Botschaft des Regierungsrats zum Entwurf eines Gesetzes über den Datenschutz

vom 24. September 2007

Herr Präsident
Sehr geehrte Damen und Herren

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

Sarnen, 24. September 2007

Im Namen des Regierungsrats

Landammann: Hans Hofer
Landschreiber: Urs Wallimann

G-Nr. 20070241

Inhaltsverzeichnis

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 kam bisher mit einem Minimalstandard an allgemeinen Datenschutzvorschriften im Staatsverwaltungsgesetz aus. Die neuen internationalen und nationalen Rechtsgrundlagen im Datenschutzbereich erfordern nun aber, sich an den entsprechenden Standard anzupassen. Deshalb ist die datenschutzrechtliche Materie im Rahmen eines selbstständigen Datenschutzgesetzes als Querschnittsgesetzgebung neu zu regeln. Daneben bleiben besondere Datenschutzvorschriften in Sachgesetznormen bestehen.

Der einzuführende allgemeine 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 Entwurf zu einem kantonalen Datenschutzgesetz verzichtet einerseits im materiellen Recht weit gehend auf eine eigenständige Regelung und verweist auf das Datenschutzrecht des Bundes, das auch im übertragenen Vollzugsbereich im Kanton zur Anwendung kommt. Er regelt aber anderseits das notwendige kantonale Organisationsrecht zur institutionellen Sicherung des Datenschutzauftrags in Kanton und Gemeinden. Der internationale Standard verpflichtet die Kantone, eine Kontrollbehörde mit ausreichenden Aufgaben und Befugnissen einzurichten. Die Kontrollbehörde muss unabhängig und wirksam arbeiten können. Dies bedingt einerseits die notwendigen institutionellen Garantien wie auch die erforderlichen personellen und finanziellen Ressourcen im kantonalen Recht. 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, in Zusammenarbeit mit anderen Kantonen gemeinsam ein unabhängiges Datenschutzorgan zu errichten. Dazu stehen im Rahmen der Zentralschweizerischen

Regierungskonferenz (ZRK) verschiedene Projekte betreffend eines gemeinsamen Kontrollorgans in Prüfung.

1. Auftrag

In der integrierten Aufgaben- und Finanzplanung (IAFP) 2007 bis 2010 ist unter dem Sicherheits- und Gesundheitsdepartement bei der Justizverwaltung 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) und 11. September 2007 (Nr. 99) tat der Regierungsrat sein Interesse , an einem 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.

2. Evaluation durch EU

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[1], 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 und beinhaltet die Beantwortung eines Fragebogens sowie die Prüfung der Umsetzung vor Ort.

Der momentan gültige Zeitplan des Bundes besagt, dass die Evaluation etwa Ende 2007 beginnen und im Frühsommer 2008 mit dem Inkraftsetzungsbeschluss durch den EU-Rat (Feststellung der Erfüllung des Schengen/Dublin-Standards) ihren Abschluss finden soll. Im Herbst 2008 soll dann die Inkraftsetzung der Assoziierungsabkommen (auf den Flugplanwechsel hin) geschehen.

Wenn die Schweiz voraussichtlich gegen Ende 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 etwa, dass spätestens dann eine gesetzliche Regelung von der vorberatenden Kommission des Kantonsrats behandelt sein muss.

3. Ausgangslage

3.1 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 Über-

[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).

einkommen 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), 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 aus dieser Zeit; vereinzelte Datenschutzbestimmungen bestanden bereits im kantonalen Recht[2].

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)[3] 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, sodass 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[4]. Es ist beabsichtigt, die Revision Mitte 2007 in Kraft zu setzen.

3.2 Die Assoziierung der Besitzstände[5] von Schengen und Dublin (Datenschutz)

3.2.1 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 Asylbewer-

---

[2] Der Entwurf des Regierungsrats 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.

