Bericht und Antrag des Regierungsrates des Kantons Schaffhausen an den Kantonsrat betreffend Teilrevision des Gesetzes über den Schutz von Personendaten (Kantonales Datenschutzgesetz); [Anpassungen im Zusammenhang mit den Abkommen von Schengen/Dublin und dem Übereinkommen des Europarates zum Schutze des Menschen bei der automatischen Verarbeitung von personenbezogenen Daten]

Sehr geehrter Herr Präsident
Sehr geehrte Damen und Herren

Wir unterbreiten Ihnen den Entwurf für eine Teilrevision des Gesetzes über den Schutz von Personendaten (Kantonales Datenschutzgesetz) vom 7. März 1994. Die Anpassungen sind notwendig im Zusammenhang mit der Umsetzung der bilateralen Abkommen von Schengen/Dublin sowie durch den Beitritt der Schweiz zum Übereinkommen des Europarates vom 28. Januar 1981 zum Schutze des Menschen bei der automatischen Verarbeitung von personenbezogenen Daten (inklusive Zusatzprotokolle).

Unserem Antrag schicken wir folgende Ausführungen voraus.

I. Ausgangslage

Das geltende kantonale Datenschutzgesetz stammt aus dem Jahre 1994. In den letzten 12 Jahren hat im Bereich der elektronischen Datenverarbeitung eine rasante Weiterentwicklung stattgefunden, so dass das heutige kantonale Datenschutzgesetz nicht mehr dem neuesten Stand entspricht und das Gesetz teilweise revisionsbedürftig ist. In der Zwischenzeit hat die Schweiz am 2. Oktober 1997 das Übereinkommen des Europarates vom 28. Januar 1981 zum Schutze des Menschen bei der automatischen Verarbeitung von personenbezogenen Daten inklusive Zusatzprotokolle (in der Folge ER-Konvention) ratifiziert. Dieses ist am 1. Februar 1998 in Kraft getreten. Durch diesen Staatsvertrag verpflichten sich die Schweiz und mithin auch die Kantone, den europäischen

Mindeststandard des Datenschutzes auch im innerstaatlichen Recht zu gewährleisten. Das kantonale Datenschutzgesetz erfüllt diesen Standard in einigen Punkten nicht, wurde bisher aber noch nicht angepasst. Der erwähnte Anpassungsbedarf wird zudem durch die Umsetzung der Abkommen von Schengen/Dublin aktuell, weil vor dem Inkrafttreten der Verträge von Schengen/Dublin ein EU-Ausschuss unter anderem prüfen wird, ob die Schweiz und die Kantone das Europäische Datenschutzniveau erreichen.

Das europäische Datenschutzniveau ist einerseits in der bereits erwähnten ER-Konvention (inkl. Zusatzprotokollen) sowie in der EU-Datenschutzrichtlinie aus dem Jahr 1995 (RL 95/46/EG; in der Folge EU-Datenschutzrichtlinie) festgelegt. Beim Anschluss an das Schengener Informationssystem (SIS) setzt die EU voraus, dass die angeschlossenen Staaten das EU-Datenschutzniveau erfüllen, und die Daten werden nur zur Verfügung gestellt, wenn der gleiche Schutz für Private gewährleistet ist.

Durch den Abschluss der bilateralen Verträge ist die Schweiz näher in Europa eingebunden. Sie kann in vielen Bereichen wie ein Mitgliedstaat profitieren und erhält dadurch Zugang zum EU-Binnenmarkt. Dieser bezweckt, den freien Markt von Waren, Personen, Dienstleistungen und Kapital innerhalb der EU zu gewährleisten. Mit dem Abschluss der Abkommen von Schengen und Dublin wird auch die Zusammenarbeit in der Sicherheits- und Asylpolitik verstärkt. Der freie Binnenmarkt setzt auch einen möglichst freien Datentransfer voraus. Um mit gleichen Spielregeln zu arbeiten und zum Schutz der Rechte und Freiheiten der Personen haben die Mitgliedstaaten der EU sowie der Europarat sich darauf geeinigt, dass alle Mitgliedstaaten im Datenschutz die gleichen Mindest-Regeln vorsehen, um ein einheitliches Schutzniveau gewährleisten zu können. Die massgebende Bestimmung in diesem Bereich ist die erwähnte EU-Datenschutzrichtlinie. Diese entspricht im Wesentlichen der ER-Konvention, zu der sich die Schweiz verpflichtet hat.

Der Bund und die Kantone sind aufgrund der ER-Konvention verpflichtet, ihre Datenschutzgesetze dem europäischen Datenschutzniveau anzugleichen, sofern diese das Schutzniveau noch nicht erreichen. Um die Umsetzung im Bereich des Datenschutzes der Kantone im Hinblick auf die Inkraftsetzung des Abkommens von Schengen und Dublin zu koordinieren, hat die Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) einen Datenschutz-Experten damit beauftragt, eine Wegleitung mit einer Checkliste zu erstellen. Anhand dieser Wegleitung kann von den Kantonen geprüft werden, in welchen Berei-

chen ein Handlungsbedarf besteht. Die beantragte Teilrevision des Datenschutzgesetzes richtet sich nach der erwähnten Wegleitung und nimmt dort Änderungen vor, wo diese aufgrund des übergeordneten nationalen und internationalen Rechts notwendig sind.

