



KANTON
NIDWALDEN

REGIERUNGSRAT

GESETZ ÜBER DEN DATENSCHUTZ (KANTONALES DATENSCHUTZ- GESETZ)

BERICHT AN DEN LANDRAT

1	Zusammenfassung	4
1.1	Vorgaben der Europäischen Union	4
1.2	Anpassung an das Bundesrecht	4
2	Ausgangslage	4
2.1	EU-Recht	4
2.2	Verpflichtung zur Umsetzung	4
2.3	Bundesdatenschutzgesetzgebung	5
2.4	Notwendigkeit	5
3	Datenschutz im Archivwesen	6
4	Ergebnis der Vernehmlassung	7
5	Erläuterungen zu den einzelnen Bestimmungen	7
5.1	Allgemeines	7
5.2	Im Einzelnen	7
6	Auswirkungen der Vorlage	24
6.1	Auf den Kanton	24
6.2	Auf die Gemeinden	25
7	Antrag	25

1 Zusammenfassung

1.1 Vorgaben der Europäischen Union

Von der Schweiz ratifizierte Übereinkommen/Konventionen der Europäischen Union (EU) und die bilateralen Abkommen der Schweiz mit der EU über die Assoziierung mit Schengen/Dublin verlangen einen gewissen Standard in Sachen Datenschutz. Begründet wird dies insbesondere mit dem Anschluss der Schweiz an das Schengener Informationssystem SIS. Zentral ist dabei insbesondere die Ausgestaltung der Datenschutzkontrollstelle hinsichtlich Unabhängigkeit, Interventionsmöglichkeit sowie personeller und ressourcenmässiger Ausstattung.

1.2 Anpassung an das Bundesrecht

Um eine kohärente Gesetzgebung zu schaffen, wird das erstmalige kantonale Datenschutzgesetz grossmehrheitlich an die bundesrechtlichen Regelungen über den Datenschutz angelehnt, dies auch bereits unter Berücksichtigung der am 1. Januar 2008 in Kraft tretenden Änderung vom 24. März 2006 (siehe dazu auch die jeweiligen Verweise in den Marginalien der Gesetzesvorlage auf die entsprechende bundesrechtliche Bestimmung).

2 Ausgangslage

2.1 EU-Recht

Die Mitgliedstaaten des Europarates haben am 28. Januar 1981 das Übereinkommen zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten (STE Nr. 108; in der Folge als „ER-Konvention“ bezeichnet) beschlossen. Die Schweiz hat diese Konvention am 2. Oktober 1997 ratifiziert. Sie ist am 1. Februar 1998 in Kraft getreten. Durch die ER-Konvention verpflichtet sich die Schweiz – und mithin auch die Kantone –, den europäischen Mindeststandard des Datenschutzes auch im innerstaatlichen Recht zu gewährleisten.

Der Handlungsbedarf des kantonalen Gesetzgebers wird zudem durch die Umsetzung der bilateralen Abkommen zwischen der Schweiz und der EU über die Assoziierung an Schengen und Dublin aktuell. Diese Abkommen sehen den grenzüberschreitenden Austausch von Personendaten vor. Er ist innerhalb der EU mit der 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 (nachfolgend als „EU-Datenschutzrichtlinie“ bezeichnet) geregelt. Die Schweiz hat sich mit den erwähnten bilateralen Abkommen verpflichtet, diesen Standard ins landesinterne Recht zu übernehmen.

2.2 Verpflichtung zur Umsetzung

Das EU-Recht verpflichtet nicht nur den Bund, sondern auch die Kantone, ihre datenschutzrechtlichen Bestimmungen europakompatibel umzusetzen. Dies führt zwangsläufig dazu, dass der Kanton Nidwalden (erstmals) ein Datenschutzgesetz zu erlassen hat. Darin ist ein strikt verwaltungsunabhängiges Datenschutz – Kontrollorgan mit weitgehenden Aufgaben und wirksamen Befugnissen einzusetzen.

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. Dieses Hilfsmittel dient den Kantonen dazu, die Vollständigkeit ihrer Datenschutzgesetzgebung zu überprüfen und den noch bestehenden Handlungsbedarf im Hinblick auf ein gleichwertiges Schutzniveau festzustellen.

Durch die in den letzten Jahren intensivierte grenzüberschreitende polizeiliche Zusammenarbeit und den damit verbundenen gesteigerten Informationsaustausch legt auch die EU zunehmend grösseres Gewicht auf den Datenschutz und dessen Vollzug. Die Erfüllung der in der Wegleitung aufgeführten allgemeinen Anforderungen sind Voraussetzung, dass Bund und Kantone an die entsprechenden Informationssysteme angeschlossen werden können. Die EU wird in einer zweistufigen Evaluation überprüfen, ob die schweizerische Gesetzgebung – auf eidgenössischer wie kantonaler Stufe – dem Schengen-Standard entspricht. Danach wird vor Ort die praktische Umsetzung geprüft, wobei auch die organisatorische Umsetzung des Datenschutzes ein Prüfungsaspekt sein wird. Die europarechtlichen Vorgaben betreffen im Wesentlichen folgende Bereiche:

- Verbesserung der Unabhängigkeit und Selbstständigkeit der Aufsichtsstelle, wobei auch Gewicht auf die Ausstattung mit genügenden finanziellen und personellen Ressourcen zu legen, da nur so eine unabhängige, aktive und anlassfreie Kontrolle im Sinne der europarechtlichen Vorgaben möglich ist;
- Präzisierung der datenschutzrechtlichen Grundsätze auf Gesetzesstufe;
- Präzisierung der Informationspflichten beim Beschaffen von besonders schützenswerten Daten und Persönlichkeitsprofilen;
- Regelung der Bekanntgabe von Daten an andere Staaten;
- Präzisierung der Datenbearbeitung für nicht personenbezogene Zwecke;
- Vorabkontrolle bei der beabsichtigten Bearbeitung von Daten mit besonderen Risiken für die Rechte der betroffenen Personen, insbesondere beim Einsatz von automatisierten Verfahren der Verwaltung;
- Verbesserung des Auskunftsrechts von betroffenen Personen;
- Ausbau der Kontrollinstrumente der Aufsichtsstelle.

2.3 Bundesdatenschutzgesetzgebung

Am 1. Juli 1993 trat das Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG; SR 235.1) in Kraft und wurde letztmals am 24. März 2006 geändert. Diese Änderung tritt gemäss Bundesratsbeschluss von Ende September 2007 auf den 1. Januar 2008 in Kraft). Das DSG gilt für die Organe des Bundes sowie die privaten Personen. Auf die Behörden des Kantons und der Gemeinden ist das Bundesgesetz nur anwendbar, soweit diese Bundesrecht vollziehen und der Kanton keine eigenen Datenschutzvorschriften kennt (Art. 37 Abs. 1 DSG). Verfügt ein Kanton – wie Nidwalden – nicht über materielle eigene Datenschutzbestimmungen, kamen sie bereits bis anhin – zumindest beim Vollzug von Bundesrecht – subsidiär zum Tragen.

2.4 Notwendigkeit

Die staatlichen Organe sind für die Wahrnehmung der ihnen übertragenen hoheitlichen Aufgaben oft auf Sammlungen von Daten angewiesen. Die nach wie vor rasch fortschreitende Entwicklung im Bereich der Informatik und der Vernetzung (inner- und ausserhalb der öffentlichen Verwaltung) eröffnet neue Möglichkeiten der Datensammlung und Bearbeitung. Das Sammeln und Bearbeiten dieser Informationen

steht in einem erheblichen Spannungsverhältnis zur Privatsphäre von Personen. Diesen fehlt in der Regel die Übersicht, welche Daten der Staat über sie besitzt und welchen Gebrauch er davon macht, ob er diese beispielsweise Dritten gegen Entgelt zur Verfügung stellt. Die Zunahme der öffentlichen Aufgaben und der damit verbundene Einsatz moderner Informationstechnologien verlangen, dass die Datenverarbeitung der öffentlichen Hand rechtlich geordnet wird, womit dem Grundrecht auf Schutz vor Missbrauch von Daten Nachachtung verschafft wird. Insbesondere darf jedermann bei der Bearbeitung seiner Daten Schutz vor unzulässigen und unnötigen Eingriffen erwarten. Im Umfeld der elektronischen Verwaltung wird das Vertrauen in die öffentlichen Organe nur dann gewährleistet werden können, wenn für die einzelne Person transparent ist, was mit seinen Daten geschieht, und wie von Staats wegen sichergestellt wird, dass ihre Daten nicht anderen Zwecken als den von Rechts wegen bestimmten zugeführt werden. Darüber hinaus wird die Akzeptanz, dem Staat persönliche Daten zur Verfügung zu stellen, durch den Schutz der Integrität der Daten gestärkt. Die Schweiz kommt sodann, wie vorstehend bereits ausgeführt, zunehmend aufgrund von EU-Recht unter Druck, weil das Fehlen von Datenschutzgesetzen in einigen Kantonen kritisiert wird. Das vorliegende Datenschutzgesetz ermöglicht eine moderne, wirksame und praktikable Regelung des Datenschutzes im Kanton Nidwalden. Es lehnt sich materiell wie formell erheblich an das eidgenössische Datenschutzgesetz an. Dennoch wird es aber auch den Besonderheiten und Bedürfnissen des Kantons gerecht, vor allem was die Datenschutzkontrolle der Gemeinden betrifft.

3 **Datenschutz im Archivwesen**

Angesichts des engen sachlichen Zusammenhangs – Archivieren ist als eine weitere, wenngleich in der Regel "finale" Art der Datenbearbeitung zu sehen – soll die Änderung der massgebenden Vorschriften der Archivgesetzgebung mit dem erstmaligen Erlasse einer Datenschutzgesetzgebung einhergehen.

Die enorme Zunahme der Informationen gilt übereinstimmend als prägendes Merkmal unseres Zeitalters. Jede Institution – gleich welcher Art – ist deshalb heute verpflichtet, dafür zu sorgen, ihre Informationen effizient zu organisieren, zu bearbeiten und zu nutzen. Archive sind ein wesentlicher Bestandteil dieser Informationen. Die öffentlichen Archive dokumentieren staatliches Handeln und sollen dieses für alle Bürgerinnen und Bürger überprüfbar machen.

Die Archivierungspflicht bildet eine unabdingbare Voraussetzung für die Rechtsstaatlichkeit und für eine demokratische Verwaltungskontrolle sowie die Basis für die Aufarbeitung unserer gemeinsamen Geschichte. Amtsstellen und Gerichte haben für Sammlung, Ordnung und sichere Aufbewahrung der zu ihrem Zuständigkeitsbereich gehörenden Unterlagen zu sorgen.