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

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

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

ber 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 allgemeine EU-DSRL[6] zur Anwendung. Mit der Assoziierung an Schengen und Dublin entfalten diese Vorschriften auch für die Schweiz Wirkung.

3.2.2 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[7] 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 bis 118 SDÜ und für den Datenaustausch ausserhalb des SIS die Art. 126 bis 130 SDÜ.

3.2.3 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:

---

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

[7] 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 bis 28 des Vertrags über die Europäische Union, EUV) und der dritte Pfeiler umfasst die polizeiliche und justizielle Zusammenarbeit in Strafsachen (Art. 29 bis 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.).

- 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.

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

3.2.4 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 konkretisiert 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.).

3.3 ER-Konv 108 und Zusatzprotokoll

3.3.1 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. Anderseits 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).

3.3.2 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.

3.4 Revision des DSG[8]

Auslöser der Revision waren:

– zwei im Jahre 1999 bzw. 2000 von den Eidgenössischen Räten angenommene Motionen zum Datenschutz[9];
– 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:

---

[8] Vgl. BBl 2003 2101 ff.

[9] 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 anderseits 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.

– Generell: Annäherung des schweizerischen Rechts an das Recht der Europäischen Union[10];
– Beschaffung und Bekanntgabe von Personendaten;
– Information und Rechte der Personen, deren Daten bearbeitet werden;
– Verantwortlichkeiten und Kontrolle bei der Delegation der Bearbeitung an Dritte;
– Kontrolle der Einhaltung des Datenschutzes;
– Festlegung eines minimalen Schutzstandards bei der Verarbeitung von Daten durch kantonale Behörden beim Vollzug von Bundesrecht.

4. Regelungsnotwendigkeit und Regelungsbedarf

4.1 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);
– Projekte im Umfeld der ZRK betreffend eines gemeinsamen Datenschutzorgans.

Ein darüber hinausgehender Regelungsbedarf besteht aus kantonaler Sicht nicht.

4.2 Regelungsbedarf aufgrund des internationalen Rechts[11]

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[12];
– bei dem die kantonalen Behörden und Amtsstellen nicht im Rahmen des Vollzugs von Bundesrecht tätig werden (vgl. nachstehend Kap. 4.3)

hat folgenden Datenschutzstandard einzuhalten:

---

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

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

[12] Z.B. Bei der Bearbeitung von Personendaten im Rahmen der polizeilichen Zusammenarbeit (dritter Pfeiler der EU), gelangen primär die Art. 102 bis 118 SDÜ und Art. 126 bis 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).

– 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.

Das kantonale Recht hat deshalb den europäischen Datenschutzstandard zu erfüllen.

4.3 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).

4.4 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.

4.5 Wegleitung der KdK[13] 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 Kantonsregierungen (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.

Die Wegleitung diente als Grundlage für den Entwurf des neuen kantonalen Datenschutzgesetzes.

---

[13] Konferenz der Kantonsregierungen

5. Konzept des kantonalen Gesetzesentwurfs

5.1 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 sein.

5.1.1 Erfordernis der formell-gesetzlichen Regelung

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.

Mit den materiellen Grundregeln des Datenschutzes (insbesondere mit den Grundsätzen des Bearbeitens von Personendaten und den Rechten der betroffenen Personen) werden Rechte und Pflichten von Privaten betroffen. Die Datenschutzgesetzgebung stellt auch einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar. Die organisatorisch-institutionellen Regeln (insbesondere zum Verfahren zur Durchsetzung der Rechte der betroffenen Personen sowie zur Sicherstellung der Unabhängigkeit und Wirksamkeit der Datenschutzkontrolle) stellen Grundzüge von Organisation und Verfahren in Kanton und Gemeinden dar. Das Datenschutzrecht ist deshalb auf (formell-)gesetzlicher Stufe zu regeln.

(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.)

5.1.2 Systematische und inhaltliche Eingliederung ins kantonale Recht

Das heute geltende Datenschutzrecht des Kantons Obwalden ist primär in Art. 8 bis 14 Staatsverwaltungsgesetz (StVG; GDB 130.1) geregelt.