Für diejenigen Kantone, die – wie der Kanton Schaffhausen – schon über ein Datenschutzgesetz verfügen, hält sich der Anpassungsbedarf in überblickbaren Grenzen. Der Anpassungsbedarf im Kanton Schaffhausen betrifft im Wesentlichen folgende Bereiche:

- Verbesserung der Unabhängigkeit des Datenschutzbeauftragten
- Präzisierung der datenschutzrechtlichen Grundsätze auf Gesetzesstufe
- Präzisierung der Informationspflichten beim Beschaffen von besonders schützenswerten Daten und Persönlichkeitsprofilen
- Ausbau des Schutzes des rechtlichen Gehörs bei der automatisierten Datenverarbeitung
- Regelung der Bekanntgabe von Daten an andere Staaten
- Präzisierung der Datenbearbeitung für nicht personenbezogene Zwecke
- Vorabkontrolle beim Einsatz von neuen automatisierten Verfahren in der Verwaltung
- Verbesserung des Auskunftsrechtes von betroffenen Personen
- Ausbau der Kontrollinstrumente des Datenschutzbeauftragten

Zudem sind einige Elemente des Datenschutzrechts bisher nur auf Verordnungsstufe vorgesehen, welche aufgrund ihrer Bedeutung nach der neuen Kantonsverfassung (vgl. Art. 50 KV) auf Gesetzesstufe zu regeln sind. Gleichzeitig soll das Gesetz punktuell übersichtlicher gestaltet werden. Der Übersicht halber werden jeweils vor der Erläuterung zu den einzelnen Bestimmungen immer die zugrunde liegenden Rechtsgrundlagen des revidierten Datenschutzgesetzes des Bundes (in der Folge Bundes-DSG), der ER-Konvention und der EU-Datenschutzrichtline erwähnt.

Die Vorlage wurde in enger Zusammenarbeit mit dem kantonalen Datenschutzbeauftragten erarbeitet.

II. Bemerkungen zu den einzelnen Bestimmungen

Zum Titel des 1. Abschnittes: «Zweck, Begriffe und Geltungsbereich»

Im 1. Abschnitt werden in den Artikeln 1 bis 3 der Zweck, die datenschutzrechtlichen Begriffe sowie der Geltungsbereich definiert. Zur Verbesserung der Gesetzessystematik und der Übersicht soll der bisherige Titel «Allgemeine Bestimmungen» neu «Zweck, Begriffe und Geltungsbereich» heissen.

Zum Titel des 2. Abschnittes: «Allgemeine Datenschutzbestimmungen»

Der 2. Abschnitt enthält in Art. 4 bis Art. 14 die allgemeinen Datenschutzbestimmungen. Der bisherige Titel «Bearbeiten von Personendaten» ist zu eng gefasst.

Zu Art. 4 Grundsätze

Zum Randtitel: In Art. 4 werden die Grundsätze des Bearbeitens von Personendaten geregelt. Der bisherige Randtitel «Zulässigkeit» nimmt nur Bezug auf den Grundsatz der gesetzlichen Grundlage als Erfordernis für die Datenbearbeitung. Dieser ist in Abs. 1 statuiert. Der Randtitel wird dementsprechend auf «Grundsätze» geändert.

Zu Art. 4 Abs. 2 Treu und Glauben und Verhältnismässigkeit

Grundlagen: Art. 4 Abs. 2 und Abs. 4 Bundes-DSG, Art. 5 lit. a ER-Konvention sowie Art. 6 Abs. 1 lit. a EU-Datenschutzrichtlinie

Bei der Bearbeitung von Personendaten durch staatliche Organe gelten die Grundsätze von Treu und Glauben und der Verhältnismässigkeit. Diese werden neu explizit in Abs. 2 aufgeführt. Das Bearbeiten von Personendaten muss nach Treu und Glauben erfolgen. Ausfluss dieses Grundsatzes ist insbesondere das Verbot der verdeckten Datenerhebung. Dies bedeutet, dass Personendaten wenn immer möglich bei der betroffenen Person zu erheben sind und dass die Erhebung (Beschaffung) und der Zweck der Bearbeitung für die betroffene Person erkennbar sein müssen.