Nach der geltenden Archivverordnung ist das Staatsarchiv das zentrale Archiv des Kantons Nidwalden. Die im Staatsarchiv aufbewahrten Unterlagen sind vom Zeitpunkt ihrer Anlage an gerechnet während einer Sperrfrist von 35 Jahren für die Öffentlichkeit nicht zugänglich. Für Archivgut, das besonders schützenswerte Daten enthält, musste jeweils eine Ausnahmegewilligung für eine längere Sperrfrist erteilt werden. Dies ist unbefriedigend und soll mit einer ebenfalls generellen Sperrfrist für solcherlei Daten geregelt werden. Im Ausnahmefall kann die zuständige Instanz auch weiterhin noch längere Sperrfristen anordnen können oder aber auch bei überwiegendem öffentlichem oder privatem Interessen gar vor dem Ablauf der Sperrfrist die Einsichtnahme bewilligen.

4 Ergebnis der Vernehmlassung

Für das Ergebnis der Vernehmlassung wird im Allgemeinen auf die separaten Ausführungen verwiesen.

Im Speziellen wird angemerkt, dass von Vernehmlassungsteilnehmern unter anderem die fehlende gesetzliche Regelung hinsichtlich Videoüberwachung beanstandet worden ist. Dieser Einwand wurde aufgenommen und umgesetzt. Die Einflechtung eines neuen Art. 17 über den Einsatz technischer Überwachungsgeräte hat zur Folge, dass die neue Nummerierung ab Art. 18 nicht mehr derjenigen der Vernehmlassungsvorlage entspricht.

5 Erläuterungen zu den einzelnen Bestimmungen

5.1 Allgemeines

Ein Grossteil der Vorschriften ist mehr oder weniger wörtlich der Bundesgesetzgebung über den Datenschutz (inklusive Änderung vom 24. März 2006, die aber mit Ausnahme von Art. 17a DSG [vgl. AS 2006, 4873] noch nicht in Kraft sind) nachempfunden, so dass in dieser Hinsicht – zur Entschlackung dieses Berichts – auch auf die beiden Botschaften des Bundesrates vom 10. Mai 1988 (vgl. BBl 1988, 413) und vom 19. Februar 2003 (vgl. BBl 2003, 2101) verwiesen werden kann.

5.2 Im Einzelnen

Art. 1 Zweck

Entspricht wörtlich Art. 1 DSG.

Der Datenschutz dient dem Schutz der Persönlichkeitsrechte von Bürgerinnen und Bürgern, den nicht nur die Bundesverfassung in Art. 13 Abs. 2 („Jede Person hat Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten.“), sondern auch die Nidwaldner Kantonsverfassung als grundrechtlichen Anspruch im Sinne von Art. 1 Abs. 1 („Die Freiheit und die Würde des Menschen sind unverletzlich“) garantiert. Dabei wird nicht eine Verhinderung jeglicher Bearbeitung von Daten bezweckt, sondern die Bekämpfung des Missbrauchs.

Art. 2 Geltungsbereich

Entspricht weitgehend Art. 2 DSG, bezieht sich jedoch auf die kantonalen und die kommunalen Organe.

In Abs. 1 ist der Grundsatz verankert, dass dieses Gesetz für das Bearbeiten von Daten durch kantonale und kommunale Organe gilt.

In Abs. 2 werden die in spezifischen Bereichen vorgenommenen Datenbearbeitungen vom Geltungsbereich des Gesetzes ausgenommen:

Ziff. 1:

Das Datenschutzgesetz gilt unter anderem namentlich nicht für die Nidwaldner Kantonalbank, obwohl diese eine kantonale öffentlich-rechtliche Anstalt ist (vgl. Art. 1 des Gesetzes über die Nidwaldner Kantonalbank (Kantonalbankgesetz, NG 866.1). Sie nimmt jedoch am wirtschaftlichen Wettbewerb teil und tritt dabei – ohne jegliche Verfügungskompetenz – nicht hoheitlich auf. Hinsichtlich der Nidwaldner Sachversicherung ist zu differenzieren: Wo diese im Rahmen des kantonalen Monopols als Gebäudeversicherer oder beispielsweise als „Fachstelle für Brandschutz und Feuerwehr“ auftritt, untersteht sie dem Datenschutzgesetz. Wo sie jedoch mit privaten

Versicherungsgesellschaften in Konkurrenz tritt, gelangt nicht das kantonale, sondern das Bundesgesetz über den Datenschutz zur Anwendung („private Person“ nach Art. 2 Abs. 1 lit. a DSG; gleiches gilt sinngemäss auch für die Nidwaldner Sachversicherung oder das Elektrizitätswerk Nidwalden beziehungsweise dessen Tochtergesellschaften).

Ziff. 2:

Aus rechtspolitischen Gründen – die demokratische Willensbildung soll durch den Datenschutz nicht beeinträchtigt werden – unterstehen Landrat und landrätliche Kommissionen – auf kommunaler Ebene auch die Gemeindeversammlungen beziehungsweise allfällige Einwohnerräte – den Bestimmungen des Datenschutzgesetzes nicht.

Ziff. 3:

Die aufgeführten Verfahrensgesetze regeln den Datenschutz selber. Wie mit Daten in diesen Fällen umzugehen ist, kann nur das Prozessrecht entsprechend seinen verfahrensrechtlichen Bedürfnissen normieren. Die entsprechenden Verfahrensgesetze enthalten Bestimmungen, die ebenfalls die Persönlichkeitsrechte der in ein staatliches Verfahren einbezogenen Personen zu schützen bezwecken. Dies gilt vor allem für Bestimmungen über Anhörungs-, Akteneinsichts- und Mitwirkungsrechte. Prozess- beziehungsweise Verfahrensrecht stellt so gesehen auch Datenschutzrecht dar.

Ziff. 4:

Darunter fallen vor allem das Grundbuch, das Register der Eigentumsvorbehalte, das Register für Schuldbetreibung und Konkurs, das Zivilstands- sowie das Handelsregister. Ihre Anlage, Führung und Benützung durch Dritte sind in den betreffenden bundesrechtlichen Vorschriften bereits besonders geregelt.

Ziff. 5

Nicht unter das Gesetz fallen nur Notizen, die als Gedankenstützen oder Arbeitshilfe zum ausschliesslich persönlichen Gebrauch erstellt werden. Sobald aber Handakten oder Notizen über mündlich erteilte Auskünfte sowie Besprechungsnotizen Teil der offiziellen Verfahrensakten bilden, sie mithin für das Verfahren wesentliche Handlungen, Ereignisse und dergleichen dokumentieren und damit Grundlage einer Entscheidung bilden, werden derartige Akten auch vom Akteneinsichtsrecht gemäss Art. 4 BV erfasst (vgl. etwa BGE 121 I 227) und unterstehen auch dem Geltungsbereich dieses Gesetzes.

Abs. 3 verweist auf die Vorschriften des Bundesdatenschutzrechtes für private Personen und Bundesorgane.

Art. 3 Begriffe

Entspricht weitgehend Art. 3 DSG.

Ziff. 1:

Den Schutz des Gesetzes geniessen nicht alle vom Staat bearbeiteten Informationen, sondern lediglich Personendaten, nicht dagegen Sachdaten. Sachdaten sind Daten, die nicht einer bestimmten oder bestimmbar Person zugeordnet werden können.

Da sich das Gesetz nur auf Personendaten bezieht, verwendet das Gesetz – und auch dieser Bericht – zur sprachlichen Vereinfachung ausschliesslich den Begriff „Daten“.

Die Ausdehnung des Datenschutzes von „bestimmten“ auf „bestimmbare“ Personen ist vor allem für kleinere Gemeinden von grosser Bedeutung. Immer wieder werden zwar anonymisierte Angaben gemacht, die aber bei überschaubaren Verhältnissen

Rückschlüsse auf eine bestimmte Person zulassen. Personen, die mit den lokalen Gegebenheiten vertraut sind, wissen sofort, um wen es sich handelt. Ist die Person noch bestimmbar, so ist die vorgenommene Anonymisierung ungenügend.

Ziff. 2:

In der Schweiz herrscht die Meinung vor, dass auch juristische Personen datenschutzrechtlich zu schützen sind. Das Interesse, in ihrer Handels- und Gewerbefreiheit durch das Bearbeiten von Daten nicht beeinträchtigt zu werden, ist nicht minder gross als dasjenige der natürlichen Person, die mit den juristischen Personen im wirtschaftlichen Wettbewerb steht. In den meisten europäischen Staaten fallen juristische Personen jedoch nicht unter den Datenschutz. Die besondere Regelung in der Schweiz beinhaltet einen Wettbewerbsvorteil. Anzumerken ist jedoch, dass in der Praxis der Datenschutz selten von juristischen Personen beansprucht wird.

Ziff. 3:

Es gibt Daten, die „normal“ schützenswert (Abs. 1) und solche, die „besonders“ schützenswert sind (Abs. 2). Diese Zweiteilung ist aus Gründen der Verhältnismässigkeit wichtig. Der Datenschutz soll mit gesundem Augenmass durchgeführt werden. Für die zweite Gruppe gelten beim Bearbeiten strengere Voraussetzungen.

Ziff. 4:

Ein besonderer Schutz muss auch gewährt werden, wenn Persönlichkeitsprofile erstellt, ausgewertet oder an Dritte bekanntgegeben werden. Ein Persönlichkeitsprofil ist eine Zusammenstellung einer grösseren Anzahl von Daten über die Persönlichkeitsstruktur, die beruflichen Fähigkeiten und Aktivitäten oder auch die ausserberuflichen Beziehungen und Tätigkeiten, die ein Gesamtbild oder ein wesentliches Teilbild der Person ergibt (beispielsweise Konsumverhalten).

Ziff. 5:

Der Begriff des Bearbeitens ist weit gefasst. Jeder Umgang mit Daten und alle Phasen der Bearbeitung fallen darunter. Die angewendeten technischen Verfahren sind ohne jeglichen Belang.

Ziff. 6:

Die Datenbekanntgabe ist Teil der Datenbearbeitung und mithin die heikelste Bearbeitungsphase, dies nicht zuletzt deshalb, weil sie in mehreren Formen erfolgen kann (unter anderem Abrufverfahren).