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

5.1.3 Ausführungsbestimmungen

Im Rahmen des Datenschutzgesetzes soll der Regierungsrat die Kompetenz erhalten, auf dem Weg der Ausführungsbestimmungen bestimmte Bereiche, insbesondere zur Sicherstellung der Anwendung, näher zu regeln. Damit kann auch dem sich entwickelnden Bedürfnis der Bevölkerung nach Transparenz, Einsicht und Auskunft im Zusammenhang mit Datenbearbeitungen durch öffentliche Organe organisatorisch und administrativ Rechnung getragen werden.

5.1.4 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 wurden im Umfeld der Zentralschweizerischen Regierungskonferenz (ZRK) verschiedene Zusammenarbeitsprojekte initiiert, die eine gemeinsame, unabhängige Datenschutzstelle zum Ziel hatten bzw. haben (die Kantone Luzern und Zug nehmen an den Projekten nicht mehr teil; sie haben die Möglichkeit der eigenständigen Lösung bzw. besondere Rahmenbedingungen).

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 sowie jene der Stellvertretung gesichert. Im Vergleich zu einer kantonalen Datenschutzaufsicht sind allerdings eine geringere Nähe zu den Bürgern und Verwaltungen sowie grössere Reisewege in Kauf zu nehmen.

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

5.2 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.

5.2.1 Umfassende Verweisung auf das DSG des Bundes im materiellen Recht; Wegleitung der KdK

Der vorliegende Entwurf verweist im materiellen Recht allgemein auf das Bundesrecht. Er regelt materiell nur jene Punkte, für welche nicht auf die Bundesgesetzgebung verwiesen werden kann. Demgemäss haben die öffentlichen Organe wie auch die Bürger zur Feststellung ihrer Rechte und Pflichten das eidgenössische Datenschutzgesetz heranzuziehen. Dies müssen die Kantone und Gemeinden bereits heute in jenen Bereichen, in welchen sie Bundesrecht vollziehen. Künftig müssen sie in der Regel in Bezug auf die materiellen Bestimmungen nicht mehr unterscheiden ob sie Bundes- oder kantonales Recht anwenden.

Dieses Vorgehen garantiert, dass im Kanton Obwalden stets der bundesrechtliche Datenschutzstandard gilt, der auch dem Schengen/Dublin-Standard entspricht. Damit dürften auch die Anforderungen aus der Wegleitung der KdK erfüllt sein.

5.2.2 Eigenständiges kantonales Organisations- und ergänzendes Recht

Die institutionellen Aspekte, das heisst namentlich Organisation und Verfahren für die Durchführung des Datenschutzes in Kanton und Gemeinden sind im Rahmen des kantonalen Organisationsrechts (Kantonsverfassung, Staatsverwaltungsgesetz, Gerichtsorganisationsgesetz) zu regeln.

Auch wo nicht auf die Bundsgesetzgebung verwiesen werden konnte und eigenständige Lösungen entworfen werden mussten, wurden folgende Quellen 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.

6. Vernehmlassungsverfahren

Mit Schreiben vom 11. Mai 2007 lud das Sicherheits- und Gesundheitsdepartement, vertreten durch die Justizverwaltung, die im Kantonsparlament vertretenen politischen Parteien, die Gemeinden, den Unterwaldner Anwaltsverband sowie die interessierten Amtsstellen (Departemente, Gerichtsbehörden usw.) ein, zum Entwurf bis 13. Juli 2007 Stellung zu nehmen.

Es haben inhaltlich Stellung genommen: die Parteien CVP, CSP, SVP, der Anwaltsverband Unterwalden (UAV), die Einwohnergemeinden (Gden.; ohne Lungern), das Volkswirtschaftsdepartement (VD), das Finanzdepartement (FD), das Informatikleistungszentrum (ILZ), das Polizeikommando (KAPO), die Staatskanzlei (STK), die Staatsanwaltschaft samt Verhöramt (Stawa/VA), das Sozialamt (SA) sowie das Gesundheitsamt (GA).