Zu Art. 4 Abs. 3 Konkretisierung der Verhältnismässigkeit der Datenbearbeitung

Grundlagen: Art. 4 Abs. 3 Bundes-DSG, Art. 5 lit. c und e ER-Konvention sowie Art. 6 Abs. 1 lit. c und e EU-Datenschutzrichtlinie

Das Bearbeiten von Personendaten muss – wie jedes behördliche Handeln – verhältnismässig sein. Das bedeutet, dass die bearbeiteten Daten zur Zweckerreichung geeignet sein müssen; die Datenbearbeitung muss das mildeste Mittel sein, mit welchem der Zweck erreicht werden kann. Zudem müssen der Zweck und der Eingriff in die informationelle Selbstbestimmung in einem vernünftigen Verhältnis zueinander stehen. Von Bedeutung ist auch die zeitliche Begrenzung der Aufbewahrung von Personendaten: Wenn sie zur Aufgabenerfüllung nicht mehr erforderlich sind, sind sie – vorbehältlich gesetzlicher Archivierungsregelungen – zu vernichten oder zu anonymisieren, so dass kein Rückschluss mehr auf die betroffene Person möglich ist. Aus diesem Grund ist in Abs. 3 festzuhalten, dass die bearbeiteten Daten zur Erreichung des Zwecks, zu dem sie bearbeitet werden, geeignet und erforderlich sein müssen und nicht länger bearbeitet werden dürfen, als es zur Zweckerreichung erforderlich ist.

Zu Art. 5 Besonders schützenswerte Daten

Grundlagen: Art. 17 Bundes-DSG, Art. 6 ER-Konvention sowie Art. 8 EU-Datenschutzrichtlinie

Die Bearbeitung von Personendaten, die besonders persönlichkeitsnah sind und ein grosses Stigmatisierungs- und Diskriminierungspotenzial besitzen, verlangt nach einem qualifizierten Schutz. Dabei handelt es sich um besonders schützenswerte Personendaten wie Persönlichkeitsprofile und Daten über religiöse oder politische Ansichten, die Gesundheit, Sozialhilfemassnahmen sowie strafrechtliche Verfolgungen. Für die Bearbeitung wird eine formell-gesetzliche Grundlage verlangt oder es werden an die Erforderlichkeit zur Erfüllung einer Aufgabe höhere Anforderungen gestellt. Wenn – im Einzelfall – die Einwilligung der betroffenen Person als Rechtfertigungsgrund dienen soll, muss die Zustimmung in Kenntnis der Sachlage, freiwillig und ohne (offene oder versteckte) Androhung von Nachteilen im Verweigerungsfall erfolgt sein. Der heutige Art. 5 ist in lit. b demzufolge mit dem Wort «unzweifelhaft» zu ergänzen. Damit wird klargestellt, dass besonders schützenswerte Personendaten sowie Persönlichkeitsprofile nur bearbeitet werden dür-

fen, wenn die betroffene Person ausdrücklich zugestimmt hat oder ihre Zustimmung nach den Umständen unzweifelhaft vorausgesetzt werden darf.

Zu Art. 5a Informationspflicht bei Datenbeschaffung bei Dritten (neu)

Grundlagen: Art. 4 Abs. 4 Bundes-DSG, Art. 8 lit. a ER-Konvention sowie Art. 10, 11 und 21 EU-Datenschutzrichtlinie

Wenn besonders schützenswerte Daten oder Persönlichkeitsprofile erhoben werden, soll die betroffene Person darüber informiert werden. Dieser Informationsanspruch bildet die Grundlage, dass die betroffene Person Kenntnis von der Datenbeschaffung erhält und ihre Rechte auch wahrnehmen kann. Diese Informationspflicht gilt im Besonderen für Daten, die bei Dritten beschafft werden. Den betroffenen Personen sind mindestens der Inhaber der Datensammlung, der Zweck des Bearbeitens sowie die Kategorien der Datenempfänger mitzuteilen. Wenn Daten nicht bei der betroffenen Person beschafft werden, hat deren Information spätestens bei Beginn der Speicherung der Daten oder, wenn auf die Speicherung verzichtet wird, mit der ersten Bekanntgabe an Dritte zu erfolgen. Die Informationspflicht des Inhabers der Datensammlung entfällt oder kann sistiert werden, wenn die betroffene Person bereits informiert wurde oder wenn die Speicherung oder die Bekanntgabe der Daten ausdrücklich durch das Gesetz vorgesehen ist oder die Information nicht oder nur mit unverhältnismässigem Aufwand möglich ist. Zudem kann die Informationspflicht sistiert werden, solange ihr überwiegende öffentliche Interessen entgegenstehen.

Als überwiegendes öffentliches Interesse gilt beispielsweise, wenn die Benachrichtigung die Sicherheit des Bundes oder des Kantons gefährden würde; die Daten oder die Tatsache ihrer Speicherung zum Schutze des Betroffenen oder zum Schutze der Rechte Dritter geheim gehalten werden müssen und deshalb das Interesse des Betroffenen zurücktreten muss (z.B. Ort der Unterbringung von bedrohtem Ehepartner).