Ziff. 7:

Unter den Begriff der Datensammlung fallen nicht nur Karteien und Sammlungen, die nach Personen gegliedert sind, sondern auch solche, die nach bestimmten Personen erschlossen werden können.

Ziff. 8:

Als Organ werden die Behörden und Verwaltungsstellen des Kantons (inklusive Regierungsrat und regierungsrätlich bestellte Kommissionen sowie Gerichte, Rekurskommissionen und die übrigen staatlichen Justizbehörden, soweit sie Verwaltungsaufgaben versehen), aber auch jene der Gemeinden bezeichnet. Die Datenschutzvorschriften beschränken sich dabei nicht nur auf die Politischen Gemeinden, sondern umfassen auch die Schul- und die Kirch- oder Kapellgemeinden im Sinne von Art. 1 Abs. 1 lit. b und lit. c des kantonalen Gemeindegesetzes (NG 171.1). In einzelnen Kantonen können Gemeinden separate Datenschutzreglemente erlassen. In Anbetracht der kleinräumigen Verhältnisse im Kanton Nidwalden ist von einer derartigen Lösung abzusehen. Es wird auch darauf verzichtet, die Gemeinden zu verpflichten, Vollzugsreglemente zu erstellen. Das Gesetz sieht daher eine vollzugstaugliche Normendichte vor, die eine sofortige und direkte Anwendung dieses Gesetzes erlaubt.

Haben Kanton oder Gemeinden Aufgabenerfüllung an kantonale beziehungsweise kommunale öffentlich-rechtliche Körperschaften und Anstalten übertragen, gelten diese gleichfalls als Organ und unterstehen somit auch den datenschutzrechtlichen Standards. Gleiches gilt letztlich auch für Private, soweit ihnen durch den Kanton oder die Gemeinden im Rahmen eines sogenannten „Outsourcing“ öffentliche Aufgaben übertragen sind (vgl. Abgrenzung zu Privaten in Art. 2 Abs. 1 lit. a DSG, die grundsätzlich dem Bundesdatenschutzgesetz unterstehen). Der Grund liegt darin, dass Bürgerinnen und Bürger durch die Auslagerung von öffentlichen Aufgaben in ihrer Rechtsstellung nicht schlechter zu stellen sind.

Ziff. 9

Inhaberin oder Inhaber einer Datensammlung ist dasjenige Organ, das über den Zweck und den Inhalt einer Datensammlung, mithin also über die Existenz und die wesentliche Ausgestaltung einer Datensammlung entscheidet. Das Gesetz verlangt hier eine Art Halterqualität, an welche die Registrier-, Melde- und Auskunftspflicht anknüpfen (vgl. auch Kommentar DSG, a.a.O., N 33 zu Art. 3).

Ziff. 10:

Keine Bemerkungen.

Art. 4 Grundsätze

(Art. 4 Abs. 3 DSG / Art. 5 lit. c und e ER-Konvention / Art. 6 Abs. 1 lit. c und e EU-Datenschutzrichtlinie)

Entspricht weitgehend Art. 4 DSG.

Diese Bestimmung enthält die Grundsätze, die bei jeder Datenbearbeitung zu beachten sind. Dass Abs. 1 den Einsatz rechtswidriger Mittel bei der Bearbeitung von Personendaten untersagt, ist vor allem für die Beschaffung von Bedeutung. So dürfen unter dem Vorbehalt gesetzlicher Ausnahmen Personendaten nicht durch Abhören des Telefons oder die Überwachung des Postverkehrs erhoben werden (Abs. 1).

Daten dürfen nicht wider Treu und Glauben bearbeitet werden. Dagegen verstiesse die Benützung von Daten zu einem Zweck, mit dem die betroffene Person bei der Angabe ihrer Daten in keiner Weise rechnen musste. Dass bei der Datenbearbeitung der Grundsatz der Verhältnismässigkeit zu beachten ist, bedeutet insbesondere, dass nur jene Daten erhoben werden dürfen, welche für die Aufgabenerfüllung benötigt werden.

Mit dem Gebot der Zweckbindung soll verhindert werden, dass einmal erhobene Daten zu beliebigen Zwecken weiterverwendet werden. Immerhin dürfen Personendaten aus einer bestehenden Datensammlung namentlich dann für einen andern als den ursprünglich vorgesehenen Zweck verwendet werden, wenn das Gesetz es vorsieht. So müssen beispielsweise gewisse Steuerdaten von der Ausgleichskasse und vom Amt für Berufsbildung benützt werden können, weil die einschlägigen Gesetze Ansprüche auf Prämienverbilligung und auf Stipendien von Steuerdaten abhängig machen.

Art. 5 Richtigkeit der Daten

Entspricht fast wörtlich Art. 5 DSG.

Die Richtigkeit der Daten ist sowohl für den Persönlichkeitsschutz wie auch für das Funktionieren der Verwaltung notwendig (Abs. 1). Mit der an sich selbstverständlichen Anforderung der Richtigkeit der Daten korreliert der Berichtigungsanspruch der Person; darüber werden im Rahmen der Rechte der Person weitere Ausführungen gemacht.

Art. 6 Bekanntgabe ins Ausland

(Art. 6 DSG / Art. 12 ER-Konvention und Art. 2 Zusatzprotokoll zur ER-Konvention / Art. 25f. EU-Datenschutzrichtlinie)

Entspricht weitgehend Art. 6 DSG, kann aber auf Vorschriften, die sich auf Private beziehen, verzichten.

Nach diesen Vorgaben ist im Gesetz festzuhalten, dass die grenzüberschreitende Bekanntgabe von Daten an Empfängerinnen und Empfänger, für welche die massgebenden europäischen Datenschutzerlasse nicht gelten, nur dann zulässig ist, wenn bei ihnen ein angemessenes Datenschutzniveau sichergestellt ist.

Abs. 1 verlangt als grundsätzliche Voraussetzung für eine gesetzeskonforme Datenübermittlung ins Ausland, dass die Gesetzgebung im Bestimmungsland einen angemessenen Schutz gewährleistet.

Abs. 2 enthält eine abschliessende Liste von alternativen Bedingungen, die das Fehlen einer hinreichenden Datenschutzgesetzgebung im Sinne von Abs. 1 kompensieren, um Daten ins Ausland bekanntgeben zu können. Die Gesetzgebung im Empfängerstaat gewährleistet dann ein angemessenes Schutzniveau, wenn sie den Anforderungen der ER-Konvention entspricht. Darüber hinaus ist aber insbesondere zu berücksichtigen, wie diese Gesetzgebung in der Praxis umgesetzt wird.

Auf europäischer Ebene ergibt sich aus Art. 2 Abs. 2 lit. b des Zusatzprotokolls zur ER-Konvention, dass die zuständige Behörde überprüfen können muss, ob die Schutzmassnahmen angemessen sind, wenn die Gesetzgebung des Empfängerstaates keinen genügenden Schutz bietet. Aus diesem Grund sieht Abs. 3 eine Informationspflicht vor.

Art. 7 Datensicherheit

(Art. 7 Zusatzprotokoll zur ER-Konvention / Art. 17 EU-Datenschutzrichtlinie)

Entspricht fast wörtlich Art. 7 DSG.

Ein wichtiger Bereich des Datenschutzes ist die Datensicherheit. Die beste Datenschutzregelung nützt nichts, wenn diejenigen Personen und Organe, die Daten bearbeiten, nicht die nötigen Sicherungsmassnahmen zum Schutze der Daten ergreifen. Gefordert sind nicht nur die Organe, sondern insbesondere auch jede einzelne Person, wird doch der Datenschutz in erster Linie durch diejenigen Personen verwirklicht, welche mit Daten arbeiten.

Hohe Anforderungen sind auch an die Betreiberinnen und Betreiber von Informatik-Infrastrukturen zu stellen: Sie haben die Anlagen auf dem geltenden Sicherheitsniveau zu betreiben und diejenigen Mittel zur Verfügung zu stellen, die es den einzelnen Anwenderinnen und Anwendern erlauben, ihrerseits notwendige Massnahmen zu ergreifen (Bereitstellung von passwortgeschützten Bereichen, Verschlüsselungs-Software, etc.).

Art. 8 Informationspflicht bei der Beschaffung von besonders schützenswerten Daten und Persönlichkeitsprofilen

Entspricht fast wörtlich Art. 7a DSG.

Dieser erhöhten (aktiven) Informationspflicht muss die Inhaberin oder der Inhaber der Datensammlung von sich aus nachkommen, sobald sie beziehungsweise er besonders schützenswerten Daten oder Persönlichkeitsprofile beschafft. Indirekt soll diese Vorschrift eine präventive Wirkung zukommen, um zu verhindern, dass Daten gesammelt werden, die für die Tätigkeit der Organe nicht unbedingt benötigt werden. Die Information ist keinem Formerfordernis unterworfen.

Art. 9 Datenbearbeitung durch Dritte

Entspricht fast wörtlich Art. 10a DSG.

Die Bearbeitung von Daten kann einem Dritten nur übertragen werden, wenn sich der Auftraggeber vergewissert hat, dass der Auftragnehmer die notwendigen Sicherheitsstandards einhält. Der Auftraggeber muss sich insbesondere vergewissern, dass die Sicherheitsstandards beim Auftragnehmer tatsächlich angewendet werden.

Art. 10 Verantwortliches Organ

Entspricht weitgehend Art. 16 DSG.

Dass dasjenige Organ verantwortlich ist, dass Daten bearbeitet, ist offensichtlich. Wichtiger ist vielmehr die Kompetenzabgrenzung, sofern mehrere Organe Daten gemeinsam bearbeiten.

Art. 11 Rechtsgrundlagen

(Art. 17 DSG / Art. 6 ER-Konvention / Art. 8 EU-Datenschutzrichtlinie)

Entspricht fast wörtlich Art. 10a DSG.

Diese Bestimmung enthält die das kantonale Datenschutzrecht überspannenden Leitlinien fest, an denen jede Bearbeitung von Personendaten zu messen ist. Die Bearbeitung von Informationen über Personen muss sich mindestens mittels Auslegung der Vorschriften über die wahrzunehmenden öffentlichen Aufgaben ableiten lassen. Umgekehrt ist nicht für jede Datensammlung eine formellgesetzliche Rechtsgrundlage zu verlangen, will der Datenschutz nicht überdehnt und die Wirksamkeit und Wirtschaftlichkeit der Verwaltungstätigkeit nicht übermässig erschwert werden. Dem Gesetzmässigkeitsprinzip entsprechend darf eine Bearbeitung von Personendaten grundsätzlich nur dann erfolgen, wenn sie sich auf eine Rechtsgrundlage beziehen kann.

