaben*

(Art. 27, 30 und 31 i.V.m. Art. 37 Abs. 2 DSG
Art. 1 ZP zur ER-Konv 108
Art. 28 EU-DSRL)

Abs. 1: Die beauftragte Person für Datenschutz ist kantonales Kontrollorgan im Sinne des eidgenössischen Datenschutzgesetzes. Damit wird die Forderung aus Art. 37 Abs. 2 umgesetzt.

Abs. 2 - 3: Der beauftragten Person obliegen mindestens die folgenden gesetzlichen Aufgaben und Pflichten:

– Kontrolle (anlassfreie Kontrollen, auf Anzeige hin oder von Gesetzes wegen [z.B. Vorabkontrollen gemäss Art. 6 des Entwurfs]);
– Beratung (insbesondere in der Rechtsetzung. In der Beratung eingeschlossen ist die Schulung der öffentlichen Organe wie aber auch die Aufklärung der betroffenen Personen über ihre Rechte, da sonst das Datenschutzrecht nicht volle Wirkung erzielt);
– Behandlung von Eingaben (Anhörung und Behandlung der Beschwerden von betroffenen Personen in Bezug auf die Bearbeitung von Personendaten durch öffentliche Organe);
– Amtshilfe (Zusammenarbeit mit den Datenschutzkontrollorganen der anderen Kantone, des Bundes und des Auslands);
– Berichterstattung (Rechenschaftsablegung gegenüber der Aufsichtsbehörde betreffend die Tätigkeit, das finanzielle Gebaren usw.; periodische Informierung der Aufsichtsbehörde sowie der Öffentlichkeit über die Resultate der Kontrolltätigkeit, also über wichtige Feststellungen und Beurteilungen sowie über die Wirkung der Datenschutzbestimmungen).

Art. 32 *c. Befugnisse*

(Art. 27 i.V.m. Art. 37 Abs. 2 DSG
Art. 1 Ziff. 2 Bst. a ZP zur ER-Konv 108
Art. 28 Abs. 3 EU-DSRL)

Abs. 1: Das Kontrollorgan muss mindestens die folgenden Befugnisse besitzen:

– Umfassende Untersuchungsbefugnisse: Die Befugnis, ungeachtet allfälliger Geheimhaltungspflichten Ermittlungen durchzuführen, alle für die Erfüllung des Kontrollauftrags erforderlichen Informationen über Datenbearbeitungen einzuholen, Einsicht in alle Unterlagen zu nehmen, Besichtigungen durchzuführen und sich Bearbeitungen vorführen zu lassen.

  Gegenüber dem Kontrollorgan können sich die öffentlichen Organe nicht auf den Datenschutz berufen und die Auskünfte verweigern. Es sind umfassende Auskünfte zu erteilen.
– Effektive Einwirkungsbefugnisse: Es ist erforderlich, dass das Kontrollorgan mit den gesetzlich festgelegten Einwirkungsbefugnissen in ihrer Gesamtheit tatsächlich Wirksamkeit entfalten kann.

Dem Beauftragen für Datenschutz werden nach der hier vorgeschlagenen Lösung keine Verfügungskompetenzen oder direkten Entscheidungsbefugnisse zugeteilt. Er kann aber dem öffentlichen Organ Antrag hinsichtlich der Art und Weise der Personendatenbearbeitung stellen. Wird dem Antrag nicht vollumfänglich entsprochen, erlässt das öffentliche Organ oder die übergeordnete Behörde eine anfechtbare Verfügung. Diese kann von der

beauftragten Person für Datenschutz auf dem Beschwerdeweg angefochten werden, womit eine effektive Einwirkungsbefugnis gegeben ist.

Ähnlich verhält es sich, wenn einer betroffenen Person namentlich die Auskunft, die Einsicht oder die Erfüllung eines Anspruchs im Sinne von Art. 27 ff. des Entwurfs nicht vollumfänglich entsprochen wird. Der beauftragten Person für Datenschutz wird die anfechtbare Verfügung des öffentlichen Organs oder der übergeordnete Behörde mitgeteilt; ihr steht das Behördenbeschwerderecht zu (vgl. Art. 34 – 36 des Entwurfs).