Zu Art. 11a und 11b Datenbekanntgabe an EU-Staaten und an Drittstaaten (neu)

Grundlagen: Art. 6 Bundes-DSG, Art. 12 ER-Konvention und Art. 2 ZP zur ER-Konvention sowie Art. 25 f. EU-Datenschutzrichtlinie

Gemäss Art. 12 ER-Konvention und Art. 2 ZP zur ER-Konvention ist für den Fall des grenzüberschreitenden Datenverkehrs im Gesetz festzuhalten, dass die grenzüberschreitende Übermittlung von Personendaten an Empfänger, für welche die ER-Konvention nicht gilt, – zusätzlich zu den allgemeinen Bekanntgabevoraussetzungen – nur dann zulässig ist, wenn beim Empfänger ein adäquates Datenschutzniveau sichergestellt ist. Damit soll verhindert werden, dass Daten an Staaten weitergegeben werden, die die Grund- und Menschenrechte nicht einhalten oder die über keinen dem europäischen Niveau gleichwertigen Datenschutz verfügen. Denn Daten, deren Bearbeitung im Inland und in den Nachbarstaaten problemlos ist, können für die betroffene Person «problematisch» werden, wenn sie ohne spezielle Vorkehrungen ins Ausland transferiert werden. Diesen Grundsatz gilt es, in das kantonale Recht aufzunehmen und zu konkretisieren. Da die EU-Staaten die Europäische Datenschutzrichtlinie im innerstaatlichen Recht umgesetzt haben und damit über ein ausreichendes Datenschutzniveau verfügen, erübrigt sich die Prüfung des Datenschutzniveaus im Einzelfall. Zu prüfen sind lediglich die allgemeinen Bekanntgabevoraussetzungen von Art. 8 ff. Datenschutzgesetz.

An Drittstaaten dürfen Personendaten dagegen nur bekannt gegeben werden, sofern diese ein angemessenes Datenschutzniveau gewährleisten. Die Angemessenheit des Datenschutzniveaus wird unter Berücksichtigung aller Umstände beurteilt, die für die Datenübermittlung von Bedeutung sind. Gewährleistet ein Drittstaat kein angemessenes Datenschutzniveau, so können ihm Personendaten im Einzelfall bekannt gegeben werden, wenn die betroffene Person ohne jeden Zweifel eingewilligt hat. Handelt es sich um besonders schützenswerte Personendaten oder Persönlichkeitsprofile, so muss die Einwilligung ausdrücklich sein (a) oder muss die Bekanntgabe erforderlich sein, um das Leben oder die körperliche Integrität der betroffenen Person zu schützen (b) oder muss die Bekanntgabe zur Wahrung überwiegender öffentlicher Interessen oder zur Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht erforderlich sein (c). Daten dürfen nicht übermittelt werden, soweit Grund zur Annahme besteht, dass sie gegen die schweizerische Rechtsordnung, insbesondere gegen die Grundfreiheiten und Menschenrechte der Bundesverfassung verstossen würden. Personendaten können zudem bekannt gegeben werden, wenn im Einzelfall hinreichende vertragliche Garantien einen angemessenen Schutz der betroffenen Person gewährleisten.

Zu Art. 12 Bearbeitung für nicht personenbezogene Zwecke

Grundlagen: Art. 22 Bundes-DSG, Art. 9 Ziff. 3 ER-Konvention sowie Art. 6 Abs. 1 lit. b und e und Art. 11 Abs. 2 EU-Datenschutzrichtlinie

Gemäss Art. 9 Ziff. 3 ER-Konvention haben die Vertragsstaaten geeignete Garantien vorzusehen, wenn Daten zu nicht personenbezogenen Zwecken bearbeitet werden. Damit ist die Auswertung von Daten für die Zwecke der Statistik oder der historischen oder wissenschaftlichen Forschung gemeint. Hier steht nicht die betroffene Person als solche im Fokus, sondern Statistik, Planung oder Forschung. Gleichwohl muss sichergestellt werden, dass die bearbeiteten Daten nicht in falsche Hände kommen oder dass Persönlichkeitsrechte verletzt werden. In diesen Fällen finden die Bestimmungen über die Bekanntgabe von Daten sowie die Informationspflichten keine Anwendung. Es ist zulässig, solche Bearbeitungen zu privilegieren. Für die Bekanntgabe von Personendaten an Empfänger ausserhalb der Verwaltung sind zusätzliche Auflagen vorzusehen (Garantien, Weitergabeverbot, Verstärkung mit Konventionalstrafe). Der bisherige Art. 12 DSG ist in diesem Sinne zu ergänzen und mit zusätzlichen Sicherheiten auszustatten. In der Praxis wurden bei der Bekanntgabe von Daten für Forschungszwecke bisher schon oft – auf freiwilliger Basis – das Einverständnis des Datenschutzbeauftragten eingeholt und unter dessen Mitwirkung mit den Privaten (vor allem Universitäten) Vereinbarungen abgeschlossen. Mit vorliegender Regelung wird somit lediglich die bisherige Praxis gesetzlich festgeschrieben. Abs. 3 wird neu zu Abs. 4.

