VERNEHMLASSUNGSBERICHT

DER REGIERUNG

BETREFFEND

DIE ABÄNDERUNG DES DATENSCHUTZGESETZES

VOM 14. MÄRZ 2002 (DSG)

Ressort Justiz

Vernehmlassungsfrist: 20. Juni 2008

INHALTSVERZEICHNIS

Beilagen:

- Text des Übereinkommens vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (LGBl. 2004 Nr. 167).
- Text des 1. Zusatzprotokolls vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (STE Nr. 108).

ZUSAMMENFASSUNG

Das Zusatzprotokoll vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitender Datenübermittlung vom 28. Januar 1981 dient der verbesserten Umsetzung des Übereinkommens. Die Verbesserung der Umsetzung ist aufgrund der steigenden Zahl von grenzüberschreitenden Datentransaktionen aus einem Vertragsstaat in einen Drittstaat oder in eine Drittorganisation nötig geworden. Einerseits werden die Zuständigkeiten der Kontrollbehörden harmonisiert; andererseits soll vermieden werden, dass Datentransfers in Drittstaaten oder an Drittorganisationen zu einer Umgehung der Gesetzgebung eines Herkunftsstaates führen, der Vertragspartei des Übereinkommens ist.

Das Übereinkommen trat für Liechtenstein am 1. September 2004 in Kraft (LGBl. 2004 Nr. 167). Mit der Ratifikation des Zusatzprotokolls bringt Liechtenstein die Absicht zum Ausdruck, das vom Europarat festgelegte Datenschutzniveau, insbesondere bei grenzüberschreitenden Datenübermittlungen, einzuhalten.

Damit Liechtenstein das Zusatzprotokoll vom 8. November 2001 ratifizieren kann, müssen einige Bestimmungen des Datenschutzgesetzes vom 14. März 2002 (DSG), LGBl. 2002 Nr. 55, angepasst werden. Die entsprechende Vernehmlassungsvorlage legt, gestützt auf dieses Zusatzprotokoll, die Kriterien für eine rechtmässige grenzüberschreitende Bekanntgabe von Daten fest und gewährt dem liechtensteinischen Datenschutzbeauftragten ein Beschwerderecht im Rahmen der Aufsicht über liechtensteinische Verwaltungsorgane.

Die EFTA Überwachungsbehörde (ESA), welche die korrekte Umsetzung des von Liechtenstein zu übernehmenden EWR-Rechts in das liechtensteinische Recht überwacht, kam bei ihrer Überprüfung des liechtensteinischen Datenschutzgesetzes zum Schluss, dass dieses die Datenschutzrichtlinie 95/46/EG in einigen Punkten nur mangelhaft in das liechtensteinische Recht umsetze. Die Vernehmlassungsvorlage enthält den aus den Gesprächen mit der ESA resultierenden Änderungsbedarf am Datenschutzgesetz.

Seit dem Erlass des DSG im Jahr 2002 konnten etliche Erfahrungen in der Anwendung des Gesetzes gesammelt werden. Die Vernehmlassungsvorlage enthält diverse auf diesen Erfahrungen beruhende Anpassungen, Vereinfachungen und Korrekturen am Datenschutzgesetz.

ZUSTÄNDIGES RESSORT

Ressort Justiz

BETROFFENE STELLEN

Stabsstelle für Datenschutz

Vaduz, 6. Mai 2008
RA 2008/1008-1731
P

1. AUSGANGSLAGE

Das Datenschutzgesetz bezweckt den Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden. Datenschutz ist somit Persönlichkeits- und Grundrechtsschutz bei der Datenbearbeitung. Die Begriffe Persönlichkeitsschutz und Grundrechtsschutz haben seit längerem ihren festen Platz in unserer Rechtstradition. Demgegenüber sind die Begriffe Datenbearbeitung und Datenschutz vergleichsweise jung. Der Schutz der Persönlichkeit ist deshalb um das Recht auf informationelle Selbstbestimmung zu erweitern. Es ist als Leistung unserer modernen Demokratie zu erkennen, dass Datenbearbeitungen Persönlichkeit und Grundrechte der Bürger verletzten können und dass mit dem Erlass des Datenschutzgesetzes entsprechende Schutzvorkehrungen getroffen wurden. Die Schutzbedürftigkeit hängt mit der ernormen Entwicklung in der Kommunikationstechnik der letzten 50 Jahre zusammen. Diese technologische Entwicklung hat auch in der demokratischen Gesellschaft Datenbearbeitungen ermöglicht, wie sie in ihrem Umfang und in ihrer Intensität früher undenkbar waren. Der Stellenwert des Datenschutzes steigt deshalb im selben Mass wie der Fortschritt in der technologische Entwicklung. Vor dieser Situation ist der Gesetzgeber daher gefordert, die Instrumente des Datenschutzes fortlaufend auf ihre Tauglichkeit hin zu überprüfen und wo nötig zu ergänzen.

2. ANLASS UND NOTWENDIGKEIT

2.1 Zusatzprotokoll zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (STE 108)

Das liechtensteinische Datenschutzgesetz vom 14. März 2002 (DSG) trat am 1. August 2002 in Kraft (LGBl. 2002 Nr. 55). Mit ihm wurde die 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 (Datenschutzrichtlinie; EWR-Rechtssammlung: Anh. XI – 5e.01) umgesetzt.

Als weiterer Schritt folgte die Ratifikation des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981 (Übereinkommen STE 108). Dieses Übereinkommen des Europarats trat für Liechtenstein am 1. September 2004 in Kraft (LGBl. 2004 Nr. 167). Angesichts des grenzüberschreitenden Informationsflusses drängte sich die internationale Zusammenarbeit auf, um ein möglichst hohes Datenschutzniveau bei gleichzeitiger Gewährleistung des freien Informationsaustausches sicherzustellen. 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. Auf dem Gebiet aller Vertragsparteien soll ein Minimum an Persönlichkeitsschutz bei der Verarbeitung von Personendaten und eine gewisse Harmonisierung des Schutzsystems sichergestellt werden; andererseits gewährleistet das Übereinkommen den internationalen Datenverkehr dadurch, dass keine Vertragspartei den Transfer von Informationen an eine andere Vertragspartei, welche den vom Übereinkommen vorgesehenen Mindestschutz gewährleistet, untersagen darf. 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 Grundfrei-

heiten (EMRK), welche Liechtenstein am 8. September 1982 ratifiziert hat (LGBl. 1982 Nr. 60/1). Seit dem Inkrafttreten des DSG am 1. August 2002 entspricht das liechtensteinische Recht den Anforderungen des Übereinkommens, indem die Richtlinie 95/46/EG vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr über das Datenschutzgesetz umgesetzt wurde.

Die EU-Richtlinie geht in ihrem Umfang weiter als das Übereinkommen STE 108. Dennoch erschien eine Ratifikation des Übereinkommens als sinnvoll, da dadurch der räumliche Schutzbereich zusätzlich um Nicht-EU-Staaten erweitert werden konnte.

Das Ministerkomitee des Europarats hat in seiner Sitzung vom 23. Mai 2001 ein Zusatzprotokoll betreffend die Kontrollbehörden und den grenzüberschreitenden Datenverkehr verabschiedet. Das Zusatzprotokoll ergänzt das Übereinkommen STE 108, indem es versucht, die Umsetzung der darin enthaltenen Grundsätze zu verbessern. Die Verbesserung der Umsetzung ist heute aufgrund der steigenden Zahl von grenzüberschreitenden Datentransaktionen aus einem Vertragsstaat in einen Drittstaat oder an eine Drittorganisation[1] nötig geworden. Sie umfasst zwei Aspekte: Einerseits geht es um eine Harmonisierung der Zuständigkeiten der Kontrollbehörden; andererseits soll vermieden werden, dass Datentransfers in Drittstaaten oder an Drittorganisationen zu einer Umgehung der Gesetzgebung eines Herkunftsstaates führen, der das Übereinkommen STE 108 unterzeichnet hat.