Sodann gilt es zu unterscheiden zwischen den „normal schützenswerten“ Daten einerseits (Abs. 1) und den „besonders schützenswerten“ Personendaten (Abs. 2) andererseits. Bei letzteren sind wesentlich strengere Anforderungen an das Bearbeiten zu stellen.

Im Interesse eines wirksamen Datenschutzes sowie der Rechtssicherheit ist es nötig, dass für jedes Bearbeiten von „normal schützenswerten“ Personendaten gemäss Abs. 1 eine gesetzliche Grundlage vorliegt. Es genügt bereits eine solche im materiellen Sinne. Diese gesetzliche Grundlage kann auf Bundes-, Kantons- oder Gemeindeebene erlassen worden sein. In den Gesetzen ist aber das Bearbeiten von Daten kaum je direkt und ausdrücklich geregelt. Ein derartiges Erfordernis würde beim Vollzug zu zahlreichen Umsetzungsproblemen führen und einigen Behörden die Arbeit bis zur Schaffung entsprechender gesetzlicher Grundlagen nahezu verunmöglichen. Aus Gründen der Praxistauglichkeit ist deshalb eine „mittelbare“, weniger weitgehende Rechtsgrundlage vorzusehen. Danach muss das Bearbeiten nicht direkt im Gesetz geregelt, sondern für eine in einer gesetzlichen Grundlage umschriebenen Aufgabe unentbehrlich sein.

Bei den besonders schützenswerten Personendaten im Sinne von Abs. 2 sind deutlich höhere Anforderungen an das Bearbeiten gestellt. Ein formelles Gesetz, somit ein referendumpflichtiger, vom Parlament verabschiedeter Erlass, muss diese Datenbearbeitung ausdrücklich vorsehen (Ziff. 1). Oder aber der Regierungsrat kann ausnahmsweise *im Einzelfall* Bewilligungen zur Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen erteilen kann. Gestützt auf diese Delegationsklausel kann somit nicht eine unbestimmte Anzahl von Fällen be-

willigt werden. Sodann kann das Bearbeiten von Daten auch rechtmässig sein, wenn die Person hierzu ausdrücklich die Einwilligung erteilt oder ihre Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat (Ziff. 3).

Art. 12 Datenbeschaffung

Entspricht weitgehend Art. 18 DSG.

Die besondere Vorschrift über das Beschaffen von Personendaten stellt eine Ergänzung zu den Grundsätzen von Art. 4 dar. Die Daten sind so zu beschaffen, dass dies für die betroffenen Personen erkennbar ist. Diesem Gebot wird am besten nachgelebt, wenn die Daten bei der betroffenen Person selbst erhoben werden. Bei systematischen Erhebungen (Fragebogen) ist eine besondere Orientierungspflicht für das Organ vorgesehen, weil hier oft in grossem Umfang Daten beschafft werden. Es teilt der betroffenen Person mit, aufgrund welcher Rechtsgrundlage und zu welchem Zweck die Daten erhoben werden. Zudem gibt es bekannt, wer Empfänger der Daten sein wird.

Art. 13 Datenbekanntgabe

1. im Allgemeinen

Entspricht weitgehend Art. 19 DSG, enthält jedoch eine gewisse Lockerung im Hinblick auf Abrufverfahren.

Die Erfahrung zeigt, dass die Regelungen über die Bekanntgabe von Daten die wichtigste Rolle im öffentlichrechtlichen Persönlichkeitsschutz spielen. Der moderne Sozial- und Leistungsstaat betreibt dabei in umfassender Weise Informationsbeschaffung. Soweit es sich dabei um Personendaten handelt, steht die Informationsbearbeitung in einem Spannungsfeld zwischen den Erfordernissen einer koordinierten und rationellen Verwaltungstätigkeit einerseits und den Anliegen des Persönlichkeitsschutzes andererseits. Selbstverständlich ist dabei, dass zusammenarbeitende Verwaltungseinheiten nicht gegenseitig in sämtliche Daten Einsicht nehmen können. Eine gewisse Abschottung zwischen den Verwaltungseinheiten ist notwendig. Abs. 1 nennt – mit dem Hinweis auf Art. 11 – insgesamt 5 Fälle der Bekanntgabe.

Mit einem Abrufverfahren wird ein Organ in die Lage versetzt, auf die Datensammlung eines anderen Organs zugreifen zu können. Damit ist aber nicht gesagt, dass das datenempfangende Organ Zugriff auf sämtliche Daten der Datenlieferantin oder des Datenlieferanten hat, sondern ausschliesslich und nur auf diejenigen, die zwingend Bestandteil ihres Vollzugsauftrages sind. Dies allerdings nur unter der Voraussetzung, dass es sich hierbei um „gewöhnliche“ Daten handelt. Sollen jedoch besonders schützenswerte Daten durch ein Abrufverfahren zugänglich gemacht werden, bedarf es einer ausdrücklichen Gesetzesbestimmung im formellen Sinn., welche dies vorsieht.

Das Abrufverfahren macht nicht mehr oder andere Daten zugänglich als andere Arten der Bekanntgabe, sondern betrifft nur die Methode. Ist ein Abrufverfahren einmal eingerichtet, hat das Organ, welches die Daten zur Verfügung stellt, allerdings keinen Einfluss mehr auf die Menge und den Zeitpunkt des Datenbezugs. Dieser Umstand rechtfertigt aber keine weitergehenden, administrativ aufwändigen Einschränkungen.

Im Einzelfall kann aus überwiegenden öffentlichen oder aus schutzwürdigen privaten Interessen die Bekanntgabe von Personendaten abgelehnt werden, wenn die Interessen der nachfragenden Partei wenig schutzwürdig sind. Erscheint eine Verweigerung der Datenbekanntgabe als unverhältnismässig, kann sie unter Auflagen erteilt oder eingeschränkt gewährt werden (Abs. 3 Ziff. 1). Vorbehalten bleiben besondere

Geheimhaltungsvorschriften, die als Spezialrecht den kantonalen Datenschutzbestimmungen vorgehen (Ziff. 2).

Art. 14 2. durch die Einwohnerkontrolle

Diese Regelung bewegt sich im Rahmen der Gesetzgebung der anderen Kantone. Die bisherige gesetzliche Bestimmung über den Datenschutz im Bereich Einwohnerkontrolle wird aus dem Gesetz über die Niederlassung der Schweizer (NG 122.1) herausgelöst (vgl. Art. 36 [Änderung bisherigen Rechts]), auf die Einwohnerkontrolle für Ausländerinnen und Ausländer ausgedehnt und präzisiert.

Im Rahmen des Vernehmlassungsverfahrens wurde diese Bestimmung insbesondere von Seiten der betroffenen politischen Gemeinden heftig kommentiert (vgl. dortige Ausführungen). Im Ergebnis lässt sich festhalten, dass eine angemessene Datenbekanntgabe an Dritte – und dies ist nicht zu verwechseln mit der Amtshilfe im Rahmen von Art. 13 Abs. 1 Ziff. 1 – je nach erfüllten Voraussetzungen möglich sein soll.

In Abs. 1 geht es um die Auskunftserteilung an Dritte. Es bestehen legitime Informationsbedürfnisse Dritter bezüglich bestimmter Personendaten. Dabei ist zu bedenken, dass im Rahmen von Art. 15 die Möglichkeit besteht, Daten sperren zu lassen. Die Einwohnerkontrollen können damit unkompliziert Basisinformationen, die teilweise ohnehin aus dem Telefonbuch zu entnehmen sind, jedermann abgeben. Es handelt sich um Daten, die in geringem Masse als schutzwürdig erscheinen. Für die Fälle nach Ziff. 1 kann die Anfrage schriftlich oder auch mündlich gestellt werden (im Gegensatz zu den nachfolgenden Ziff. 2 und 3, letzterer in Verbindung mit Abs. 2).

Soweit sich die Auskunftserteilung an Dritte nicht nur auf die voraussetzungslos zugänglichen Daten nach Abs. 1 Ziff. 1 bezieht, ist sie gemäss Ziff. 2 lediglich auf schriftliches Gesuch hin möglich (E-Mail-Anfragen genügen dieser Schriftlichkeit) – und erfolgt auch schriftlich. Dies ermöglicht dem auskunftsgebenden Organ eine bessere Überprüfungsmöglichkeit der Voraussetzungen der Datenbekanntgabe. Der Interessennachweis muss nach Ziff. 2 „nur“ glaubhaft gemacht werden. Es hat also nicht ein hieb- und stichfester Beweis vorzuliegen. Auf der anderen Seite genügt aber unter Umständen eine blosser Behauptung nicht.

Bei Sammelauskünften im Sinne von Abs. 1 Ziff. 3 müssen schützenswerte ideelle Zwecke vorliegen. Zu denken ist dabei insbesondere an politische, wohltätige, gesellschaftliche oder wissenschaftliche Gründe. Auch hier muss der Interessennachweis glaubhaft gemacht werden. Zulässig ist damit etwa die wiederkehrende Bekanntgabe der Adressen aller Neuzuzüger einer Gemeinde an politische Parteien, an Sportvereine und anderes mehr. Um Missbräuche zu verhindern, sollten die Datenbezügerinnen und Datenbezüger schriftlich auf die datenschutzrechtlichen Bestimmungen, insbesondere auch auf die strafrechtlichen Folgen nach Art. 34 Ziff. 1 bei Zuwiderhandlungen aufmerksam gemacht werden. Für Werbung oder andere kommerzielle Zwecke, beispielsweise für den Adresshandel, werden hingegen keinerlei Sammelauskünfte erteilt.

Das kantonale Amt in Sachen Migration ist den kommunalen Einwohnerkontrollen gleichgestellt, weil es für ausländische Staatsangehörige ähnliche Funktion wie die Einwohnerkontrollen erfüllt. Die Abs. 1 und 2 sind daher auch für dieses anwendbar.

Für die Frage der Erhebung von Gebühren im Zusammenhang mit der Erteilung von Auskünften ist Art. 33 Abs. 3 [Gebühren] massgebend.

Art. 15 Sperrung der Bekanntgabe

Ist identisch mit Art. 20 DSG.

Die Datensperre ist nur zulässig, soweit ein schutzwürdiges Interesse glaubhaft gemacht wird.