Zu Art. 16a Vorabkontrolle (neu)

Grundlagen: Art. 31 Abs. 1 lit. b Bundes-DSG; Art. 20 EU-Datenschutzrichtlinie

Neue Datenverarbeitungen, welche besondere Risiken für die Rechte und Freiheiten von Personen beinhalten können, sind vor dem Einsatz durch den Datenschutzbeauftragten prüfen und genehmigen zu lassen. Kriterien für die Beurteilung der Risiken sind etwa die Zahl der erfassten Personen, die Zahl der beteiligten öffentlichen Organe oder die Sensitivität der Daten. Objekte der Vorabkontrolle sind vor allem IT-Projekte für Datenbanken. Bisher enthielt § 12 Abs. 4 der Datenschutzverordnung nur eine vage Regelung.

Zu Art. 18 Auskunftsrecht; Grundsatz der Transparenz und Informationsanspruch

Das internationale Recht schreibt zum Schutz von Personen gewisse Minimalstandards beim Auskunftsrecht in Datensammlungen vor. Danach müssen Datensammlungen für Private transparent sein (sog. Grundsatz der Transparenz) und zur Wahrnehmung der Rechte muss in einem bestimmten Umfang ein Informationsrecht gewährleistet werden. Das Auskunftsrecht darf auch nicht durch (hohe) Gebühren verhindert werden.

Zu Art. 18 Abs. 1 Transparenzgebot

Grundlagen: Art. 4 Abs. 4 Bundes-DSG, Art. 8 lit. a ER-Konvention sowie Art. 10, 11 und 21 EU-Datenschutzrichtlinie

Das Auskunftsrecht besteht aus dem Transparenzgebot und dem Informationsanspruch. Transparenz bezüglich der Bearbeitung von Personendaten ist eines der Kernanliegen des Datenschutzrechts. Das Transparenzgebot besteht aus dem allgemeinen Recht zu wissen, welche Datenbearbeitungen erfolgen oder welche Datensammlungen bestehen. Dazu gehören auch die wichtigsten Angaben über deren Hauptzwecke und das verantwortliche Organ. Das Transparenzgebot ist aufgrund seiner Bedeutung auf Gesetzesstufe festzuhalten. Bisher ist dieses nur auf Verordnungsstufe umschrieben (§ 10 Abs. 2 Datenschutzverordnung). Jede Person hat somit das Recht, Auskunft über das Vorhandensein einer Datensammlung, ihre Hauptzwecke sowie das verantwortliche öffentliche Organ zu erhalten. Der bisherige Informationsanspruch in Abs. 1 wird neu zu Abs. 2.

Zu Art. 18 Abs. 2 Informationsanspruch

Grundlagen: Art. 8 Bundes-DSG, Art. 8 lit. b ER-Konvention und Art. 12 lit. a EU-Datenschutzrichtlinie

Der Informationsanspruch ist ein weiterer Kernpunkt des Datenschutzrechts. Der bisherige Informationsanspruch von Art. 18 Abs. 1 DSG ist neu in Abs. 2 zu präzisieren, da die Grundzüge des Anspruches bisher nur in § 10 der Datenschutzverordnung und somit nicht auf Gesetzesstufe geregelt sind. Jede Person erhält Auskunft, ob und wenn ja, welche Daten über sie von einem öffentlichen Organ in einer bestimm-

ten Datensammlung bearbeitet werden, und zwar unabhängig davon, ob das öffentliche Organ die Daten selber bearbeitet oder bearbeiten lässt. Jede Person erhält auf Verlangen auch Einsicht in ihre Daten. Der Informationsanspruch ist der Ausgangspunkt für die weiteren Rechte und Ansprüche der betroffenen Person. Die Schranken des Einsichtsrechtes ergeben sich aus dem bisherigen Art. 19 DSG.

Zu Art. 18 Abs. 3 Grundsatz der Gebührenfreiheit für Auskunft

Grundlagen: Art. 8 Abs. 5 Bundes-DSG, Art. 8 lit. b ER-Konvention und Art. 12 lit. a EU-Datenschutzrichtlinie

Das Recht auf Auskunft (und Einsicht) ist einer der wichtigsten Ausflüsse des verfassungsrechtlichen Persönlichkeitsschutzes. Es darf nicht durch eine übermässige Kostenbeteiligung der betroffenen Person erschwert oder gar vereitelt werden. Es ist deshalb im Gesetz festzuhalten, dass die Auskunft grundsätzlich kostenlos, mindestens aber ohne «übermässige Kosten» (also nicht bei normalem Aufwand wie für das Hervorsuchen eines Dossiers, einfaches Kopieren usw.) zu erteilen ist. Da es jedoch erfahrungsgemäss Personen gibt, die die Verwaltung notorisch übermässig mit solchen Auskunftsbegehren beschäftigen, muss es möglich sein, dass sich diese angemessen an den von ihnen dem Staat und der Allgemeinheit verursachten Kosten zu beteiligen haben. Aufgrund der Bedeutung dieses Grundsatzes für das Auskunftsrecht soll die Regelung neu auf Gesetzesstufe erfolgen (bisher § 14 Datenschutzverordnung).