Das Zusatzprotokoll sieht insbesondere die Einsetzung von Kontrollbehörden vor, denen es obliegt, über die Einhaltung der Massnahmen zu wachen, welche im jeweiligen Landesrecht die im Übereinkommen und im Protokoll stipulierten Grundsätze durchsetzen sollen. Diese Behörden sollten über Untersuchungsbefugnisse verfügen sowie Klagen führen bzw. der zuständigen Gerichtsbehörde

[1] Organisationen wie z.B. die UNO

Verletzungen der einschlägigen Bestimmungen des Landesrechts zur Kenntnis bringen können. Weiter sieht das Zusatzprotokoll vor, dass der Transfer von personenbezogenen Daten an einen Datenempfänger, der vom Übereinkommen nicht erfasst ist, nur erfolgen kann, wenn der Empfängerstaat oder die Empfängerorganisation ein angemessenes Schutzniveau gewährleistet. Die Garantien können insbesondere aus entsprechend ausgestalteten Vertragsklauseln hervorgehen. Die vom Zusatzprotokoll vorgesehenen Anforderungen an die einzurichtende Aufsichtsbehörde und den grenzüberschreitenden Datenverkehr sind jenen der Datenschutzrichtlinie 95/46/EG sehr ähnlich.

Das Zusatzprotokoll kann nur von denjenigen Staaten ratifiziert werden, die auch das Übereinkommen STE 108 ratifiziert haben. Für das Inkrafttreten waren fünf Ratifikationen nötig, die seit dem 3. März 2004 vorliegen, so dass am 1. Juli 2004 das Protokoll in Kraft treten konnte. Jeder Vertragsstaat kann das Protokoll jederzeit mit einer Notifikation an das Generalsekretariat des Europarates kündigen. Bisher haben 11 Staaten das Zusatzprotokoll ratifiziert, 18 weitere Staaten haben es unterzeichnet.

Liechtenstein hat das Zusatzprotokoll noch nicht unterzeichnet. Die Unterzeichnung erfolgt vor der Ratifikation, wie dies formal vorgesehen ist, da ein Beitritt ohne Unterzeichnung für Mitgliedstaaten des Europarats nicht möglich ist. Mit der Ratifikation des Zusatzprotokolls gibt Liechtenstein seiner Absicht Ausdruck, das vom Europarat festgelegte Datenschutzniveau, insbesondere bei grenzüberschreitenden Datenübermittlungen, einzuhalten.

2.2 Mangelhafte Umsetzung der Datenschutzrichtlinie

Die EFTA Überwachungsbehörde (ESA), welche die korrekte Umsetzung des von Liechtenstein zu übernehmenden EWR-Rechts in das liechtensteinische Recht überwacht, kam bei ihrer Überprüfung des liechtensteinischen DSG zum Schluss, dass dieses die Datenschutzrichtlinie 95/46/EG in einigen Punkten nur mangelhaft in das liechtensteinische Recht umgesetzt habe. In der Folge wurden diese Punkte

zwischen den zuständigen liechtensteinischen Behörden und der ESA diskutiert und entsprechender Anpassungsbedarf festgestellt.

2.3 Vollzugserfahrungen mit dem Datenschutzgesetz

Seit dem Erlass des Datenschutzgesetzes im Jahr 2002 konnten etliche Erfahrungen in der Anwendung des Gesetzes gesammelt werden. Diese Erfahrungen sollen in die gegenständliche Revision einfliessen und eine Verbesserung sowie Vereinfachung in der Anwendung des DSG bezwecken.

3. SCHWERPUNKTE DER VORLAGE

Aufgrund der soeben unter Punkt 2. gemachten Ausführungen zum Anlass und zur Notwendigkeit ergeben sich folgende Schwerpunkte der Vorlage.

3.1 Notwendige Anpassungen in Bezug auf das Zusatzprotokoll zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

Um den Anforderungen des Zusatzprotokolls vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitender Datenübermittlung vom 28. Januar 1981 (Zusatzprotokoll) zu entsprechen und dieses Zusatzprotokoll ratifiziert werden kann, sind verschiedene Anpassungen notwendig. Dies betrifft die Art. 8 (Bekanntgabe von Personendaten ins Ausland) und 32 Abs. 1 Bst. g (Ergänzung der Aufgabenbereichs des Datenschutzbeauftragten aus der erweiterten Zuständigkeit nach Art. 8 Abs. 3) sowie die Art. 29 Abs. 5 und Art. 30 Abs. 4 (erweiterte Beschwerdemöglichkeiten des Datenschutzbeauftragten) der Vorlage. Dazu Folgendes:

Das Zusatzprotokoll verpflichtet jeden Vertragsstaat, eine oder mehrere unabhängige Aufsichtsbehörden vorzusehen (Art. 1 Abs. 1 und Abs. 3). Diese Behörden

müssen Ermittlungen durchführen und einschreiten können sowie die Befugnis haben, Klagen anzustrengen bzw. den zuständigen Justizbehörden Verstösse gegen die innerstaatlichen Rechtsvorschriften zur Umsetzung der Grundsätze des Übereinkommens oder des Zusatzprotokolls zur Kenntnis zu bringen. Jede Aufsichtsbehörde soll dazu innerhalb ihres Zuständigkeitsbereiches die Beschwerden von Personen bezüglich ihrer Rechte und Freiheiten hinsichtlich der Bearbeitung personenbezogener Daten anhören (Art. 1 Abs. 2). Die Entscheide der Aufsichtsbehörden können vor Gericht angefochten werden (Art.1 Abs. 4). Die Aufsichtsbehörden pflegen die Zusammenarbeit und insbesondere den Informationsaustausch (Art. 1 Abs. 5):

Das DSG sieht bereits zwei unabhängige Aufsichtsbehörden vor, nämlich den Datenschutzbeauftragten (Art. 28 ff. DSG) und die Datenschutzkommission (Art. 33 ff. DSG), deren Mitglieder den Bestimmungen des Gesetzes über die allgemeine Landesverwaltungspflege (LVG) unterliegen (Art. 33 Abs. 2 DSG). Der Datenschutzbeauftragte hat Untersuchungskompetenzen (Art. 29 Abs.1 bis 3 sowie Art. 30 Abs. 1 und 2 DSG) und bestimmte Eingriffsmöglichkeiten; insbesondere kann er Empfehlungen abgeben (Art. 29 Abs. 4 und 5 und Art. 30 Abs. 3 und 4 DSG). Er kann von Amtes wegen oder auf Gesuch Dritter hin tätig werden. Das geltende Recht entspricht demnach bereits in weiten Teilen den Anforderungen des Protokolls, mit einer Ausnahme: Der Datenschutzbeauftragte hat heute im Rahmen der Aufsicht nicht die Kompetenz, Beschwerde gegen Entscheide der Datenschutzkommission zu führen.

Die notwendigen Änderungen in Art. 29 Abs. 5 und Art. 30 Abs. 4 DSG, um dem Datenschutzbeauftragten die vom Zusatzprotokoll vorgesehene Beschwerdemöglichkeit zu ermöglichen, sind auch in der Vorlage enthalten, welche im Rahmen der gesetzlichen Anpassungen zu Schengen/Dublin notwendig sind. Je nach Umsetzungszeitpunkt werden diese Abänderungen aus dieser oder jener Vorlage dann herausgenommen.

3.2 Notwendige Anpassungen zur korrekten Umsetzung der Datenschutzrichtlinie

Die nachfolgend aufgeführten Punkten stellen das Resultat aus der Diskussion mit der ESA dar und resultieren aus der Zusicherung Liechtensteins, die mangelhaften Umsetzungspunkte zu bereinigen.