Abs. 2: Hiezu bedarf es keiner Erläuterungen.

Abs. 3: Wichtig für die erfolgreiche Umsetzung des Datenschutzrechts ist die Unterstützung durch die öffentlichen Organe. Eine entsprechende Pflicht ist deshalb zu statuieren.

Art. 33 *Datenschutzstellen der Gemeinden*

Abs. 1: Soweit das Bedürfnis nach einer eigenen Datenschutzstelle besteht, sollen die Gemeinden durch das Datenschutzgesetz nicht in ihrer Autonomie beschränkt sein.

Abs. 2 und 4: Wichtig ist, dass die kommunalen Datenschutzstellen ihre datenschutzrechtlichen Aufgaben in Unabhängigkeit und effektiver Wirksamkeit ausüben können. Insoweit sind die Anforderungen an den Beauftragen für Datenschutz (Art. 30 – 32 des Entwurfs) sinngemäss auch bei der Einführung einer kommunalen Datenschutzstellen zu beachten.

Gegebenenfalls treten an die Stelle der beauftragten Person für Datenschutz die kommunalen Datenschutzstellen. Diese können als eine erste Anlaufstelle, insbesondere für verwaltungsinterne Fragestellungen angegangen werden. Den betroffenen Personen soll es aber freigestellt bleiben, an welche Stelle sie sich wenden möchten. Kommunale Datenschutzstellen sorgen für eine breite Verankerung des Datenschutzes innerhalb des Kantons.

Die Wahrung eines einheitlichen Datenschutzes innerhalb des Kantons wird mittels Aufsicht durch die beauftragte Person für Datenschutz gewährleistet, welcher die kommunalen Datenschutzstellen auch schult.

Abs. 3: Da dem Regierungsrat die Aufsicht über die Gemeinden obliegt, entscheidet er, freilich nach Anhörung der beauftragten Person für Datenschutz, die das kommunale Konzept in Bezug auf die Sicherstellung der effektiven Aufgabenerfüllung prüft, über die Einsetzung einer kommunalen Datenschutzstelle.

Abs. 4: Hiezu bedarf es keiner Erläuterungen.

Art. 34 *Verfahren:*
a. Allgemein

Das Verfahren richtet sich nach dem StVG und seinen Ausführungserlassen, namentlich der Verordnung über das Verwaltungs- und Verwaltungsbeschwerdeverfahren vom 29. Januar 1998 (VwVV; GDB 133.21).

Art. 35 *b. Anspruch auf Massnahmen*

Die beauftragte Person für Datenschutz hat die Aufgabe, im Streitfall zwischen den öffentlichen Organen und den betroffenen Personen zu vermitteln (Art. 32 Abs. 2 Bst. b des Entwurfes). Allerdings wird auf die Ausgestaltung eines formellen Schlichtungsverfahrens verzichtet.

Im Übrigen wird auf die Ausführungen zu Art. 32 Abs. 1 des Entwurfs verwiesen.

Art. 36 *c. Aufsicht über die öffentlichen Organe*

Abs. 1 und 2: Hiezu bedarf es keiner Erläuterungen.

Abs. 2 und 3: Es wird auf die Ausführungen zu Art. 32 Abs. 1 des Entwurfs verwiesen.

Abs. 5: Nach Art. 67 Abs. 3 Bst. b StVG ist jede andere Person, Organisation oder Behörde, die durch die Gesetzgebung dazu ermächtigt ist, zur Beschwerde berechtigt. Insoweit ist das Beschwerderecht der beauftragten Person für Datenschutz (Behördenbe-

schwerde) explizit in der Gesetzgebung zu statuieren. Darüber hinausgehende Zivil- oder Strafklagerechte erscheinen nicht notwendig, zumal der beauftragten Person für Datenschutz das (Straf-)Anzeigerecht zusteht. Im Übrigen wird auf die Ausführungen zu Art. 32 Abs. 1 verwiesen.