Zu Art. 23 Datenschutzbeauftragter a) Kanton

Grundlagen: Art. 26 f. Bundes-DSG, Präambel Abs. 2 und Art. 1 ZP zur ER-Konvention und Art. 28 EU-Datenschutzrichtline

Gemäss Art. 1 ZP zur ER-Konvention sowie Art. 28 Abs. 1 und 2 EU-Datenschutzrichtlinie ist die behördliche Datenbearbeitung durch ein unabhängiges Kontrollorgan zu kontrollieren. Die Unabhängigkeit des Kontrollorgans ist mit gesetzlichen und institutionellen Garantien (Wahlorgan, Anstellungsverhältnis, Amtsdauer, eigenes Budget usw.) sicherzustellen. Zudem ist es mit genügenden personellen und finanziellen Ressourcen auszustatten, so dass es die Aufgaben auch wahrnehmen kann.

Wegen der Bedeutung der Unabhängigkeit ist diese neu im Gesetz festzuschreiben (bisher § 11 Abs. 1 Datenschutzverordnung). Zur Sicherstellung der Unabhängigkeit des Datenschutzbeauftragten ist dieser neu für eine Amtsdauer von vier Jahren zu wählen. Wie bisher soll er über ein eigenes Budget verfügen, was indessen ausdrücklich festzuhalten ist. Eine Abwahl kann – während der Amtsdauer – nur aus wichtigen sachlichen Gründen erfolgen. Um eine wirksame Kontrolle ausüben zu können, ist bei der Auswahl auf die fachliche Qualifikation zu achten.

Zu Art. 25 Aufgaben des Datenschutzbeauftragten

Grundlagen: Art. 26 f. Bundes-DSG, Präambel Abs. 2 und Art. 1 ZP zur ER-Konvention und Art. 28 EU-Datenschutzrichtlinie

Zu den wirksamen Einwirkungsbefugnissen gehört auch die Befugnis zur Vorabkontrolle von Erlassen sowie das Recht zur Veröffentlichung von Stellungnahmen. Die bisherige Bestimmung ist dahingehend zu ergänzen, dass der Datenschutzbeauftragte beim Erlass von Gesetzen, die für den Datenschutz erheblich sind, einzubeziehen ist und er nach eigenem Ermessen berechtigt ist, diese Stellungnahmen zu veröffentlichen. Das wurde in der Praxis bisher meistens schon so gehandhabt. Bisher war in § 12 Abs. 4 Datenschutzverordnung lediglich vorgesehen, dass die Aufsichtsstelle zu Erlassen Stellung nehmen kann, nicht jedoch, dass sie automatisch von der Verwaltung einzubeziehen ist.

Der Datenschutzbeauftragte ist zudem berechtigt und verpflichtet, zur Erfüllung seiner Kontrollaufgaben mit den Kontrollorganen (Datenschutzbeauftragten) der anderen Kantone, des Bundes und des Auslandes zusammenzuarbeiten.

Zu Art. 26, Art. 26a und 26b Befugnisse des Datenschutzbeauftragten

Grundlagen: Art. 26 f. Bundes-DSG, Präambel Abs. 2 und Art. 1 ZP zur ER-Konvention und Art. 28 EU-Datenschutzrichtlinie

Das europäische Recht setzt zum Schutz von Personen eine proaktive und unabhängige Datenschutzkontrolle mit wirkungsvollen Untersuchungs- und Eingriffsbefugnissen voraus. Die derzeitigen im kantonalen Datenschutzgesetz vorgesehenen Kontrollbefugnisse sind durch die

Verbesserung der Schutzmöglichkeiten an das EU-Datenschutzniveau anzugleichen.

Der Datenschutzbeauftragte muss gemäss Art. 1 Ziff. 2 lit. a ZP zur ER-Konvention über umfassende Untersuchungsbefugnisse und wirksame Einwirkungsbefugnisse verfügen. Dabei ist wesentlich, dass die Aufsichtsstelle mit den gesetzlich festgelegten Einwirkungs- und Untersuchungsbefugnissen in ihrer Gesamtheit tatsächlich Wirksamkeit entfalten kann. Vor diesem Hintergrund ist Art. 26 zu ergänzen und zu präzisieren.

Zu den wirksamen Einwirkungsbefugnissen gehören die Anordnung eines vorläufigen Datenverarbeitungsverbotes, die Empfehlung an die betroffene Amtsstelle sowie die Anordnung der Sperrung, der Löschung oder der Vernichtung von Daten. Wird die Empfehlung abgelehnt, so kann der Datenschutzbeauftragte seine Empfehlung in der Form einer anfechtbaren Verfügung anordnen. Als weiteres Eingriffsinstrument steht ihm die Möglichkeit der Berichterstattung über datenschutzrelevante Mängel an den Regierungsrat oder an den Kantonsrat zur Verfügung.