- Die öffentlichen Register sind nach Art. 2 Abs. 1 Bst. f DSG vom Anwendungsbereich des DSG ausgenommen. Dies geht über die von der Richtlinie zugelassenen Ausnahmen hinaus.
- Das liechtensteinische DSG sieht in Art. 4 Abs. 3 vor, dass der Zweck der Datensammlung den Betroffenen bekannt gegeben werden muss bzw. für den Betroffenen erkennbar sein muss. Die Bestimmung lässt dafür auch eine Ersichtlichkeit aus den Umständen gelten. Dies vermag dem von der Richtlinie geforderten Kriterium der Ausdrücklichkeit nicht zu genügen.
- Es fehlt eine Bestimmung, welche private Personen zur Anonymisierung oder Vernichtung von Personendaten verpflichtet, welche nicht mehr für den Zweck, für den sie erhoben wurden, benötigt werden. Diese Lücke soll durch den neuen Art. 19a geschlossen werden.
- Die in Art. 15 Abs. 3 DSG festgelegten Ausnahmen von der Verpflichtung privater Personen zur Anmeldung von Datensammlungen erwecken den Anschein, dass die Bearbeitung von nicht besonders schützenswerten Personendaten die Rechte der betroffenen Personen nicht verletzen könne, wenn diese über die Bearbeitung informiert seien oder eine entsprechende gesetzliche Bestimmung die Bearbeitung erlaube. Dies ist von der Richtlinie nicht gedeckt. Es wird deshalb ein neuer Abs. 3a in Art. 15 vorgeschlagen.
- Die Befugnisse des Datenschutzbeauftragten, im Privatrechtsbereich Abklärungen zu tätigen und Empfehlungen abzugeben, sind in Art. 30 Abs. 1 Bst. a unzulässigerweise auf den Fall der Betroffenheit „einer grösseren Anzahl

von Personen“ beschränkt. Die Befugnisse müssen auch für den Einzelfall gegeben sein; dies erfolgt durch eine Anpassung in Art. 30 Abs. 1 Bst. a.

3.3 Teilrevision des Datenschutzgesetzes aufgrund Vollzugserfahrungen

Schliesslich wird in einem dritten Schwerpunkt eine Teilrevision des Datenschutzgesetzes auf Grund der im Vollzug des Gesetzes gemachten Erfahrungen umgesetzt. Dieser umfasst diverse verfeinerte Formulierungen und Korrekturen am Gesetzeswortlaut; die Einführung einer Regelung betreffend allgemein verfügbarer Daten und die Einführung von Regelungen zur Schaffung einer Zertifizierungsmöglichkeit für datenschutzrelevante Abläufe und Strukturen.

Dieser Schwerpunkt betrifft in Art. 4 Abs. 1 und 4 die Erweiterung der Voraussetzung der Rechtmässigkeit und das Informations- und Zustimmungserfordernis für Datenbearbeitungen; in Art. 14a die Einführung eines Zertifizierungsverfahrens; in Art. 17 Abs. 2 Bst. f die Regelung allgemein zugänglicher Daten; in Art. 21 Abs. 2 Bst. b und c die Präzisierung des Ausnahmefalls und die Untersagung der Datenbearbeitung; in Art. 23 Abs. 1 Bst. c die Regelung allgemein zugänglicher Daten; in Art. 25 die Anonymisierung und Vernichtung von Daten; in Art. 32 Abs. 1 Bst. h die Ergänzung der Aufgabenbereichs des Datenschutzbeauftragten aus der erweiterten Zuständigkeit nach Art. 14a und in Art. 40 die Korrektur und Anpassung der Strafbarkeit.

4. ERLÄUTERUNGEN ZU DEN EINZELNEN ARTIKELN

Zu Art. 2 Abs. 3 Bst. f

Die ESA kritisierte die Ausnahme der öffentlichen Register des Privatrechtsvekehrs vom Anwendungsbereich des DSG, wie sie in Art. 2 Abs. 1 Bst. f statuiert ist. Mit der Aufhebung von Bst. f wird dieser Kritik nachgekommen.

Zu Art. 2 Abs. 3 Bst. g

Buchstabe g wurde anlässlich der zweiten Lesung des DSG eingefügt und wie folgt begründet:

„Aufgrund der geltenden Gesetzgebung können Parteien, gegen welche aufgrund des Sorgfaltspflichtgesetzes Massnahmen ergriffen werden, u.U. Einsicht in die über sie im Rahmen solcher Verfahren angelegten Daten verlangen. Dies ist nicht im öffentlichen Interesse: Solche Daten sollen nämlich effizient und ohne „tipping off" (vorzeitige Information des Klienten) durchgeführt werden können. Im Gegensatz zum schweizerischen GwG [Geldwäschereigesetz] existieren im SPG [Sorgfaltspflichtgesetz] keine Datenschutzbestimmungen, weshalb eine Bestimmung mit Bezug auf das SPG hier aufzunehmen ist."

Diese Argumentation betraf noch das alte Gesetz vom 22. Mai 1996 über die beruflichen Sorgfaltspflichten bei der Entgegennahme von Vermögenswerten (Sorgfaltspflichtgesetz), welches inzwischen durch das Gesetz vom 26. November 2004 über die beruflichen Sorgfaltspflichten bei Finanzgeschäften (Sorgfaltspflichtgesetz, SPG) ersetzt wurde.

Es macht keinen Sinn, Personendaten, die nach SPG anzulegen sind, vom DSG mit der Argumentation auszunehmen, dies müsse geschehen, weil das SPG keine Datenschutzbestimmungen enthalte. Auch wenn das SPG Datenschutzbestimmungen enthält - was das neuere SPG vom 26. November 2004 auch tut - ist es nicht sinnvoll, es vom Geltungsbereich des DSG auszunehmen, da das SPG als Spezialgesetz dem DSG vorgeht und das DSG nur ergänzend zur Anwendung kommt (vgl. Art. 2 Abs. 4 DSG).

Wenn es gemäss der zitierten Argumentation ausserdem im öffentlichen Interesse liegt, dass eine Einsicht (Auskunft) wegen der Gefahr eines „tipping off" unterbleiben soll, dann kann auf Art. 12 Abs. 2 Bst. a DSG verwiesen werden, wonach ein überwiegendes öffentliches Interesse Behörden eine Einschränkung oder Verweigerung der Auskunft erlaubt. Auch sieht Art. 12 weitere Gründe für eine Aus-

kunftseinschränkung vor, so z.B. behördlich angeordnete Informationssperren (Abs. 1 Bst b) oder die Gefährdung des Zwecks einer Untersuchung (Abs. 2 Bst b). Davon unberührt bleiben selbstverständlich auch Bestimmungen über die Akteneinsicht bei laufenden Verfahren.

Daher ist Art. 2 Abs. 3 Bst. g aufzuheben.

Zu Art. 4 Abs. 1, 3 und 4

In Abs. 1 ist das Wort „beschafft“ durch „bearbeitet“ zu ersetzen. Es handelt sich bei dieser Anpassung um die Korrektur eines redaktionellen Versehens. Es hat nicht nur die Beschaffung von Personendaten, sondern natürlich deren Bearbeitung insgesamt rechtmässig zu erfolgen.

Durch den Wegfall des Textteiles „aus den Umständen ersichtlich“ in Abs. 3 wird den Bedenken der ESA entsprochen, dass diese Formulierung bezüglich der durch die Richtlinie geforderten Ausdrücklichkeit der Bekanntgabe bzw. Ersichtlichkeit des Zwecks der Datenbearbeitung nicht genüge.