Das Sperrrecht ist jedoch nicht absolut und erfährt dort seine Grenzen, wo eine gesetzliche Grundlage das Organ zur Datenbekanntgabe verpflichtet beziehungsweise die Erfüllung seiner Aufgabe sonst gefährdet wäre. Die Sperrung der Bekanntgabe ist darüber hinaus auch nicht absolut, wenn Dritte in der Verfolgung ihrer schutzwürdigen Ansprüche behindert sind (vgl. Art. 13 Abs. 1 Ziff. 4; beispielsweise wenn ein Gläubiger glaubhaft macht, dass er eine Forderung gerichtlich geltend machen will und für die Einreichung einer Klage den Wohnsitz des Schuldners eruieren muss. Der Schuldner entzieht sich diesen Nachforschungen, indem er bei der Einwohnerkontrolle eine Sperrung veranlasst. Dieses Verhalten darf nicht geschützt werden).

Art. 16 Datenbearbeitung für nicht personenbezogene Zwecke

(Art. 22 DSG / Art. 9 Ziff. 3 ER-Konvention / Art. 6 Abs. 1 lit. b und e und Art. 11 Abs. 2 EU-Datenschutzrichtlinie)

Ist identisch mit Art. 8 DSG.

Die Bearbeitung von Personendaten für Zwecke der Statistik, Planung oder der wissenschaftlichen Forschung geniesst datenschutzrechtlich weitgehende Privilegien, weil die Person nicht als individuelle Persönlichkeit, sondern lediglich anonym, als statistische Einheit, fungiert. Das verantwortliche öffentliche Organ hat sich aber zu vergewissern, dass die für eine bestimmte Untersuchung nötigen Daten so weitergegeben werden, dass Rückschlüsse auf Personen möglichst erschwert sind (beispielsweise durch Unkenntlichmachen des Familiennamens und der Adresse, durch Anonymisieren oder Pseudonymisieren).

Art. 17 Einsatz technischer Überwachungsgeräte

Im Rahmen des Vernehmlassungsverfahrens wurde von Seiten von politischen Gemeinden beantragt, eine kantonal einheitliche Regelung betreffend die Videoüberwachung an öffentlich zugänglichen Orten zu schaffen. In der Tat macht es Sinn, die öffentlichen Gemeinwesen einheitlichen Vorschriften in diesem Hinblick zum Schutz von Personen und Sachen zu unterstellen. Ansonsten hätten insbesondere die Gemeinden in ihren Reglementen jeweils selbstständig rechtliche Grundlagen zu schaffen, um Videoüberwachungsanlagen einsetzen zu können. Damit kann auch der Kanton gleichzeitig für sich eine Gesetzeslücke schliessen (vgl. Medienmitteilung des Bundesrates vom 28. September 2007 betreffend Sicherheit an öffentlichen Orten: rechtliche Lücken im Bereich der Videoüberwachung sollen geschlossen werden), um die verfassungsmässigen Voraussetzungen für die Einschränkung von Grundrechten betroffener Personen zu erfüllen. Das Bestehen einer gesetzlichen Grundlage ist indes nur einer von drei Aspekten der Einschränkung; auch das öffentliche Interesse und die Verhältnismässigkeit der Massnahme müssen erfüllt sein. Einem ausufernden Einsatz von Überwachungsgeräten sind daher auch bei der Schaffung entsprechender rechtlicher Grundlagen Grenzen gesetzt. Die zuständige Instanz hat sich deshalb vorgängig Rechenschaft abzulegen, ob nicht auch andere Massnahmen wie beispielsweise baulicher, personeller oder sozialer Natur geeignet wären, das anvisierte Ziel zu erreichen, die aber das Grundrecht auf Schutz der Privatsphäre weniger tangieren. Dass diesem Umstand hinreichend Rechnung getragen wird, dafür sorgt die Verpflichtung zur Information an die Aufsichtsstelle gemäss Abs. 1 Ziff. 3.

Gemäss Abs. 1 ist der Einsatz technischer Geräte wie insbesondere Bildaufzeichnungsgeräten an öffentlich zugänglichen Orten zulässig, wenn und soweit er zum Schutz von Personen und Sachen unter den obgenannten Voraussetzungen ange-

ordnet wird. Sodann muss durch Tafeln, Schilder oder dergleichen darauf hingewiesen werden, dass dieser Ort überwacht wird (Abs. 1 Ziff. 1). Sodann muss sichergestellt werden, dass Bildaufzeichnungen nach einer bestimmten Frist gelöscht werden, sofern sie nicht als Beweismittel verwendet werden sollen. Fristen von einigen wenigen Tagen sind unrealistisch. Andererseits hat das Bundesgericht in seinem Urteil vom 14. Dezember 2006 erkannt, die Regelung des St. Galler Polizeireglements, wonach Videoaufzeichnungen erst nach 100 Tagen vernichtet werden müssen, könne verfassungskonform gehandhabt werden (Urteil 1P.358/2006). Das Bundesgericht begründete dies unter anderem damit, es müsse Opfern von Delikten zugestanden werden, mit ihrer Anzeige eine gewisse Zeit zuzuwarten, ohne dass die Bilder als Beweismittel dann bereits vernichtet seien. Die Frist von 30 Tagen erscheint angemessen, um entsprechende straf- oder zivilprozessuale Massnahmen einleiten zu können (zum Vergleich: Kanton Schwyz: 120 Stunden; Kanton Obwalden: 100 Tage; Bund: 1 Monat im Rahmen der Verordnung über den Einsatz von Bildaufnahme-, Bildaufzeichnungs- und anderen Überwachungsgeräten durch die Eidgenössische Zollverwaltung [SR 631.053], 24 Stunden im Rahmen der Verordnung über die Videoüberwachung durch die Schweizerischen Bundesbahnen SBB [SR 742.147.2]).

Art. 18 Datenarchivierung, Datenvernichtung

Entspricht inhaltlich weitgehend Art. 21 DSG.

Personendaten, soweit sie von den Organen für die ursprüngliche Zweckbestimmung oder zu Sicherungs- und Beweis Zwecken nicht mehr benötigt werden, sind in ein Archiv zu überführen oder dann aber zu vernichten (physisches Vernichten und / oder ☐ Löschen elektronischer Daten unter gleichzeitiger Erstellung eines Vernichtungsprotokolls). Was zu archivieren ist, wird durch die Archivgesetzgebung bestimmt (Abs. 1).

Art. 19 Registerführung

Die erste Aufgabe eines wirkungsvollen Datenschutzes besteht darin, sich einen Überblick über die vorhandenen Datensammlungen zu verschaffen. Das Register ist lediglich eine Aufstellung aller Datensammlungen mit den Angaben gemäss Art. 20 Abs. 1 [Registerinhalt]. Es enthält somit selber keine Informationen über die in den einzelnen Datensammlungen aufgeführten Personen (beziehungsweise der dazugehörigen Daten).

Der Aufbau dieses Registers ist zeitintensiv und erfordert für den Kanton voraussichtlich rund ein Jahr. Die Erarbeitung seines Registers ist Aufgabe der Direktionen in enger Zusammenarbeit mit beziehungsweise unter Anleitung der Aufsichtsstelle. Für die übrigen Registerführungspflichtigen ist der Aufwand erheblich niedriger. Der Aufbau der Register ist – aufgrund der Erfahrungen in anderen Kantonen – mit einem grossen Sensibilisierungseffekt für die Registerführungspflichtigen verbunden. Gerade die Erstellung des Registers zwingt die Verantwortlichen einer Datensammlung, sich intensiv mit der einzelnen Datensammlung auseinanderzusetzen.

Die Aufsichtsstelle führt das Register des Kantons. Sie instruiert hierzu die Verwaltung, welche Datensammlungen wie zu erfassen sind. Die Angaben zu den vorhandenen Datensammlungen müssen jedoch von den jeweiligen Verwaltungsstellen selber geliefert werden. Die Aufsichtsstelle ist auch hier auf eine enge Zusammenarbeit mit der Verwaltung angewiesen. Sodann führt die Aufsichtsstelle ein zentrales Register der übrigen registrierten Datensammlungen.

Das Register dient als Kontrollinstrument für die Aufsichtsstelle. Diese soll zur Gewährleistung einer gewissen Harmonisierung der Register im Einzelfall oder generell Weisungen über die Registerführung erteilen dürfen.

Art. 20 Registerinhalt

Der erforderliche Aufwand für die Erstellung der Register der angelegten Datensammlungen soll angesichts deren Vielzahl in Grenzen gehalten werden. Die Auflistung des Inhalts der Register entspricht unter anderen den aktuellen Regelungen der Kantone Luzern und Zug.

Aus Gründen der Verhältnismässigkeit sind nicht alle Datensammlungen in das Register aufzunehmen (Abs. 2). Datensammlungen, die nur für kurze Zeit geführt werden (während der Bearbeitung eines umfangreichen Falles bis zu dessen Erledigung), rechtmässig veröffentlicht sind (beispielsweise Wahllisten) oder reine Hilfsdatensammlungen darstellen (Pendenzenlisten), brauchen nicht registriert zu werden.

Art. 21 Einsichtsrecht

Dieser Artikel statuiert das Recht jeder Person, Einsicht in die Register zu nehmen. Beim Einsichtsrecht geht es zunächst darum, dass sich Personen darüber erkundigen können, welche Datensammlungen mit welchem generellen Inhalt überhaupt vorhanden sind. Es geht aber noch nicht darum, in Erfahrung zu bringen, ob und allenfalls welche Daten über eine Person vorhanden sind. Über die konkreten Einzeldaten verfügt nicht die registerführende Aufsichtsstelle, sondern die Inhaberin oder der Inhaber der Datensammlung.

Art. 22 Auskunftsrecht

(Art. 4 und 8 DSG / Art. 8 lit. a und b ER-Konvention / Art. 10, 11, 12 und 21 EU-Datenschutzrichtlinie)

Ist identisch mit Art. 8 DSG.

Das Auskunftsrecht ist das bedeutendste Institut des Datenschutzrechtes. Erst die ausdrückliche Erwähnung eines Anspruches auf Auskunft – und damit verbunden die Mitteilungspflicht der Inhaberin oder des Inhabers der Datensammlung – erlaubt Betroffenen die wirksame Durchsetzung der Abwehrrechte. Nur wenn sie erfahren, welche Daten über sie bearbeitet werden, können sie die ihnen zustehenden weiteren Rechte und Ansprüche (beispielsweise auf Berichtigung oder Unterlassung) wahrnehmen.

Abs. 3 hat den Zweck, die Person vor Schaden zu bewahren, der ihr entstehen könnte, wenn sie unvermittelt und unvorbereitet mit Tatsachen konfrontiert wird, die ihr noch nicht bekannt waren oder die sie aufgrund fehlender Fachkenntnisse nicht richtig beurteilen kann.