Erfahrungsgemäss wird es in der Regel genügen, wenn die Aufsichtsstelle der betroffenen Amtsstelle eine Empfehlung abgibt (vgl. Art. 26 Abs. 2). Diese Einwirkungsbefugnis war bisher lediglich in der kantonalen Datenschutzverordnung festgehalten. Sie soll wegen ihrer Bedeutung neu auf Gesetzesstufe geregelt werden. Neu soll die anzeigende Person im Sinne der Transparenz über das Ergebnis der Untersuchung und über den Inhalt der Empfehlung informiert werden. Das «Empfehlungsverfahren» wird wirksamer ausgestaltet. Danach erlässt der Datenschutzbeauftragte seine Empfehlung an die betroffene Amtsstelle zunächst wie bisher ohne besondere Formerfordernis. Die Empfehlungs-Adressaten sind verpflichtet, sich innert 30 Tagen dazu zu äussern. Sie können die Empfehlung ganz oder teilweise ablehnen bzw. ganz oder teilweise annehmen. Wenn eine Empfehlung ganz oder teilweise abgelehnt wird, hat der Datenschutzbeauftragte die Möglichkeit, die Empfehlung als Ganzes oder diejenigen Teile daraus, bei denen er das Durchsetzungsinteresse hoch gewichtet, als Verfügung zu erlassen. Er könnte also beispielsweise verfügen, eine Datenverarbeitung auf eine bestimmte Weise zu ändern oder den Zugang zu Daten zu beschränken. In letzter Konsequenz kann der Datenschutzbeauftragte auch die Sperrung, Löschung oder Vernichtung von Daten anordnen. So wäre die Vernichtung anzuordnen, wenn Daten widerrechtlich erhoben würden. Die Erweiterung der Einwirkungsbefugnisse bedingt, dass sie auf ihre Rechtmässigkeit überprüft werden können. Die betroffene Amtsstelle

kann deshalb gegen diese Verfügung beim Regierungsrat Rekurs erheben. Die Überprüfbarkeit einer Verfügung des Datenschutzbeauftragten, mithin also die Anfechtbarkeit auf dem ordentlichen Rechtsmittelweg, wird von Art. 1 Abs. 4 ZP zur ER-Konvention verlangt. Der Datenschutzbeauftragte – nicht aber die betroffene Amtsstelle – hat seinerseits wiederum die Möglichkeit, gegen den regierungsrätlichen Rekursentscheid mit Verwaltungsgerichtsbeschwerde an das Obergericht zu gelangen. Dadurch wird sichergestellt, dass die Empfehlungen des Datenschutzbeauftragten vom Verwaltungsgericht auf ihre Rechtmässigkeit hin überprüft werden können. Der Datenschutzbeauftragte erhält damit ähnlich wie die Staatsanwaltschaft im Strafverfahren die Möglichkeit, einen Entscheid im öffentlichen Interesse dem Verwaltungsgericht zur Überprüfung vorzulegen.

Ergeben sich Hinweise auf eine strafbare Handlung, ist der Datenschutzbeauftragte verpflichtet, diese Feststellung den Strafverfolgungsbehörden zu melden. Im Gegensatz dazu sieht Art. 206 Strafprozessordnung eine Pflicht zur Strafanzeige für Behörden nur vor, wenn ihnen in ihrer amtlichen Stellung eine schwerwiegende Straftat bekannt wird. Bei Verstössen gegen das Datenschutzgesetz ist diese Voraussetzung regelmässig nicht erfüllt. Für Verstösse unterhalb der strafrechtlichen Schwelle ist der Datenschutzbeauftragte berechtigt und verpflichtet, gemäss Art. 30 f. Verwaltungsrechtspflegegesetz eine Aufsichtsbeschwerde zu erheben. Diese Befugnisse gehören ebenfalls zu den wirkungsvollen Eingriffsinstrumenten des Datenschutzbeauftragten.

III. Personelle und finanzielle Auswirkungen

Durch die neuen Aufgaben resultiert voraussichtlich ein gewisser Mehraufwand für den Datenschutzbeauftragten von schätzungsweise 10 bis 20 Prozent, was Mehrkosten von rund Fr. 6'000.-- pro Jahr zur Folge haben wird.

Sehr geehrter Herr Präsident
Sehr geehrte Damen und Herren

Gestützt auf die vorstehenden Ausführungen beantragen wir Ihnen, auf die Vorlage einzutreten und dem im Anhang beigefügten Entwurf für eine Teilrevision des Gesetzes über den Schutz von Personendaten (Kantonales Datenschutzgesetz) zuzustimmen.

Schaffhausen, 24. Oktober 2006

Im Namen des Regierungsrates

Der Präsident:

Dr. Hans-Peter Lenherr

Der Staatsschreiber:

Dr. Reto Dubach

Gesetz
über den Schutz von Personendaten (Kantonales Datenschutzgesetz)

Anhang

Änderung vom

Der Kantonsrat Schaffhausen

beschliesst als Gesetz:

I.