Vorweg ist darauf hinzuweisen, dass Abs. 4 der Vernehmlassungsvorlage das geltende Recht nicht ändert, sondern lediglich den Begriff „Zustimmung“ klärt.

Das Erfordernis der Zustimmung als Bedingung für die Datenbearbeitung wird vom geltenden DSG (Art. 17 Abs. 1, Art. 21 Abs. 2 Bst. c) und der vorliegenden Vernehmlassungsvorlage (Art. 8 Abs. 2 Bst. b) wiederholt aufgestellt. Dem Begriff der „Zustimmung“ zur Datenbearbeitung kommt in der Praxis grosse Bedeutung zu. Die Zustimmung der betroffenen Personen ist für die Daten bearbeitenden privaten Personen der am häufigsten vorliegende Rechtfertigungsgrund für die Datenbearbeitung. Deshalb sieht Art. 4 Abs. 4 der Vernehmlassungsvorlage vor, diesen Begriff zu klären.

Abs. 4 definiert, unter welchen Voraussetzungen die Zustimmung als gültig gelten kann. Es geht somit weder darum, die Zustimmung zur Bedingung für jede Datenbearbeitung zu erheben, noch geht es darum, gegenüber dem geltenden Recht

weitergehende Anforderungen aufzustellen. Der Begriff der Zustimmung orientiert sich an demjenigen der „Einwilligung des aufgeklärten Patienten“[2], und zwar in dem Sinne, dass die betroffene Person über alle Informationen im konkreten Fall verfügen muss, die erforderlich sind, damit sie eine freie Entscheidung treffen kann. Der Begriff „freiwillig“ entspricht im Übrigen auch der im Gemeinschaftsrecht verwendeten Terminologie. Das bedeutet insbesondere, dass die betroffene Person über mögliche negative Folgen oder Nachteile informiert sein muss, die sich aus der Verweigerung ihrer Zustimmung ergeben können. Die alleinige Tatsache, dass eine Verweigerung einen Nachteil für die betroffene Person nach sich zieht, kann dagegen die Gültigkeit der Zustimmung nicht beeinträchtigen. Dies ist nur dann der Fall, wenn dieser Nachteil keinen Bezug zum Zweck der Bearbeitung hat oder diesem gegenüber unverhältnismässig ist. So gibt eine Person, die einem Kreditinstitut das Einverständnis zur Überprüfung ihrer Kreditwürdigkeit erteilt, um eine Kreditkarte zu erhalten, ihre Zustimmung freiwillig. In einer solchen Situation ist der aus der Nichtzustimmung resultierende Nachteil gegenüber dem Zweck der Bearbeitung verhältnismässig. Dagegen kann der Arbeitnehmer, der gezwungen ist, in eine nicht im Arbeitsvertrag vorgesehene Datenbearbeitung einzuwilligen, weil ihm die Entlassung angedroht wird, diese Zustimmung nicht freiwillig erteilen. Der Nachteil, der aus einer Verweigerung der Zustimmung resultieren würde, wäre eindeutig unverhältnismässig. Die Einwilligung ist nicht an eine bestimmte Form gebunden und kann stillschweigend bzw. durch konkludentes Handeln erfolgen, sofern es nicht um die Bearbeitung von besonders schützenswerten Daten oder Persönlichkeitsprofilen geht. Bereits heute wird gemäss dem Verhältnismässigkeitsgrundsatz davon ausgegangen, dass die Zustimmung umso klarer zu erfolgen hat, je sensibler die fraglichen Personendaten sind.

---

[2] Wie zum Beispiel vom Schweizerischen Bundesgericht insbesondere in BGE 117 Ib 197; BGE 114 Ia 350 E. 6; BGE 119 II 456 definiert.

Zu Art. 8

Das Zusatzprotokoll verpflichtet die Vertragsstaaten sicherzustellen, dass personenbezogene Daten nur dann an Empfänger übermittelt werden, die der Rechtshoheit eines Staates oder einer Organisation unterliegen, welche nicht Vertragspartei des Übereinkommens sind, wenn dieser Staat bzw. diese Organisation einen adäquaten Schutz für die beabsichtigte Datenübermittlung gewährleistet (Art. 2 Abs. 1). Die Vertragsstaaten können im innerstaatlichen Recht Abweichungen von diesem Grundsatz vorsehen, um bestimmten Interessen der Betroffenen oder legitimen überwiegenden Interessen, insbesondere wichtigen öffentlichen Interessen, Rechnung zu tragen (Art. 2 Abs. 2 Bst. a). Desgleichen können sie die Übermittlung zulassen, sofern von der für die Übermittlung verantwortlichen Person Sicherheitsvorkehrungen getroffen werden (die sich insbesondere aus vertraglichen Klauseln ergeben können) und diese nach Auffassung der zuständigen Behörde ausreichend sind (Art. 2 Abs. 2 Bst. b).

Ob das Schutzniveau im Empfängerstaat oder bei der Empfängerorganisation angemessen ist, ist mit Blick auf die gesamten Umstände der Datenübermittlung zu prüfen. Diese Prüfung umfasst auch die Berücksichtigung der im Übereinkommen STE 108 und im Zusatzprotokoll aufgestellten Grundsätze in der Gesetzgebung sowie der Rechtspraxis des Empfängerstaates. Ebenfalls ist zu berücksichtigen, wie die betroffene Person bei Nichteinhaltung dieser Grundsätze ihre Interessen wahren kann. Die zuständige Behörde eines Vertragsstaates kann die Angemessenheit des Schutzniveaus für bestimmte Staaten oder Organisationen als Ganzes evaluieren.

Bei der Bestimmung der Abweichungen vom Grundsatz des angemessenen Schutzniveaus verfügen die Vertragsstaaten über einen Ermessensspielraum. Solche Abweichungen können vorgesehen werden, um ein wichtiges öffentliches Interesse im Sinne von Art. 8 Abs. 2 der EMRK oder Art. 9 Abs. 2 des Übereinkommens STE 108 zu schützen. Ausnahmen sind ebenfalls möglich, um bestimmten Interessen der betroffenen Person Rechnung zu tragen (z.B. die Erfüllung ei-

nes Vertrags, der Schutz lebenswichtiger Interessen der betroffenen Person oder das Vorliegen der Zustimmung der betroffenen Person).

Das liechtensteinische DSG regelt schon die Übermittlung von personenbezogenen Daten ins Ausland; die Regelung entspricht aber nicht voll dem Zusatzprotokoll. Art. 8 DSG untersagt derzeit die Bekanntgabe von Personendaten ins Ausland, wenn die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, namentlich weil ein Datenschutz fehlt, der dem liechtensteinischen gleichwertig ist. Andererseits muss, wer Datensammlungen ins Ausland übermitteln will, dies dem Datenschutzbeauftragten vorher melden, wenn für die Bekanntgabe keine gesetzliche Pflicht besteht und die betroffenen Personen davon keine Kenntnis haben (Art. 8 Abs. 2 DSG).

Die bisherige Verpflichtung, dem Datenschutzbeauftragten die Bekanntgabe von Personendaten ins Ausland zu melden, hat sich in der Praxis nicht bewährt. Nur wenige Unternehmen erstatten diese Meldung und der Datenschutzbeauftragte verfügt – vor allem in personeller Hinsicht – nicht über die erforderlichen Mittel, um Kontrollen durchzuführen. Dies ist einer der Gründe, warum die Vorlage diese Meldepflicht zu Gunsten einer Sorgfaltspflicht aufgibt, die private Personen und Behörden trifft, welche Personendaten ins Ausland übermitteln. Die Sorgfaltspflicht ist verbunden mit einer Bewilligungspflicht, die im Gegensatz zur bisherigen Meldepflicht allerdings nur noch punktuell besteht.