Beim Auskunftsrecht handelt es sich um einen unverzichtbaren Anspruch jeder Person (Abs. 5).

Art. 23 Einschränkungen des Auskunftsrechts

Ist identisch mit Art. 9 DSG, soweit sich diese Vorschrift auf Bundesorgane bezieht.

Die Einschränkung des Rechts auf Auskunft über und auf Einsicht in Daten darf zunächst nur aus gesetzlichen Gründen erfolgen, wobei dabei insbesondere die Bestimmungen über die Geheimhaltung im Vordergrund stehen. Eine Einschränkung des Auskunfts- und Einsichtsrecht ist darüber hinaus unter anderem gegeben, sofern ei-

ner Bekanntgabe der Daten an Personen überwiegende öffentliche oder private Interessen entgegenstehen.

Art. 24 Weitere Ansprüche

(Art. 8 Zusatzprotokoll zur ER-Konvention / Art. 12 EU-Datenschutzrichtlinie)

Ist identisch mit Art. 25 Abs. 1 – 3 DSG.

Dieser Artikel garantiert der Person Abwehrrechte im Falle einer widerrechtlichen Datenbearbeitung. Betroffene können sich gegen alle Arten widerrechtlicher oder unzulässiger Bearbeitung wehren.

Eine Datenbearbeitung ist in der Regel aus zwei Gründen widerrechtlich: Entweder sind die Daten unrichtig, das heisst falsch, nicht aktuell oder unvollständig. In diesen Fällen besteht ein selbstständiger Anspruch der betroffenen Person auf Berichtigung oder – kann die Richtigkeit nicht erstellt – ein Anspruch auf Anbringung eines Vermerks. Oder aber die Bearbeitung der möglicherweise richtigen Daten erfolgte ohne ausreichende Rechtsgründe. In diesem Falle stehen der betroffenen Person diverse Ansprüche offen:

- der Unterlassungsanspruch kann sich namentlich auf die Weitergabe von Daten an Dritte beziehen und ist bereits dann zuzulassen, wenn eine widerrechtliche Bearbeitung ernstlich zu befürchten ist (Abs. 1 Ziff. 1).
- die Beseitigung der Folgen einer unzulässigen Datenbearbeitung ist manchmal nur mehr in beschränktem Umfang möglich, namentlich wenn Dritte schon Kenntnis von einer Information erhalten haben. Widerrechtlich bearbeitete Daten sind grundsätzlich zu vernichten (Abs. 1 Ziff. 2).
- auch die blosse Feststellung der Widerrechtlichkeit einer Datenbearbeitung kann von Bedeutung sein. Die Person hat damit einen Rechtstitel in Händen, der es ihr ermöglicht, bei nachträglich auftauchenden Folgen widerrechtlicher Bearbeitung unverzüglich einzuschreiten (Abs. 2 Ziff. 1).

Die Person kann letztlich unter anderem auch verlangen, dass Daten berichtigt, vernichtet oder die Bekanntgabe von Daten an Dritte gesperrt wird (Abs. 3).

Art. 25 Ablehnung von Gesuchen

Die Person kann im Einzelfall von der Inhaberin oder vom Inhaber der Datensammlung einen beschwerdefähigen Entscheid verlangen, falls ihre datenschutzrechtlichen Begehren (ganz oder teilweise) abgelehnt werden (Abs. 1).

Damit die Aufsichtsstelle von ihrem Recht der Behördenbeschwerde Gebrauch machen kann, sind ihr diese Verfügungen mitzuteilen (Abs. 2).

Art. 26 Aufsichtsstelle

(Art. 26f. DSG / Art. 1 Zusatzprotokoll zur ER-Konvention / Art. 28 EU-Datenschutzrichtlinie)

Diese Vorschrift verschaffte der Forderung von Art. 37 Abs. 2 DSG Nachachtung, wonach der Kanton ein Kontrollorgan einzusetzen hat, das beim Vollzug von Bundesrecht über die Einhaltung der Datenschutzvorschriften wacht. Wie die Erfahrung in anderen Kantonen zeigte, kann ein befriedigender und wirksamer Datenschutz nur gewährleistet werden, wenn eine unabhängige Kontrollinstanz seine Verwirklichung überwacht.

Die europäischen Vorschriften verpflichten die Mitgliedstaaten und die Gliedstaaten zur Einführung völlig unabhängiger Kontrollorgane. Die erforderliche Unabhängigkeit der kantonalen Aufsichtsstelle kann unter anderem dadurch bewirkt werden, dass

sie auf die verfassungsmässige Amtsdauer von vier Jahren gewählt wird (vgl. Art. 45 KV). Bei der Wahl ist auf die fachliche Kompetenz der zu wählenden Person zu achten. Sie hat fachlich selbständig und unabhängig zu sein. Unter einer unabhängigen Stellung wird verstanden, dass die Aufsichtsstelle in der Ausführung ihrer Aufgaben vollständig weisungsungebunden und nur dem Gesetz und der Verfassung unterworfen ist (Kommentar DSG, a.a.O., N 28ff. zu Art. 26).

Ob der Kanton Nidwalden diese Aufgabe selbst allein wahrnehmen will respektive kann, ist aufgrund der Rahmenbedingungen und weiteren Prämissen (Stichwort Stellvertretungsregelung) zweifelhaft. Der Kanton Nidwalden wird möglicherweise nicht umhin kommen, die Lösung in einem interkantonalen Verbund zu suchen (Abs. 3). Um eine solche Zusammenarbeit auf einfache Weise bewerkstelligen zu können, sieht das Gesetz eine Ermächtigung des Regierungsrates zum Abschluss einer entsprechenden Verwaltungsvereinbarung vor. Gestützt darauf könnte der Regierungsrat mit andern Kantonen eine Lösung anstreben, die Personalressourcen zusammenlegt und gemeinsam nutzt (Kompetenzzentrum).

Art. 27 Aufgaben

(Art. 26f DSG / Art. 1 Zusatzprotokoll zur ER-Konvention / Art. 20 und 28 EU-Datenschutzrichtlinie)

Die gesetzliche Ausgestaltung zeigt, dass nicht nur an die nachträgliche Kontrolle gedacht worden ist. Vorgesehen ist unter anderem eine unterstützende, im Vorfeld von Konflikten beratende und vermittelnde Tätigkeit. Kontrollen bleiben aber nichtsdestotrotz unerlässlich und müssen insbesondere dort durchgeführt werden können, wo eine grosse Anzahl von Personen gravierend beeinträchtigt zu werden droht. Die Aufsicht verfolgt demnach zwei Stossrichtungen: einerseits Beratung und Information, andererseits Kontrolle und Überwachung.

Das europäische Recht verlangt die gesetzliche Verankerung einer Vorabkontrolle durch das Kontrollorgan für die Bearbeitung von Daten, die besondere Risiken für die Rechte und Freiheit der betroffenen Personen mit sich bringen können. Dabei kann sich das Verletzungspotential der Bearbeitungsmethode entweder aufgrund der Art der Bearbeitung oder der zu bearbeitenden Daten ergeben. Kriterien für die Beurteilung des Risikos können zum Beispiel die Zahl der erfassten Personen, die Zahl der beteiligten öffentlichen Organe oder die Sensitivität der Daten sein. Objekt der Vorabkontrolle können vor allem Projekte für IT-Systeme, für Datenbanken oder Register sein. Im Sinne einer Steigerung der Wirksamkeit des Kontrollorgans fordern die massgebenden internationalen Erlasse, dass das Kontrollorgan seinen jährlichen Tätigkeitsbericht und Stellungnahmen, welche beispielsweise im Rahmen einer Vorabkontrolle erstellt wurden, veröffentlicht.

Art. 28 Arbeitsweise

Die gesetzliche Ausgestaltung zeigt, dass nicht nur an die nachträgliche Kontrolle gedacht worden ist. Vorgesehen ist unter anderem eine unterstützende, im Vorfeld von Konflikten beratende und vermittelnde Tätigkeit. Kontrollen bleiben aber nichtsdestotrotz unerlässlich und müssen insbesondere dort durchgeführt werden können, wo eine grosse Anzahl von Personen gravierend beeinträchtigt zu werden droht. Die Aufsicht verfolgt demnach zwei Stossrichtungen: einerseits Beratung und Information, andererseits Kontrolle und Überwachung. Notfalls ist es der Aufsichtsstelle in Einzelfällen gestattet, für gewisse Belange Expertinnen oder Experten beizuziehen (Abs. 1).

Weil die Aufsichtsstelle zur Abklärung des rechtserheblichen Sachverhalts über weitreichende Kompetenzen verfügt und sie dadurch Einsicht in sensible Personendaten erhalten kann, wird sie einer Verpflichtung zur Verschwiegenheit unterstellt. Daraus

ergibt sich für die Kontrollstelle die Pflicht, dieselben Geheimhaltungsbestimmungen einzuhalten wie die öffentlichen Organe, welche Personendaten bearbeiten. Diese Pflicht besteht über die Beendigung der Funktion hinaus weiter (Abs. 2).

Das Organ hat umfassend Auskünfte zu erteilen. Dabei hat sich insbesondere auch die in andern Kantonen gesetzlich ausdrücklich vorgeschriebene Verpflichtung der Organe zur Zusammenarbeit mit der Aufsichtsstelle als nützlich erwiesen (Abs.3).

Art. 29 Massnahmen

1. Empfehlung

(Art. 1 Ziff. 2a Zusatzprotokoll zur ER-Konvention / Art. 28 Abs. 3 EU-Datenschutzrichtlinie)

Gemäss diesen europäischen Vorgaben muss das Kontrollorgan über umfassende Untersuchungsbefugnisse, wirksame Einwirkungsbefugnisse und eine klage- beziehungsweise Anzeigebefugnis bei Verstössen gegen das Datenschutzrecht verfügen. Es gibt allerdings keine Vorschrift über einen Minimalsatz an Einwirkungsbefugnissen. Es ist erforderlich, dass das Kontrollorgan mit den gesetzlich festgelegten Einwirkungsbefugnissen in ihrer Gesamtheit tatsächlich Wirksamkeit entfalten kann. Stellt die Aufsichtsstelle Verletzungen von Datenschutzvorschriften fest, empfiehlt sie der Inhaberin oder dem Inhaber der Datensammlung zunächst, die Bearbeitung in ihrem Sinne zu ändern oder zu unterlassen. Mit dieser Empfehlung kann es jedoch nicht sein Bewenden haben (vgl. Art. 30).