Art. 37 *Kosten*

(Art. 8 Abs. 5 DSG i.V.m. Art. 37 Abs. 1 DSG
Art. 8 Bst. b ER-Konv 108
Art. 12 Bst. a EU-DSRL)

Das Recht auf Auskunft und Einsicht ist eine der wichtigsten Ausflüsse des verfassungsrechtlichen Persönlichkeitsschutzes. Es darf nicht durch eine übermässige Kostenbeteiligung der betroffenen Person erschwert oder gar vereitelt werden. Es ist deshalb im Gesetz festzuhalten, dass Auskunft und Einsicht in der Regel, d.h. für einen durchschnittlichen Arbeitsaufwand wie für das Hervorsuchen des Dossiers, einfaches Kopieren usw. kostenlos ist.

Der Regierungsrat kann das Nähere in Ausführungsbestimmungen regeln, mithin also die Kosten für einen überdurchschnittlichen Arbeitsaufwand bei der Erteilung von Auskunft und Einsicht, aber auch andere Kosten, die im Zusammenhang mit der Anwendung des Datenschutzgesetzes anfallen (vgl. z.B. Art. 12 Abs. 2 StVG).

Art. 38 *Ergänzendes Recht:*
a. Ausführungsbestimmungen

Der Regierungsrat kann mittels Ausführungsbestimmungen die zum Vollzug erforderlichen Bestimmungen erlassen und namentlich folgende Bereiche näher regeln:

– die Voraussetzungen der Ausnahmebewilligung für das Bearbeiten von besonders schützenswerten Personendaten und Persönlichkeitsprofilen;
– die Verantwortlichkeit bei gemeinsamer Datenbearbeitung mehrerer öffentlicher Organe;
– den sicheren Umgang mit Personendaten;
– die Modalitäten des Zugangs zum Register der Datensammlungen;
– die Modalitäten des Auskunftsrechts gegenüber den Inhabern der Datensammlungen;
– die Modalitäten der Anspruchserhebung und Umsetzung der Massnahmen im Sinne von Art. 27 ff. diese Entwurfs;
– die Kosten (z.B. wenn die Ausübung des Auskunfts- und Einsichtsrecht das übliche Mass übersteigt usw.).

Art. 39 *b. Verweis*

Das Datenschutzgesetz kann nicht jede Problemstellung vorsehen, die sich in der Praxis ergeben wird. Wenn es in Bezug auf bestimmte Fragen lückenhaft sein sollte, dann rechtfertigt es sich, sinngemäss die ausführlicheren Bestimmungen des eidgenössischen Datenschutzgesetztes sowie deren Auslegung heranzuziehen, woraus unter Umständen eine Lösung entnommen werden kann.

8.5 Strafbestimmungen

Art. 40 *Strafbestimmungen*

(Art. 24 EU-DSRL)

Die Auslagerung der Datenbearbeitung an Dritte hat in den letzten Jahren zugenommen – mit anhaltendem Trend. Der vorliegende Entwurf bewirkt, dass das Anliegen des Datenschutzes bei den öffentlichen Organen wesentlich besser verankert sein wird, als dies in der Privatwirtschaft der Fall ist.

Wird die Datenbearbeitung an Private ausgelagert, so ist mit verschiedenen Mitteln dafür zu sorgen, dass den datenschutzrechtlichen Anliegen mit der gleichen Sorgfalt nachge-

lebt wird. Neben vertraglichen Abmachungen (vgl. Art. 8 des Entwurfs), die für den Fall vertragswidrigen Verhaltens ausdrücklich auf Konventionalstrafe, Schadenersatz- und Genugtuungsansprüche verweisen können, haben sich im Bund und in anderen Kantonen auch explizite Strafbestimmungen als hilfreich erwiesen. Die betreffenden Personen in den öffentlichen Organen wie auch die beauftragte Person für Datenschutz selbst (inkl. Hilfspersonen) unterliegen den Bestimmungen des Schweizerisches Strafgesetzbuches vom 21. Dezember 1937 (StGB; SR 311.0). Weiterer Schutzmassnahmen bedarf es nicht.