Art. 8 Abs. 1 der Vernehmlassungsvorlage verlangt als grundsätzliche Voraussetzung für eine gesetzeskonforme Datenübermittlung ins Ausland, dass die Gesetzgebung im Bestimmungsland einen angemessenen Schutz gewährleistet. Dies bedeutet aber im Ergebnis nicht, dass gegenüber dem geltenden Recht – wo ein dem liechtensteinischen Recht gegenüber gleichwertiger Datenschutz verlangt wird – eine Verschärfung der Anforderungen für eine grenzüberschreitende Bekanntgabe vorgenommen wird. Abs. 2 der Vernehmlassungsvorlage enthält – anders als das geltende Recht – eine Liste der alternativen Bedingungen, unter welchen die Be-

kanntgabe von persönlichen Daten ins Ausland erlaubt ist. Dadurch verdeutlicht die Vernehmlassungsvorlage die verschiedenen Möglichkeiten der Sicherstellung einer gesetzeskonformen Übermittlung und lässt die Inhaber der Datensammlungen in der Wahl ihrer Mittel frei. Auch mit der Verwendung des Begriffes „bekannt geben“ statt wie im geltenden Recht „übermitteln“ wird keine materielle Änderung angestrebt, sondern lediglich durch die Verwendung des in Art. 3 DSG definierten Begriffes die Terminologie vereinheitlicht.

Die Gesetzgebung im Empfängerstaat gewährleistet dann ein „angemessenes Schutzniveau“, wenn sie von der EU als gleichwertig eingestuft wurde oder den Anforderungen des Übereinkommens STE 108 entspricht. Darüber hinaus ist aber insbesondere zu berücksichtigen, wie diese Gesetzgebung in der Praxis umgesetzt wird. Privatpersonen und Behörden, welche Personendaten ins Ausland übermitteln, müssen mit angemessenen Mitteln gewährleisten, dass die Übermittlung der Daten die Persönlichkeit der betroffenen Personen nicht schwerwiegend gefährdet. Art. 8 stellt damit Anforderungen auf, welche denen der Datenschutzrichtlinie 95/46/EG entsprechen. Das Datenschutzrecht Liechtensteins wird damit konform mit dem Zusatzprotokoll zum Übereinkommen STE 108.

Nach Art. 8 Abs. 2 Bst. a ist eine Bekanntgabe ins Ausland beim Fehlen einer Gesetzgebung mit angemessenem Schutz zulässig, wenn andere hinreichende Garantien vorliegen. Solche können sich beispielsweise aus einem Verhaltenskodex ergeben, d.h. aus einem Regelwerk, dem sich Private freiwillig unterstellen können, wie etwa dem „Safe Harbor Privacy Framework“, das zwischen der EU-Kommission und den USA ausgehandelt wurde, dem die Empfängerorganisation oder der ausländische Staat verpflichtet ist. Wer Personendaten ins Ausland übermittelt, verfügt also über einen grossen Handlungsspielraum, doch haftet er für Nachteile, die sich aus einer Verletzung der Sorgfaltspflicht ergeben können. Es ist grundsätzlich Sache desjenigen, welcher Personendaten ins Ausland übermittelt, nachzuweisen, dass er alle erforderlichen Massnahmen getroffen hat, um ein angemessenes Schutzniveau zu gewährleisten.

Abs. 2 erlaubt den grenzüberschreitenden Datenverkehr unter bestimmten Voraussetzungen auch dann, wenn die Anforderungen von Abs. 1 nicht erfüllt sind. Die in den Buchstaben a bis g aufgestellten Bedingungen entsprechen teilweise den Rechtfertigungsgründen von Art. 17 Abs. 1 und 2 DSG. Im Gegensatz zur Enumeration der überwiegenden Interessen gemäss Art. 17 Abs. 2 DSG ist die Aufzählung der Bedingungen in Art. 8 Abs. 2 der Vernehmlassungsvorlage aber abschliessend. Es ist darauf hinzuweisen, dass es sich ausschliesslich um alternative Bedingungen handelt.

Abs. 2 Bst. b betrifft eine konkrete ausservertragliche Situation. Der Ausdruck „im Einzelfall“ ist in dem Sinne weit zu interpretieren als nicht jede einzelne grenzüberschreitende Datenübermittlung, sondern auch eine Gesamtheit von Übermittlungen erfasst werden kann. So ist zum Beispiel die Übermittlung von mehreren Protokollen einer Arbeitsgruppe, der Personen aus verschiedenen Ländern angehören, zulässig, ohne dass die Zustimmung jeder betroffenen Person für die Übermittlung jedes Dokuments eingeholt werden muss.

Abs. 2 Bst. c sieht vor, dass im Rahmen einer vertraglichen Beziehung Personendaten ins Ausland bekannt gegeben werden können, wenn die Bearbeitung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrages steht und es sich um Personendaten des Vertragspartners handelt. Es ist darauf hinzuweisen, dass diese Bestimmung nur Anwendung findet, wenn die Bekanntgabe von Personendaten ins Ausland für den Abschluss oder den Vollzug eines Vertrages unabdingbar ist.

In Abs. 2 Bst. d werden die Rechtfertigungsgründe des überwiegenden öffentlichen Interesses und des Feststellens, Ausübens und Durchsetzens von Rechtsansprüchen vor Gericht analog zur den Art. 17 und 18 auch für die Bekanntgabe ins Ausland aufgenommen.

Abs. 2 Bst. e lässt die grenzüberschreitende Bekanntgabe von Personendaten zu, wenn sie im Einzelfall erforderlich ist, um das Leben oder die körperliche Integri-

tät der betroffenen Person zu schützen. Eine Übermittlung ist gestützt auf diese Bestimmung also einzig dann zulässig, wenn es darum geht, lebenswichtige Interessen der betroffenen Person zu schützen. Buchstabe e will jene Situation regeln, in welcher die betroffene Person nicht in der Lage ist, ihre eigenen Interessen geltend zu machen und vermutet werden kann, dass sie ihre Zustimmung zu einer solchen Datenübermittlung gegeben hätte. Der Ausdruck „Schutz des Lebens oder der körperlichen Integrität“ entspricht dem Begriff „Schutz lebenswichtiger Interessen“, der im Gemeinschaftsrecht verwendet wird (Art. 26 Abs. 1 Bst. e und Abs. 7 Bst. d der Richtlinie 95/46/EG).

In Abs. 2 Bst. f wird der Rechtfertigungsgrund der durch die betroffenen Person bereits allgemein zugänglich gemachten Daten aufgenommen. Dieser Rechtfertigungsgrund folgt dem bereits bestehenden Grundsatz, wie er im DSG in den Art. 16 Abs. 3; 17 Abs. 2 Bst. f und 21 Abs. 2 Bst. c bereits besteht.

Abs. 2 Bst. g stellt eine auf Konzerne reduzierte Lösung nach Bst. a dar. Daten sollen konzernintern grenzüberschreitend bekannt gegeben werden können, solange konzernweit ein einheitlicher angemessener Datenschutz gewährleistet ist und die Daten nicht aus dem Konzern nach aussen weitergegeben werden. Der Konzernbegriff entspricht demjenigen des Gesellschaftsrechts.

Auf europäischer Ebene ergibt sich aus Art. 2 Abs. 2 Bst. b des Zusatzprotokolls, dass die zuständige Behörde überprüfen können muss, ob die Schutzmassnahmen nach Bst. a angemessen sind, wenn die Gesetzgebung des Empfängerstaates keinen genügenden Schutz bietet. Ebenso sieht die Richtlinie 95/46/EG in Art. 26 Abs. 2 und 3 vor, dass ein Mitgliedstaat solche Ausnahmen zu prüfen und zu genehmigen hat und er der Kommission (bzw. der EFTA-Überwachungsbehörde) die genehmigten Ausnahmen notifizieren muss.