Allgemein würdigte die Mehrheit der Teilnehmer die Entwürfe positiv bzw. als ausreichend, sachgerecht und notwendig (CSP, SVP, SA, GA, FD). Der sorgfältig ausgearbeitete Entwurf und der ausführliche Bericht wurden gewürdigt, da damit mögliche Konflikte von vornherein beseitigt würden (UAV). Eine Minderheit der Teilnehmer sah keinen Handlungsbedarf (Gden., UAV) oder regte die konsequente Verweisung auf das materielle Bundesrecht an (VD, STK). Für andere Teilnehmer war die Beurteilung der Vorlagen mangels Unterlagen oder Sachkenntnisse nicht möglich (Gden., VD). Einige Teilnehmer forderten den Einbezug in das Anschlussgesetzgebungsverfahren (Ausführungsbestimmungen; ILZ, Gden.).

Nebst vielen Praxisfragen wurden auch zahlreiche Verbesserungs- und Änderungsbegehren eingereicht, die vor allem Detailpunkte betrafen. Die Justizverwaltung wertete die Antworten tabellarisch aus und hat Bericht und Entwürfe entsprechend angepasst. Die wichtigsten Vernehmlassungspunkte seien nachfolgend erwähnt:

Zweck, Geltungsbereich und Begriffe: Es wurde verlangt, dass der Gemeinderat aus dem Geltungsbereich heraus zu nehmen ist (Gden.), dagegen aber das ILZ klar zu erfassen sei (SVP, ILZ). Auch wurde angeregt, die Begriffe im Gesetz selber zu definieren (SVP).

Bearbeiten von Personendaten/Allgemeine Bestimmungen: Unklar war der Zeitpunkt sowie die Anwendung der Vorprüfung (ILZ, KAPO). Weiter wurden Fragen nach der Verantwortlichkeit bei gemeinsamer Datenbearbeitung aufgeworfen; dabei wurde die Wichtigkeit von regierungsrätlichen Ausführungsbestimmungen betont. Die Datensicherheit soll klarer und ausführlicher beschrieben werden. Unklar sei, ob die Löschung von elektronischen Daten genügend geregelt sei (SVP, ILZ).

Bekanntgabe von Personendaten: Es wurde gefordert, dass Personendaten und insbesondere Heimatort und Staatsangehörigkeit bei der Einwohnerkontrolle eingesehen werden können; auch die Möglichkeit von Nachforschungsbegehren müsse im beschränkten Rahmen möglich sein (ILZ, CVP).

Besondere Formen der Personendatenbearbeitung: Die Möglichkeit der Videoüberwachung wurde begrüsst (Gden.).

Rechte der betroffenen Personen: Das Register der Datensammlungen müsse in Obwalden einsehbar sein, auch bei einem interkantonalen Datenschutzorgan (CSP). Der Inhalt des Registers soll im Gesetz definiert werden (SVP, ILZ).

Organisation, Verfahren und ergänzendes Recht: Eine interkantonale Lösung für die Besetzung des Datenschutzorgans wurde begrüsst (Gden., UAV, FD, CVP, SVP, VD). Die Kosten hierfür seien vom Kanton zu tragen (Gden.). Die Wahl des Organs sei vom Kan-

tonsrat vorzunehmen (STK), allerdings sei die Kontrolle durch den Kantonsrat aus praktischer Sicht schwierig (CVP). Es wurde gefragt, weshalb in Bezug auf die Befugnisse des Organs nicht Art. 27 DSG übernommen worden sei, der offenbar weniger weit gehe (CSP). Die Statuierung einer freiwilligen Datenschutzstelle der Gemeinden wurde von einer Mehrheit der Teilnehmer nicht als notwendig erachtet (CSP, SVP Gden., UAV, STK). Die Kosten für Auskünfte und Einsicht seien konkret im Gesetz zu regeln bzw. in Einklang mit dem Allgemeinen Gebührengesetz zu bringen (ILZ, SVP).