Art. 30 2. Verfügung

(Art. 1 Ziff. 2a Zusatzprotokoll zur ER-Konvention / Art. 28 Abs. 3 EU-Datenschutzrichtlinie)

Um den Vorgaben des europäischen Rechts nach einer Durchsetzung der datenschutzrechtlichen Einwände zu genügen, muss der Aufsichtsstelle ein Instrument in die Hand gegeben werden, gegen ein Organ vorgehen zu können, das die notwendigen Massnahmen nicht von sich aus trifft. Die Angelegenheit ist der orientierten Instanz zum Entscheid vorzulegen, der gegebenenfalls auch von der Aufsichtsstelle angefochten werden kann (vgl. dazu auch Art. 27 Abs. 4 – 6 DSG).

Art. 31 Beschwerde

(Art. 1 Ziff. 2a Zusatzprotokoll zur ER-Konvention / Art. 22 und 28 Abs. 3 EU-Datenschutzrichtlinie)

Die europäischen Bestimmungen verlangen, dass sowohl Betroffenen wie dem Kontrollorgan die Befugnis zusteht, bei Verletzungen des Datenschutzes bei einer gerichtlichen Instanz einen Rechtsbehelf einzulegen beziehungsweise Klage zu erheben oder eine Anzeige einzureichen. Die Entscheide des Kontrollorgans unterstehen dabei letztlich einer gerichtlichen Kontrolle (Abs. 2). Da es sich bei diesen zusätzlichen Befugnissen der Aufsichtsstelle hauptsächlich um Massnahmen im Sinne einer ultima ratio handelt, dürfte es sich bei den verursachten Beschwerdeverfahren nur um wenige Einzelfälle handeln.

Art. 32 Beschwerdebefugnis

(Art. 1 Ziff. 2a Zusatzprotokoll zur ER-Konvention / Art. 28 Abs. 3 EU-Datenschutzrichtlinie)

Nach § 70 Ziff. 2 Verwaltungsverfahrensverordnung (VRPV; NG 265.1) ist jede andere natürliche oder juristische Person oder Behörde, welche die Gesetzgebung dazu ermächtigt, zur Einreichung eines Rechtsmittels berechtigt. Die Behördenbeschwerde ist deshalb, soweit dies die massgebenden europäischen Bestimmungen zwingend vorsehen, in der jeweiligen Spezialgesetzgebung zu postulieren.

Art. 33 Gebühren

Dieser Artikel garantiert den Betroffenen im Grundsatz, dass sie ihre im Gesetz garantierten Kontrollrechte ohne die abschreckende oder behindernde Wirkung eines Kostenrisikos wahrnehmen können (Abs. 1). Die Kostenlosigkeit der Geltendmachung von Ansprüchen nach diesem Gesetz ist eines der Kernelemente; sie gilt jedoch nicht generell (vgl. Abs. 2). Vorbehalten bleibt letztlich auch die Gebührenpflicht nach der Gebührengesetzgebung bei der Bekanntgabe von Daten für nicht ideelle Zwecke (Abs. 3).

Art. 34 Strafbestimmung

(Art. 24 EU-Datenschutzrichtlinie)

Nach der Vorgabe der EU-Datenschutzrichtlinie müssen Sanktionen vorgesehen werden, welche bei Verstössen gegen das Datenschutzgesetz anzuwenden sind. Als mögliche Lösungen nennt die Wegleitung Strafbestimmungen für Amtsgeheimnisverletzungen oder für die auftragswidrige Verwendung oder Bekanntgabe von Personendaten durch die Beauftragten bei einer Datenbearbeitung im Auftrag. Das Amtsgeheimnis wird durch Art. 320 des Schweizerischen Strafgesetzbuches (StGB; SR 311) genügend geschützt. So wird die Verletzung der datenschutzrechtlichen Schweigepflicht durch eine Amtsperson der kantonalen oder kommunalen Verwaltung fast immer bereits durch Art. 320 StGB erfasst (Kommentar DSG, a.a.O., Vorbemerkungen zum 7. Abschnitt, N 8). Es erübrigt sich damit Strafbestimmungen für Amtsgeheimnisverletzungen in das kantonale Recht aufzunehmen, dies auch für beauftragte (Privat-) Personen im Sinne von Art. 3 Ziff. 8 lit. b. Nehmen sie öffentliche Funktionen im Dienste der Gemeinwesens wahr, unterstehen sie ebenfalls dem Geltungsbereich von Art. 320 StGB: Es werden somit nur Strafnormen begründet, die sich auf Private beziehen, denen unter bestimmten Voraussetzungen Daten bekanntgegeben worden sind, diese aber nicht zum hierfür bestimmten Zweck verwendet worden sind.

Art. 35 Übergangsbestimmung

Diese Bestimmungen sollen ein möglichst reibungsloses Anpassen an das neue Gesetz beziehungsweise der bestehenden Personendatenansammlungen an die neuen Vorschriften ermöglichen. Da es dazu eines erheblichen Aufwandes bedarf und allenfalls bereichsspezifische Rechtsgrundlagen geschaffen werden müssen, rechtfertigt sich die Einräumung einer angemessenen Frist. Die unterschiedlichen Fristen erklären sich aus dem Umstand, dass der Aufsichtsstelle ebenfalls Zeit für den Aufbau ihres zentralen öffentlichen Registers einzuräumen ist.

**Art. 36 Änderung bisherigen Rechts
1. Niederlassungsgesetz**

Die datenschutzrechtlichen Vorschriften von Art. 13 und Art. 15 Abs. 2 Ziff. 5 der kantonalen Niederlassungsgesetzgebung (NG 122.1) werden durch den Erlass des Datenschutzgesetzes, welches unter anderem die Grundsätze der Datenbearbeitung und dabei vor allem auch die Bekanntgabe von Personendaten durch die kommunale Einwohnerkontrolle an Dritte im Besonderen regelt (vgl. Art. 14) hinfällig. Sie sind daher aufzuheben (Art. 13) beziehungsweise abzuändern (Art. 15 Abs. 2 Ziff. 5).

Art. 37 2. Personalgesetz

Das kantonale Gesetz über das öffentlichrechtliche Arbeitsverhältnis (Personalgesetz, PersG; NG 165.1) enthält in den Art. 74 – 77 spezialrechtliche Vorschriften über den Datenschutz. Art. 76 PersG verpflichtet den Regierungsrat, die Aufbewah-

rungsdauer von Personaldaten von Mitarbeiterinnen und Mitarbeitern zu regeln. Der Regierungsrat regelte zwar wohl gestützt darauf in § 4 der kantonalen Vollzugsverordnung zum Personalgesetz (Personalverordnung) die Übergabefrist der Personalakten zu Händen des Staatsarchivs (10 Jahre nach Austritt). Damit ist aber insbesondere nicht gesagt, welche Daten überhaupt über das Austrittsdatum hinaus aus datenschutzrechtlichen Gründen noch aufbewahrt werden dürfen und welche nicht. Art. 84 ist dementsprechend zu ergänzen. Dies umso mehr, als sich gerade bei Personaldossiers weitere datenschutzrechtliche Probleme stellen können, die es mit Vorteil in generell-abstrakter Weise in der Personalverordnung detaillierter zu regeln gilt.

Art. 38 3. Verordnung über das Staatsarchiv

§ 12 Aufgehoben

Die Bestimmungen über die Sperrfrist für die Einsichtnahme durch Dritte wird – systematisch korrekt – aus denjenigen über die Aktenablieferung der §§ 11 – 15 herausgebrochen und nach diesen in die Archivverordnung modifiziert integriert (vgl. dazu die §§ 16a ff. hiernach).

§ 16a Sperrfristen 1. Grundsatz

Da das Archivgut auch Unterlagen umfasst, die bereits vor ihrer Einlagerung im Staatsarchiv nicht öffentlich zugänglich war, werden die archivierten Akten grundsätzlich erst nach einer Sperrfrist (andernorts auch Schutzfrist genannt) von 30 Jahren zugänglich. Bis anhin betrug diese 35 Jahre; sie wird aber an die in anderen Kantonen (AG, ZH, ZG) geltende Frist angepasst. Diese Sperrfrist greift indes nicht, wenn die Akten bereits vor ihrer Archivierung öffentlich zugänglich waren.

§ 16b 2. Besonders schützenswerte Personendaten oder Persönlichkeitsprofile

Die Sperrfrist wird bei besonders schützenswerten Personendaten oder Persönlichkeitsprofilen soweit erhöht, dass garantiert ist, dass keine solchen Daten zu Lebzeiten betroffener Personen eingesehen oder bekannt gemacht werden. Dabei wird aus verwaltungsökonomischen Gründen davon abgesehen, sogenannte „dynamische Sperrfristen“ (Sperrfrist ab Todestag beziehungsweise Geburtstag der betroffenen Person) festzusetzen. Dies hätte einen erheblichen Mehraufwand für das Staatsarchiv zur Folge, weil mit der Einführung einer unbekannten Variable die Vorteile der vom Staatsarchiv verwendeten automatisierten Archivdatenbank CMISar 3 zunichte gemacht würden (vgl. dazu § 12 des Zuger Archivgesetzes vom 29. Januar 2004).

§ 16c 3. Einsichtsrecht der übergabepflichtigen Instanzen

Sind die Akten dem Staatsarchiv übergeben worden, können sie von den übergabepflichtigen Instanz jederzeit im Rahmen der dienstlichen Tätigkeit jederzeit eingesehen werden (Abs. 1); sie sind und bleiben jedoch unveränderbar (Abs. 2).

§ 16d 4. Beschränkung der Einsichtnahme

In der langen zeitlichen Betrachtung, in denen das Archiv agiert, gilt es zu beachten, dass die Gründe für den Ausschluss des Zugangs zu Unterlagen ändern können. So wie es heute Gründe gibt, den Zugang zu amtlichen Dokumenten von nicht öffentlichen Sitzungen auszuschliessen, gibt es Dokumente, die erst in zeitlicher Distanz in ihrer Bedeutung als besonders schützenswerte Daten zu bewerten sind. Dazu

kommt, dass im Laufe der Zeit das gleiche Thema und die entsprechenden Unterlagen (Beispiel Adoption) nicht mit dem gleichen Geheimhaltungsverständnis behandelt wurden. Das Staatsarchiv, welches seine Bestände kennt, trägt den besonders schutzwürdigen Interessen Rechnung, indem die Einsichtnahme eingeschränkt, aufgeschoben oder verweigert werden kann (Abs. 1). Das Verfahren richtet sich nach den Vorschriften der Datenschutzgesetzgebung, soweit Einsichtsgesuchen nicht vollumfänglich entsprochen wird und diese ganz oder teilweise abschlägig behandelt werden (Abs. 2).