8.6 Übergangs- und Schlussbestimmungen

Art. 41 *Übergangsbestimmungen*

Abs. 1: Hiezu bedarf es keiner Erläuterungen.

Abs. 2: Die neue Gesetzgebung soll möglichst reibungslos, jedoch mit Rücksicht auf die bearbeitenden öffentlichen Organe, eingeführt werden. Da für diese die Anpassung an das neue Recht ein erheblicher Aufwand bedeutet und allenfalls bereichsspezifische Grundlagen erst geschaffen werden müssen, rechtfertigt sich für die Inhaber von Datensammlungen die Einräumung einer angemessenen Frist.

Art. 42 *Änderung bisherigen Rechts*

Mit der Einführung eines Datenschutzgesetzes können Art. 8 ff. StVG aufgehoben werden; es ist auch der Geltungsbereich anzupassen.

Art. 11 StVG wird nunmehr direkt in der Einwohnerkontrollverordnung[23] verankert.

Die Weitergabe von besonders schützenswerten Personendaten an ein Drittsystem durch die Polizei (Art. 8b Abs. 2 Bst. b StPO) ist nicht mehr durch den Regierungsrat, sondern durch die beauftragte Person für Datenschutz im Sinne von Art. 6 des Entwurfs vorzuprüfen.

Die übrigen Änderungen bedürfen keiner Erläuterungen.

Art. 43 *Inkrafttreten*

Hiezu bedarf es keiner Erläuterungen.

9. Auswirkungen

Das kantonale Datenschutzrecht sowie die Organisation des Datenschutzorgans genügen dem internationalen und nationalen Rechtsstandard nicht mehr. Auch mit Blick auf die zur Verfügung stehenden personellen Ressourcen ist es für das Datenschutzorgan unmöglich geworden, unter den Bedingungen und Voraussetzungen von damals die vermehrten Bedürfnisse von Bevölkerung und Verwaltung nach Beratung und Klärung zu bearbeiten.

Der notwendig gewordene Erlass eines kantonalen Datenschutzgesetzes, insbesondere die Institutionalisierung einer Aufsichtsstelle, wird zwangsläufig erhebliche Mehraufwendungen mit sich bringen. Dies ist insbesondere eine Folge des Anschlusses an Schengen/Dublin. Denn solange die Schweiz auf Bundes-, kantonaler und kommunaler Ebene keinen hinreichenden und flächendeckenden Datenschutz gewährleisten kann, so lange wird die EU den Anschluss an seine Informationssysteme nicht freigeben.

Die finanziellen Auswirkungen können nicht abschliessend abgeschätzt werden, zumal – im Gegensatz zu anderen Kantonen – zunächst noch ein Nachholbedarf besteht (z.B. Erstellung der Register der Datensammlungen).

Die Wegleitung der KdK (Ziff. 7.7) geht davon aus, dass für eine wirksame Datenschutzaufsicht – ohne Infrastrukturkosten – folgende personelle Ressourcen zur Verfügung ste-

[23] Einwohnerkontrollverordnung vom 22. November 1996 (GDB 113.11).

hen müssen:

– grössere und mittlere Kantone: mehrere 100 Stellenprozente;
– kleinere Kantone: mindestens 50 – 100 Stellenprozente.

Berücksichtigt man, dass die Aufsichtsstelle nicht nur für den Kanton, sondern auch für die Gemeinden tätig sein wird – soweit diese keine eigenen Datenschutzstellen einrichten – so kann nicht vom absoluten Minimum ausgegangen werden.

Die Wegleitung der KdK schlägt als alternative Möglichkeit die staatsvertragliche Übertragung der Datenschutzaufsicht durch kleinere Kantone an einen Kanton mit einer ausgebauten Datenschutzaufsicht oder mittelfristig allenfalls gemeinsame regionale Lösungen verschiedener (kleinerer) Kantone vor.

Im Fall einer interkantonalen Lösung könnten aller Voraussicht nach die Kosten nicht massgeblich gesenkt werden. Zu den Vor- und Nachteilen vgl. die Ausführungen unter Ziff. 5.1.4.

Beilagen zur Botschaft

– Entwurf zu einem neuen ...