Strafbestimmungen: Im Vergehensbereich seien nicht Bussen, sondern Geldstrafen zu statuieren (Stawa/VA).

7. Erläuterungen zu den einzelnen Artikeln des Datenschutzgesetzes

7.1 Geltungsbereich

Art. 1 *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 und 2: 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. 3: 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 (insbesondere zur Beschaffung und Bekanntgabe von Personendaten sowie zu den Rechten der betroffenen Personen und zur Aufsicht) enthalten.

  Gleiches gilt für die Verwaltungsrechtspflege, d.h. 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. c: 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.
– Bst. d: 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. e: 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. 4: Beim Datenschutzgesetz handelt es sich um eine Querschnittsgesetzgebung, die als „allgemeiner Teil" für alle Datenschutzvorschriften im ganzen kantonalen Recht gilt. Daneben bleiben Datenschutzregelungen in der Sachgesetzgebung, die den Datenschutz für einen konkreten Bereich regeln, vorbehalten.

7.2 Allgemeine Datenschutzbestimmungen

Art. 2 *Grundsätze*

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

Abs. 1: Keine Bemerkungen.

Abs. 2: 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.

Namentlich bei automatisierten Datenverarbeitungssystemen oder Abrufverfahren verwenden oft mehrere Organe, evt. 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 anderseits, dass das hauptverantwortliche Organ der Datensammlung für die Weiterbearbeitung eines beteiligten Organs verantwortlich gemacht wird.

Art. 3 *Datenquellen*

(Art. 4 Abs. 2 und 4 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.

Abs. 3: 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 Erkennbarkeit 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: Abs. 3 stellt eine Konkretisierung des Grundsatzes dar, dass eine Bearbeitung nach Treu und Glauben zu erfolgen hat. Die Pflicht, Daten primär bei der betroffenen Person zu erheben (Abs. 1), wurde dem Grundsatz der Erkennbarkeit (Abs. 3) 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. 4 *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. 4 statuiert den Grundsatz der Vorabkontrolle sowie die Pflicht der öffentlichen Organe, heikle Bearbeitungen durch die beauftragte Person für Datenschutz prüfen zu lassen.

Art. 5 *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[14] sind.

Abs. 3: 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.

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

Art. 6 *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, sodass 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.

Art. 7 *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 Fall 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. Zudem ist die Öffentlichkeit mit Hinweistafeln auf den Einsatz von Überwachungsmassnahmen aufmerksam zu machen.

7.3 Organisation und Verfahren

Art. 8 *Regierungsrat*

Abs. 1 und 2: Keine Bemerkungen.

Art. 9 *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)

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 bis 3: Die rechtlichen Vorgaben verlangen ein Kontrollorgan, das seine Aufgabe „in völliger Unabhängigkeit“ wahrnehmen kann[15]. 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[16]:

- Budget: Das Kontrollorgan muss ein eigenes Budget für Personal- und Sachressourcen haben (inkl. der Möglichkeit, im Fall von Kapazitätsproblemen weiteres Personal oder externe Fachspezialisten anzustellen bzw. beizuziehen):
  - Die Erstellung des Budgets geschieht durch das Kontrollorgan.
  - Dieses unterbreitet das Budget unmittelbar dem Kantonsrat zum Entscheid.
- Planung und Durchführung der Kontrolltätigkeit:
  - Eine wirksame, aktive Kontrolle muss anlassfrei möglich sein und aufgrund eines autonomen, aufgrund einer Risikobeurteilung erstellten Prüfprogramms erfolgen können[17].
  - 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.

---

[15] 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).

[16] 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.