Aus diesem Grund sieht die Vernehmlassungsvorlage eine Genehmigungspflicht vor. Nach Art. 8 Abs. 3 der Vernehmlassungsvorlage muss der Inhaber der Datensammlung über die von ihm vorgesehenen Garantien im Sinne von Art. 8 Abs. 2

Bst. a um eine Begutachtung durch den Datenschutzbeauftragten und eine Bewilligung durch die Regierung besorgt sein. Gleiches gilt für grenzüberschreitende Datenbekanntgabe gestützt auf Art. 8 Abs. 2 Bst. g an eine Konzerngesellschaft, die sich in einem Land befindet, in dem eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet.

Die Verordnung der Regierung wird präzisieren, wie das Bewilligungsverfahren abzulaufen hat. So könnte z.B. vorgesehen werden, dass eine einmalige Bewilligung genügt, wenn eine Firma allgemeine und verbindliche Regeln für die Übermittlung aufgestellt hat oder wenn regelmässig bestimmte Standardvertragsklauseln verwendet werden. Beim Datentransfer zwischen Konzerngesellschaften wird eine einmalige Bewilligung über die für die beteiligten Firmen verbindlichen Datenschutzregeln genügen. Es wird darauf zu achten sein, dass das Verfahren der Bewilligung möglichst einfach ausgestaltet wird.

Zu Art. 14a

Mit der hier neu vorgeschlagenen Bestimmung wird ein Element der Selbstregulierung ins Datenschutzgesetz eingeführt. Damit soll die Selbstverantwortung der Inhaber der Datensammlungen gestärkt und der Wettbewerb stimuliert werden. Dies trägt zu einer kontinuierlichen Verbesserung von Datenschutz und Datensicherheit bei; bestehende Defizite beim Vollzug der einschlägigen Gesetzgebung können so abgebaut werden. Darüber hinaus führt das Konzept der Selbstkontrolle bis zu einem gewissen Grad zu einer Berücksichtigung der technologischen Entwicklung.

Abs. 1 hält das Grundprinzip fest. Gefördert werden sollen sowohl Zertifizierungsverfahren von datenschutzrelevanten betrieblichen Abläufen bzw. Organisationsstrukturen (Datenschutz-Audits) als auch die Evaluation informatiktechnischer Systeme oder Programme – also von Produkten – hinsichtlich der Einhaltung von Datenschutzstandards. Das Zertifizierungsverfahren soll, wenn festgestellt wird, dass die einschlägigen gesetzlichen und technischen Normen und

Standards eingehalten werden, zur Vergabe eines Datenschutz-Qualitätszeichens (Datenschutz-Label) führen. Diese Auszeichnung kann durch zertifizierte Firmen insbesondere zu Werbezwecken verwendet und dazu der Öffentlichkeit zur Kenntnis gebracht werden.

Damit für Behörden und Firmen ein Anreiz für die Zertifizierung besteht, kann eine erfolgte Zertifizierung mit Erleichterungen belohnt werden. Denkbar ist insbesondere eine Ausnahme von der Meldepflicht und der Registrierung nach Art. 15 Abs. 6 DSG.

Die Stellen, die solche Zertifizierungsverfahren durchführen, müssen gegenüber den zu bewertenden Privaten oder Behörden vor allem organisatorisch, aber auch faktisch unabhängig sein. Die Anerkennung der Zertifizierungsstellen wird durch die Regierung in der Verordnung zu regeln sein (Abs. 2). Denkbar ist etwa, dort vorzusehen, dass die Zertifizierungsstellen über eine Akkreditierung verfügen müssen.

Darüber hinaus hat der Datenschutzbeauftragte zu überprüfen, ob Bewertungsverfahren und Vergabe der Gütesiegel mit dem geltenden Recht vereinbar sind (vgl. Art. 32 Abs. 1 Bst. h der Vernehmlassungsvorlage). Er kann mit den vom DSG vorgesehenen Instrumenten eingreifen (insb. Abgabe von Empfehlungen; vgl. Art. 29 und 30 DSG). Der Datenschutzbeauftragte wird aber nicht selbst als zertifizierende Instanz auftreten.

Zu Art. 15 Abs. 3a

Der eingeschobene neue Abs. 3a regelt die weiteren Sammlungen privater Personen, welche nicht bereits von Abs. 3 erfasst werden. Damit wird die von der ESA kritisierte Lücke geschlossen, wonach Sammlungen die nicht unter Abs. 3 fallen, keinerlei Anmeldung unterliegen, obwohl auch diese die Persönlichkeitsrechte von betroffenen Personen zu verletzen geeignet sein können und deshalb nicht generell von der Meldung auszunehmen sind. Da es aber Sammlungen gibt, welche nicht geeignet sind, die Persönlichkeitsrechte von betroffenen Personen zu

verletzen - und deren Meldung somit nur eine unangemessene Verwaltungsformalität darstellen würde - wird für die Festlegung von Ausnahmen auf die bestehende Verordnungskompetenz der Regierung in Abs. 6 verwiesen. Die Regierung hat bislang (auf Grund der Lücke) von dieser Kompetenz zur Befreiung privater Sammlungen von der Meldung nur im Fall der Medien (vgl. Art. 4 Datenschutzverordnung vom 9. Juli 2002 (DSV), LGBl. 2002 Nr. 102) Gebrauch gemacht.

Zu Art. 17 Abs. 2 Bst. f und Art. 23 Abs. 1 Bst. c

Die Formulierung betreffend Daten, welche eine betroffene Person „allgemein zugänglich gemacht hat“, hat sich in der Praxis als zu eng erwiesen. Die enthaltene Bedingung, dass die Daten von der betroffenen Person allgemein zugänglich gemacht wurden, erfasst jene Daten nicht, welche überhaupt öffentlich zugänglich sind, und macht eine Erweiterung nötig. Durch die Einführung der Formulierung „allgemein zugänglich sind“ werden auch die zugänglich gemachten Daten erfasst und somit eine umfassende Regelung geschaffen. Dies stellt keine Schwächung des Persönlichkeitsschutzes der betroffenen Personen dar, da diese nach wie vor kontrollieren können, welche Daten sie selbst der Öffentlichkeit bekannt geben. Es ist festzuhalten, dass eine solche Bekanntgabe auch keinen Freipass darstellt, vgl. dazu Art. 16 Abs. 3 DSG, wonach die Bearbeitung solcher Daten „in der Regel“ keine Persönlichkeitsverletzung darstellt.

Mit der neuen Formulierung soll im Sinne einer grosszügigeren Praxis und Klarstellung eine generelle Möglichkeit zur Datenbearbeitung für öffentlich zugängliche Daten geschaffen werden, wie sie auch in anderen Ländern mit gleichem Datenschutzrecht besteht (z.B.: Deutschland, § 28 Bundesdatenschutzgesetz). Zu denken ist dabei an die den Privaten oder der Wirtschaft zugänglichen öffentlichen Daten wie z.B. Angaben aus Massenmedien, Lexika, Telefonverzeichnisse, Dokumentationen, Internetseiten oder öffentlich zugängliche Register.

Zu Art. 19a

Die ESA kritisierte, dass die in Art. 25 DSG enthaltene Verpflichtung für Behörden, nicht mehr notwendige Daten löschen oder anonymisieren zu müssen, nicht auch in analoger Form für die Datenbearbeitung durch Private gelte. Die Datenschutzrichtlinie 95/46/EG schreibe dies in Art. 6 Abs.1 Bst. e generell vor. Es fehle deshalb im DSG eine analoge Bestimmung für Private. Dieser Kritik wird mit der Einführung des Art. 19a Rechnung getragen.