Mit der Formulierung "besonders schutzwürdiges Interesse" wird darauf hingewiesen, dass nicht ein jegliches, irgendwie schützenswertes Interesse genügt. Es muss sich vielmehr um (Ausnahme-) Fälle handeln, die von entsprechend schwerwiegender Bedeutung sind. Auch der "physische" Zustand von Archivalien kann ein guter Grund sein, die Einsichtnahme einzuschränken oder zu verweigern, wenn dadurch Dokumente beispielsweise besser erhalten werden können.

§ 16e 5. Einsichtnahme vor Ablauf der Sperrfrist

Durch die Schutzfristen wird der Schutz der Persönlichkeit bei der Einsichtnahme gewahrt. Die Schutzfristen für besonders schützenswerte Daten werden in diesem Gesetz ausgeweitet und umfassen die ganze Lebenszeit. Es braucht eine Ausnahmeregelung für die Unterschreitung der Schutzfristen einerseits für die Forschung und andererseits für den Fall, dass überwiegende öffentliche oder private Interessen es gebieten. Das Gesuch muss begründet sein und wird vom Staatsarchiv beurteilt.

Abs. 3 regelt die Einsichtnahme vor Ablauf der Sperrfrist für nicht personenbezogene Zwecke wie insbesondere Forschung, Planung und Statistik. Für die Modalitäten wird auf Art. 10 des kantonalen Datenschutzgesetzes verwiesen. Entsprechend Abs. 1 ist es auch hier das Staatsarchiv, das die Einsichtnahme vor Ablauf der Schutzfristen bewilligen kann. In der historischen Forschung ist die Abgrenzung von Fällen, die entweder unter Abs. 1 oder 3 zu subsumieren sind, fließend; deshalb ist die Kompetenzzuweisung in einer Hand zu regeln.

Art. 39 4. Polizeigesetz

Art. 83 Polizeiliche Daten

Neu ist vor allem Abs. 4. Wie in der parallel laufenden Vorlage zur Revision des Polizeigesetzes betreffend ViCLAS ausgeführt ist, steht nicht zweifelsfrei fest, ob die Vorschrift von § 45 StPO eine hinreichende gesetzliche Grundlage dafür darstellt, dass eine Datenweitergabe von Strafuntersuchungsbehörden und Gerichten an die polizeiliche Ermittlungsbehörde ausreichend ist. Mithin ist es gerechtfertigt, nicht nur für ViCLAS im Speziellen, sondern im Allgemeinen für Datenbanken, die zur Erfüllung polizeilicher Aufgaben rechtmässig geführt werden – im Sinne der Amtshilfe – eine ausdrückliche gesetzliche Grundlage zu verankern, um allfällige datenschutzrechtlichen Bedenken zu zerstreuen.

Die Daten dürfen nur weitergegeben werden, wenn dies zur Erfüllung der gesetzlichen Aufgaben des Datenempfängers erforderlich ist. Die Einsicht muss aber auch in diesem Fall verhältnismässig sein. Diese Verhältnismässigkeit ist nur gegeben, wenn die Kantonspolizei ihrer gesetzlichen Aufgabe im Allgemeinen ohne Einsicht in die Untersuchungsakten der Strafverfolgungsbehörde nicht nachkommen kann, das heisst im Speziellen betreffend ViCLAS die korrekte Erfassung eines Falles beziehungsweise die Beantwortung des umfassenden Fragenkataloges in der Regel unmöglich wäre. Die Polizei hat keine Einsicht in die untersuchungsrichterlichen Einvernahmen, in die Expertisen (der Psychiatrie, der Ballistik usw.) und in alle weiteren

Untersuchungsakten, die zur Klärung des genauen Tatvorganges und der Tätermotivation unerlässlich sind.

Die Einsicht muss sodann im Einzelfall mit Begründung durch die Kantonspolizei beantragt werden und darf nur der zuständigen, für die Erfassung von in der ViC-LAS- Datenbank ausgebildeten Fachperson gewährt werden, welche die erhaltenen Informationen nicht zweckentfremden darf. Die Fachperson darf zwar Kopien der notwendigen Unterlagen anfertigen. Diese sind aber gesondert abzulegen und dürfen den anderen Mitarbeitenden des Polizeikorps nicht zugänglich gemacht werden.

Art. 84 Abrufverfahren

Der Polizei soll es gestattet sein, zwecks Personenidentifikation bei sicherheits- und kriminalpolizeilichen Ermittlungen direkt Daten der Einwohnerkontrolle abrufen zu können. Weil nicht ausgeschlossen ist, dass auch besonders schützenswerte Daten damit einhergehen, ist dieses Abrufverfahren im Polizeigesetz zu verankern. Diese Vorschrift stimmt sodann inhaltlich überein mit der Vorschrift über die Bekanntgabe von Daten über ausländische Staatsangehörige im Abrufverfahren an die Polizeibehörden der Kantone und Gemeinden nach Art. 7 Abs. 2 lit. d der ZAR-Verordnung.

Art. 85-89 Aufgehoben

Nachdem die Bearbeitung von Daten und die Kontrollrechte Betroffener bereits im Datenschutzgesetz geregelt sind und dieses auch für die polizeilichen Daten Geltung hat, kann auf die entsprechenden Vorschriften der Polizeigesetzgebung inskünftig verzichtet werden.

Art. 40 und 41

Keine Bemerkungen.

6 Auswirkungen der Vorlage

6.1 Auf den Kanton

Die Betreuung des Datenschutzes wurde – obwohl nach der kantonalen Regierungsratverordnung (NG 152.11; IV., Abs. 1 lit. b Ziff. 10) fachlich dem Amt für Justiz zugewiesen – faktisch bislang ausschliesslich vom kantonalen Rechtsdienst wahrgenommen. Sie beschränkte sich aufgrund seiner begrenzten personellen Ressourcen darauf, im Bedarfsfall Auskünfte zu erteilen.

Der Erlass des kantonalen Datenschutzgesetzes, insbesondere die Institutionalisierung einer Aufsichtsstelle mit ihren Eingriffsmöglichkeiten, wird zwangsläufig erhebliche Mehraufwendungen mit sich bringen. Dies ist nicht zuletzt der Preis für die Anbindung 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 abzuschätzen ist ausserordentlich schwierig, da vorerst – anders als in den übrigen Kantonen – zunächst noch die Register der Datensammlungen zu erstellen sind. Hernach sind die Schutzmassnahmen jeweils aufgrund von Analysen laufend anzupassen. Sie hängen von der Anzahl der eingereichten Auskunfts- respektive Einsichtsgesuche ab. Sodann wird das neue Gesetz

möglicherweise im Bereich der Recht sprechenden Organe aufgrund vermehrten Aufwands durch Rechtsmittelverfahren finanzielle Auswirkungen haben.

Die von der Konferenz der Kantonsregierungen in Auftrag gegebene Wegleitung für die kantonale Umsetzung von Schengen/Dublin im Bereich des Datenschutzes geht davon aus, dass für eine wirksame Datenschutzaufsicht in grösseren und mittleren Kantonen – dies offenbar unter der stillschweigenden Voraussetzung, dass zur Zeit bereits eine funktionierende Aufsicht besteht – ein Kontrollorgan mit mehreren Stellen, in kleineren Kantonen ein solches mit mindestens einem 50–100-%-Pensum eingerichtet werden muss. Berücksichtigt man, dass die Aufsichtsstelle nicht nur für den Kanton, sondern vor allem auch für die Gemeinden tätig sein wird, so muss für den Kanton Nidwalden für die Fachaufsicht an sich tendenziell von gegen einem 100 %-Pensum ausgegangen werden. Dazu kommen die Kosten für eine Teilzeit-Sekretariatsstelle und für die Stellvertretung, die allerdings nicht zwingend mit einem fixen Pensum beschäftigt werden muss, sondern auch bloss bei Bedarf (beispielsweise bei dauernder Krankheit oder Ausstandsgründen) zum Einsatz kommen kann. Insgesamt ist folglich mit Vollzugskosten von ca. 100'000 bis 150'000 Franken zu rechnen. In einer vergleichbaren, tendenziell aber eher geringeren Grössenordnung würden sich die Kosten bei einer interkantonalen Lösung bewegen. Ihre möglichen Vorteile im Vergleich zu einer kantonalen Lösung liegen aber vor allem darin, dass sie eine Spezialisierung und Arbeitsteilung (Recht, Informatikrevision) unter den Mitarbeitenden und einen einfacheren Erfahrungsaustausch erlaubte sowie die gegenseitige Stellvertretung erleichterte.

6.2 Auf die Gemeinden

Auch die Politischen, die Schul- sowie die Kirch- und Kapellgemeinden unterstehen den Vorschriften des Datenschutzes und hätten grundsätzlich selbst – wie der Kanton – die erforderlichen Vorkehrungen zu treffen, um insbesondere auch den Vorschriften über die Aufsichtsstelle zu entsprechen. Aufgrund der kleinräumigen Verhältnisse im Kanton Nidwalden macht es aber keinen Sinn, diese auch zu verpflichten, je eine eigene Aufsichtsstelle zu institutionalisieren. Sie werden der Aufsicht durch die kantonale Aufsichtsstelle unterstellt, nachdem auch der Kanton selbst von Gesetzes wegen verpflichtet ist, eine Aufsichtsstelle einzurichten. Damit können die Ressourcen gebündelt und bei einer Instanz konzentriert werden. Der Kanton übernimmt damit Aufgaben und die Kosten von rund 30 kommunalen Organisationen bzw. Körperschaften. Die Gemeinden sind aber gleichzeitig verpflichtet, zunächst beim Aufbau der Register der Datensammlungen (vgl. dazu Art. 19 und 20) aktiv mitzuwirken und die kantonale Aufsichtsstelle in der Folge bei all ihren Handlungen (vgl. dazu Art. 28) zu unterstützen.

7 Antrag

Der Regierungsrat beantragt dem Landrat, auf die Vorlage zum Erlass eines Gesetzes über den Datenschutz (Kantonales Datenschutzgesetz) einzutreten und dieser zuzustimmen.

Stans, 06. November 2007

REGIERUNGSRAT NIDWALDEN

Landammann

Hugo Kayser

Landschreiber

Josef Baumgartner