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

  - 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. Deshalb ist eine Wahl durch den Kantonsrat zu bevorzugen.
- Anstellungsverhältnis der leitenden Person:
  - Die leitende Person ist auf eine feste Amtsdauer anzustellen.
  - Eine Auflösung ist ausschliesslich bei schwerwiegenden Amtspflichtverletzungen in Betracht zu ziehen.
  - Die Auflösung ist gerichtlich anfechtbar.
- 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 Grundsätzen der Unabhängigkeit und Wirksamkeit der Kontrolle messen lassen.

Vorliegende Lösung sieht die Wahl einer beauftragten Person für Datenschutz vor. Wahl- und Aufsichtsorgan ist der Kantonsrat. 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. Wie in den meisten Kantonen und im Bund ist die beauftragte Person für Datenschutz organisatorisch der Staatskanzlei anzugliedern (vgl. auch die Finanzkontrolle).

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: Allgemein wurde im Vernehmlassungsverfahren gefordert, dass eine Zusammenarbeit mit den Kantonen der ZRK anzustreben sei. 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). Im Vernehmlassungsverfahren wurde gefordert, dass das Register der Datensammlungen vor Ort, d.h. in Obwalden einsehbar sein müsse.

Art. 10 *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 und kommunales Kontrollorgan im Sinne des eidgenössischen Datenschutzgesetzes. Damit wird die Forderung aus Art. 37 Abs. 2 umgesetzt.

Abs. 2 bis 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);
– 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. 11 *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 ganz oder teilweise verweigert wird. Der beauftragten Person für Datenschutz wird die anfechtbare Verfügung des öffentlichen Organs oder der übergeordnete Behörde mitgeteilt; ihr steht das Behördenbeschwerderecht zu.

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. 12 *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. 13 *b. Anspruch auf Massnahmen*

Die beauftragte Person für Datenschutz hat die Aufgabe, im Streitfall zwischen den öffentlichen Organen und den betroffenen Personen zu vermitteln. Allerdings wird auf die Ausgestaltung eines formellen Schlichtungsverfahrens verzichtet.

Im Übrigen wird auf die Ausführungen zu Art. 11 des Entwurfs verwiesen.

Art. 14 *c. Aufsicht über die öffentlichen Organe*

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

Abs. 3 und 4: Es wird auf die Ausführungen zu Art. 11 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 (Behördenbeschwerde) ausdrücklich in der Gesetzgebung zu statuieren. Darüber hinausgehende Zivil- oder Strafklagerechte erscheinen nicht notwendig, zumal der beauftragten Person für Datenschutz das (Straf-)Anzeigerecht zusteht.

Art. 15 *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. den heute noch geltenden Art. 12 Abs. 2 StVG).

7.4 Übergangs- und Schlussbestimmungen

Art. 16 *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 nachgelebt wird. Neben vertraglichen Abmachungen, die für den Fall vertragswidrigen Verhaltens ausdrücklich auf Konventionalstrafe, Schadenersatz- und Genugtuungsansprüche verweisen können, haben sich im Bund und in anderen Kantonen auch ausdrückliche 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 Schweizerischen Strafgesetzbuchs vom 21. Dezember 1937 (StGB; SR 311.0). Weiterer Schutzmassnahmen bedarf es nicht.

Art. 17 *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. 18 *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[18] 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 vorzuprüfen.

Die übrigen Änderungen bedürfen keiner Erläuterungen.

Art. 19 *Inkrafttreten*

Hiezu bedarf es keiner Erläuterungen.

8. 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 ihre 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 stehen müssen:

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

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 Umfeld der ZRK sind entsprechende Zusammenarbeitsprojekte initiiert worden und noch im Gange. Zu den Vor- und Nachteilen einer interkantonale Zusammenarbeit vgl. die Ausführungen unter Ziff. 5.1.4.

Im IAFP 2008 bis 2011 ist beim Kantonsrat für eine unabhängige Datenschutzstelle (in interkantonaler Zusammenarbeit) vorsorglicherweise für 2008 ein Betrag von Fr. 20 000.– aufgenommen worden.

---

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