Die Bestimmung des Art. 19a sieht eine mehrstufige Lösung vor, womit unterschiedlichen Umständen Rechnung getragen werden kann. Als geringster Eingriff ist die Sperre der Daten vorgesehen. Diese wird immer dann anzuwenden sein, wenn die Daten auf Grund gewisser Umstände weiter aufbewahrt werden müssen, obwohl diese nicht mehr unmittelbar benötigt werden. Gründe dafür können gesetzliche Bestimmungen, Vertrags- oder Standespflichten oder schutzwürdige Interessen des Betroffenen sein. Es ist aber auch denkbar, dass auf Grund der Art der Speicherung der Daten, diese nur mit einem unverhältnismässig hohen Aufwand anonymisiert oder vernichtet werden können. In einem solchen Fall ist anstatt einer Löschung sicherzustellen, dass niemand mehr diese Daten einsehen kann.

Als stärkerer Eingriff ist die Anonymisierung der Daten vorgesehen. Dabei verlieren die Daten ihren Bezug zu einer bestimmten Person. Dieser Schritt wird immer dann zu wählen sein, wenn ein Personenbezug nicht mehr nötig ist, die Daten selbst aber z.B. für statistische Zwecke nötig sind.

Schliesslich sind Daten zu vernichten (löschen), wenn sie tatsächlich nicht mehr benötigt werden und keiner der oben genannten Gründe für eine mildere Handhabung vorliegt.

Zu Art. 21 Abs. 2 Bst. b und c

Abs. 2 erfährt einige präzisierende Änderungen.

In Bst. b wird präzisiert, dass die Regierung nur ausnahmsweise im Einzelfall Bewilligungen zur Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen erteilen kann.

In Bst. c wird dem Recht der betroffenen Person, die Bearbeitung zu untersagen, Rechnung getragen. In Analogie zur für den Privatsektor geltenden Regelung (Art. 16 Abs. 3 DSG) ist es gerechtfertigt, dass das Recht der betroffenen Person, sich der Bearbeitung zu widersetzen, selbst dann stärker gewichtet wird, wenn sie ihre Daten allgemein zugänglich gemacht hat. Mit der Entwicklung des Internet nimmt die Bearbeitung von besonders schützenswerten Personendaten eine Dimension an, die der Kontrolle der betroffenen Personen entgleiten kann. Dies rechtfertigt, dass eine Bearbeitung auch untersagt werden kann, obwohl die fraglichen Daten allgemein zugänglich gemacht worden sind.

Zu Art. 25

Art. 25 übernimmt auf Gesetzesstufe unverändert die heute geltende Bestimmung des Art. 27 der DSV. Dadurch werden die inhaltlich praktisch identischen Normen in einer einzigen Bestimmung vereint, was die Übersicht in der Datenschutzgesetzgebung verbessert.

Zu Art. 29 Abs. 5

Das Zusatzprotokoll verpflichtet jeden Vertragsstaat, eine oder mehrere unabhängige Aufsichtsbehörden vorzusehen (Art. 1 Abs. 1 und Abs. 3). Diese Behörden müssen Ermittlungen durchführen und einschreiten können sowie die Befugnis haben, Klagen anzustrengen bzw. den zuständigen Justizbehörden Verstösse gegen die innerstaatlichen Rechtsvorschriften zur Umsetzung der Grundsätze des Übereinkommens oder des Zusatzprotokolls zur Kenntnis zu bringen. Jede Aufsichtsbehörde soll dazu innerhalb ihres Zuständigkeitsbereiches die Beschwerden von Personen bezüglich ihrer Rechte und Freiheiten hinsichtlich der Bearbeitung personenbezogener Daten anhören (Art. 1 Abs. 2). Die Entscheide der Aufsichtsbehörden können vor Gericht angefochten werden (Art.1 Abs. 4). Die Aufsichts-

behörden pflegen die Zusammenarbeit und insbesondere den Informationsaustausch (Art. 1 Abs. 5):

Das DSG sieht bereits zwei unabhängige Aufsichtsbehörden vor, nämlich den Datenschutzbeauftragten (Art. 28 ff. DSG) und die Datenschutzkommission (Art. 33 ff. DSG), deren Mitglieder den Bestimmungen des Gesetzes über die allgemeine Landesverwaltungspflege (LVG) unterliegen (Art. 33 Abs. 2 DSG). Der Datenschutzbeauftragte hat Untersuchungskompetenzen (Art. 29 Abs.1 bis 3 sowie Art. 30 Abs. 1 und 2 DSG) und bestimmte Eingriffsmöglichkeiten; insbesondere kann er Empfehlungen abgeben (Art. 29 Abs. 4 und 5 und Art. 30 Abs. 3 und 4 DSG). Er kann von Amtes wegen oder auf Gesuch Dritter hin tätig werden. Das geltende Recht entspricht demnach bereits in weiten Teilen den Anforderungen des Protokolls, mit einer Ausnahme: Der Datenschutzbeauftragte hat heute im Rahmen der Aufsicht nicht die Kompetenz, Beschwerde gegen Entscheide der Datenschutzkommission zu führen.

Die Änderungen in Art. 29 Abs. 5 und Art. 30 Abs. 4 DSG gewähren dem Datenschutzbeauftragten die vom Zusatzprotokoll vorgesehene Beschwerdemöglichkeit.

Zu Art. 30 Abs. 1 Bst. a und Abs. 4

Unter Berücksichtigung der Kritik der ESA wird durch die Abänderung des Textteiles „einer grösseren Anzahl von“ in „einer oder mehrerer“ sichergestellt, dass der Datenschutzbeauftragte auch tätig werden kann, wenn die Bearbeitungsmethoden geeignet sind, die Persönlichkeit auch nur einer einzelnen Person zu gefährden.

Betreffend Abs. 4 sei auf die vorgehenden Erläuterungen zu Art. 29 Abs. 5 verwiesen.

Zu Art. 32 Abs. 1 Bst. g und h

In Bst. g wird die Liste der weiteren Aufgaben des Datenschutzbeauftragten nach Artikel 32 im Hinblick auf Art. 8 Abs. 1 und 3 der Vernehmlassungsvorlage er-

gänzt. In Bst. h wird die Liste der weiteren Aufgaben des Datenschutzbeauftragten nach Artikel 32 im Hinblick auf Art. 14a der Vernehmlassungsvorlage ergänzt bzw. präzisiert.

Zu Art. 40

Die Vernehmlassungsvorlage erweitert die Strafbarkeit auf Fehlverhalten bei der Informationspflicht nach Art. 5. Obwohl der Sachtitel des Art. 40 auch von der Verletzung der Informationspflicht spricht, war der entsprechende Artikel im Gesetzestext nicht aufgezählt. Der Begriff der unvollständigen Auskunft umfasst auch die Verletzung der Pflicht zur vorgängigen Information über die geplante Datenbearbeitung nach Art. 5.

Der in Art. 8 vorgenommene Wechsel vom System einer Meldepflicht zu Gunsten einer Sorgfaltspflicht verbunden mit einer punktuellen Bewilligungspflicht (vgl. Ausführungen zu Art. 8), führt in Artikel 40 zu einer notwendigen begrifflichen Anpassung. Die Strafbarkeit der Nichtmeldung von Datenbekanntgaben ins Ausland wurde in Abs. 2 aus Bst. a gelöscht und neu mit Bst. c die Strafbarkeit einer Datenbekanntgabe ins Ausland ohne Bewilligung hinzugefügt.

5. VERFASSUNGSMÄSSIGKEIT

Der Vernehmlassungsvorlage und der Ratifikation des Zusatzprotokolls stehen keine Bestimmungen der Verfassung entgegen.

6. VERNEHMLASSUNGSVORLAGE

Gesetz

vom …

über die Abänderung des Datenschutzgesetzes

Dem nachstehenden vom Landtag gefassten Beschluss erteile Ich Meine Zustimmung:

I.

Abänderung bisherigen Rechts

Das Datenschutzgesetz (DSG) vom14. März 2002, LGBl. 2002 Nr. 55, in der geltenden Fassung, wird wie folgt abgeändert:

Art. 2 Abs. 3 Bst. f und g

f) Aufgehoben

g) Aufgehoben

Art. 4 Abs. 1, 3 und 4

1) Personendaten dürfen nur rechtmässig bearbeitet werden.

3) Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde oder gesetzlich vorgesehen ist.

4) Ist für die Bearbeitung von Personendaten die Zustimmung der betroffenen Person erforderlich, so ist diese Zustimmung erst gültig, wenn sie nach angemessener Information freiwillig erfolgt. Bei der Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen muss die Zustimmung ausdrücklich erfolgen.

Art. 8 (neu)

Bekanntgabe ins Ausland

1) Personendaten dürfen nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, namentlich weil im Empfängerstaat eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet. Dies gilt nicht im Verhältnis zu Mitgliedstaaten des EWR-Abkommens.

2) Fehlt eine Gesetzgebung, die einen angemessenen Schutz gewährleistet, können persönliche Daten ins Ausland nur bekannt gegeben werden, wenn:

a) der für die Verarbeitung Verantwortliche hinreichende Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten, sowie hinsichtlich der Ausübung damit verbundener Rechte, insbesondere durch Vertragsklauseln, gewährleistet;

b) die betroffene Person im Einzelfall zugestimmt hat;

c) die Bearbeitung in unmittelbarem Zusammenhang mit dem Abschluss oder der Erfüllung eines Vertrags steht und es sich um Personendaten des Vertragspartners handelt;

d) die Bekanntgabe im Einzelfall entweder für die Wahrung eines überwiegenden öffentlichen Interesses oder für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht unerlässlich ist;

e) die Bekanntgabe im Einzelfall erforderlich ist, um das Leben oder die körperliche Integrität der betroffenen Person zu schützen;

f) die betroffene Person die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat;

g) die Bekanntgabe innerhalb derselben juristischen Person oder Gesellschaft oder zwischen juristischen Personen oder Gesellschaften, die einer einheitlichen Leitung unterstehen, stattfindet, sofern die Beteiligten einheitlichen Datenschutzregeln unterstehen, welche einen angemessenen Schutz gewährleisten.

3) Die Angemessenheit des Schutzes durch Garantien nach Abs. 2 Bst. a oder einheitlichen Datenschutzregelungen nach Abs. 2 Bst. g ist vor der Bekanntgabe der Daten dem Datenschutzbeauftragten zur Begutachtung (Art. 32 Abs. 1 Bst. c) vorzulegen und von der Regierung auf dessen Empfehlung hin zu bewilligen. Die Regierung regelt die Einzelheiten dieser Bewilligungspflicht mit Verordnung.

Art. 14a (neu)

Zertifizierungsverfahren

1) Um den Datenschutz und die Datensicherheit zu verbessern, können die Hersteller von Datenbearbeitungssystemen oder -programmen sowie private Personen oder Behörden, die Personendaten bearbeiten, ihre Systeme, Verfahren und ihre Organisation einer Bewertung durch anerkannte unabhängige Zertifizierungsstellen unterziehen.

2) Die Regierung erlässt Vorschriften über die Akkreditierung von Zertifizierungsverfahren und die Einführung eines Datenschutz-Qualitätszeichens. Sie berücksichtigt dabei das internationale Recht und die international anerkannten technischen Normen.

Art. 15 Abs. 3a (neu)

3a) Sammlungen privater Personen, welche nicht unter Abs. 3 fallen, unterliegen der Anmeldung, sofern sie nicht unter eine Ausnahme nach Abs. 6 fallen.

Art. 17 Abs. 2 Bst. f

f) Daten bearbeitet, welche allgemein zugänglich sind;

Art. 19a (neu)

Anonymisieren und Vernichten von Personendaten

1) Private haben Personendaten zu anonymisieren oder zu vernichten, wenn diese für die Erreichung der Zwecke, für die sie ermittelt wurden, nicht mehr benötigt werden.

2) Soweit gesetzliche Bestimmungen, Vertrags- oder Standespflichten, schutzwürdige Interessen des Betroffenen oder ein unverhältnismässig hoher Aufwand einer Anonymisierung oder Vernichtung entgegenstehen, tritt an deren Stelle eine Sperre.

Art. 21 Abs. 2 Bst. b und c

b) die Regierung es im Einzelfall bewilligt, weil die Rechte der betroffenen Person nicht gefährdet sind; oder

c) die betroffene Person im Einzelfall eingewilligt oder ihre Daten allgemein zugänglich gemacht und eine Bearbeitung nicht untersagt hat.

Art. 23 Abs. 1 Bst. c

c) die betreffenden Daten allgemein zugänglich sind; oder

Art. 25 (neu)

Anonymisieren und Vernichten von Personendaten

1) Die Behörden bieten nach dem Archivgesetz alle Personendaten, die sie nicht mehr ständig benötigen, dem Landesarchiv zur Übernahme an, soweit sie nicht selbst für deren Archivierung zuständig sind.

2) Die Behörden vernichten die Personendaten, die vom Landesarchiv als nicht archivwürdig bezeichnet wurden, ausser wenn sie:

a) anonymisiert sind;

b) zu Beweis- oder Sicherungszwecken erhalten bleiben müssen.

Art. 29 Abs. 5

5) Wird eine Empfehlung nicht befolgt oder abgelehnt, so kann er die Angelegenheit der Datenschutzkommission zum Entscheid vorlegen. Der Entscheid wird der betroffenen Person mitgeteilt. Der Datenschutzbeauftragte ist berechtigt, gegen den Entscheid der Datenschutzkommission Beschwerde zu führen.

Art. 30 Abs. 1 Bst. a und Abs. 4

a) Bearbeitungsmethoden geeignet sind, die Persönlichkeit einer oder mehrerer Personen zu verletzen;

4) Wird eine solche Empfehlung des Datenschutzbeauftragten nicht befolgt oder abgelehnt, so kann er die Angelegenheit der Datenschutzkommission zum Entscheid vorlegen. Er ist berechtigt, gegen den Entscheid der Datenschutzkommission Beschwerde zu führen.

Art. 32 Abs. 1 Bst. g und h (neu)

g) Er prüft die ihm nach Art. 8 Abs. 3 gemeldeten Garantien und Datenschutzregeln.

h) Er prüft die Zertifizierungsverfahren nach Art. 14a und kann dazu Erklärungen nach Art. 29 Abs. 4 oder Art. 30 Abs. 3 abgeben.

Art. 40

1) Private Personen, die ihre Pflichten nach den Art. 5 und Art. 11 bis 13 verletzen, indem sie vorsätzlich eine falsche oder eine unvollständige Auskunft erteilen, werden auf Verlangen des Verletzten vom Landgericht wegen Übertretung mit Busse bis zu 20 000 Franken, im Nichteinbringlichkeitsfalle bis zu drei Monaten Freiheitsstrafe, bestraft.

2) Ebenso ist zu bestrafen, wer als private Person vorsätzlich:

a) Datensammlungen nach Art. 15 nicht meldet oder bei der Meldung falsche Angaben macht;

b) dem Datenschutzbeauftragten bei der Abklärung eines Sachverhaltes (Art. 30) falsche Auskünfte erteilt oder die Mitwirkung verweigert;

c) Datenbekanntgaben ohne Bewilligung nach Art. 8 Abs. 3 ins Ausland tätigt.

II.

Inkrafttreten

Dieses Gesetz tritt unter Vorbehalt des ungenutzten Ablaufs der Referendumsfrist am … in Kraft, andernfalls am Tage der Kundmachung.