Das Gesetz über den Schutz von Personendaten (Kantonales Datenschutzgesetz) vom 7. März 1994 wird wie folgt geändert:

Gliederungstitel

I. Zweck, Begriffe und Geltungsbereich

Gliederungstitel

II. Allgemeine Datenschutzbestimmungen

Art. 4 Randtitel, Abs. 2 und Abs. 3

Grundsätze

[2] Das Bearbeiten von Personendaten hat nach Treu und Glauben zu erfolgen und muss verhältnismässig sein.

[3] Die bearbeiteten Daten müssen zur Erreichung des Zwecks, zu dem sie bearbeitet werden, geeignet und erforderlich sein und dürfen nicht länger bearbeitet werden, als es zur Zweckerreichung erforderlich ist.

Art. 5 lit. b

Besonders schützenswerte Personendaten sowie Persönlichkeitsprofile dürfen nur bearbeitet werden, wenn:

b) die betroffene Person ausdrücklich zugestimmt hat oder ihre Zustimmung nach den Umständen unzweifelhaft vorausgesetzt werden darf.

Art. 5a

Informationspflicht beim Beschaffen von besonders schützenswerten Personendaten und Persönlichkeitsprofilen

[1] Der Inhaber der Datensammlung ist verpflichtet, die betroffene Person über die Beschaffung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen zu informieren; diese Informationspflicht gilt auch dann, wenn die Daten bei Dritten beschafft werden.

[2] Der betroffenen Person sind mindestens mitzuteilen:

a) der Inhaber der Datensammlung;

b) der Zweck des Bearbeitens;

c) die Kategorien der Datenempfänger, wenn eine Datenbekanntgabe vorgesehen ist.

[3] Wenn Daten nicht bei der betroffenen Person beschafft werden, hat deren Information spätestens bei Beginn der Speicherung der Daten oder, wenn auf die Speicherung verzichtet wird, mit der ersten Bekanntgabe an Dritte zu erfolgen.

[4] Die Informationspflicht des Inhabers der Datensammlung entfällt, wenn die betroffene Person bereits informiert wurde oder, in Fällen nach Absatz 3, wenn:

a) die Speicherung oder die Bekanntgabe der Daten ausdrücklich durch das Gesetz vorgesehen ist oder

b) die Information nicht oder nur mit unverhältnismässigem Aufwand möglich ist oder

c) überwiegende öffentliche Interessen der Information entgegenstehen, solange diese bestehen.

Art. 11a

e) Bekanntgabe an europäische Staaten

Für die Bekanntgabe personenbezogener Daten an ausländische Stellen der Europäischen Union sowie Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum gelten neben dem übergeordneten Recht und dem Staatsvertragsrecht die Bestimmungen gemäss Art. 8 ff. sinngemäss.

Art. 11b

f) Bekanntgabe von Personendaten an Drittstaaten

[1] An Drittstaaten dürfen Personendaten unter Vorbehalt von Art. 8 ff. nur bekannt gegeben werden, sofern diese ein angemessenes Datenschutzniveau gemäss Art. 2 Ziff. 2 des Zusatzprotokolles des Europarates vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung von personenbezogenen Daten (SEV Nr. 108) gewährleisten.

[2] Die Angemessenheit des Datenschutzniveaus wird unter Berücksichtigung aller Umstände beurteilt, die für die Datenübermittlung von Bedeutung sind.

[3] Gewährleistet ein Drittstaat kein angemessenes Datenschutzniveau, so können ihm Personendaten im Einzelfall bekannt gegeben werden, wenn:

a) die betroffene Person ohne jeden Zweifel eingewilligt hat; handelt es sich um besonders schützenswerte Personendaten oder Persönlichkeitsprofile, so muss die Einwilligung ausdrücklich sein;
b) die Bekanntgabe erforderlich ist, um das Leben oder die körperliche Integrität der betroffenen Person zu schützen; oder
c) die Bekanntgabe zur Wahrung überwiegender öffentlicher Interessen oder zur Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht erforderlich ist.

[4] Die Übermittlung unterbleibt, soweit Grund zur Annahme besteht, dass sie gegen die schweizerische Rechtsordnung verstossen würde oder die Übermittlung der ordre public widerspricht.

[5] Personendaten können bekannt gegeben werden, wenn im Einzelfall hinreichende vertragliche Garantien einen angemessenen Schutz der betroffenen Person gewährleisten.

Art. 12 Abs. 1 lit. c, Abs. 3 und Abs. 4

Bearbeitung für nicht personenbezogene Zwecke

[1] Personendaten dürfen für nicht personenbezogene Zwecke, wie die Statistik, Planung, Wissenschaft oder Forschung, bearbeitet werden, wenn:

c) die Zustimmung des Datenschutzbeauftragten vorliegt.

[3] Bei der Datenbekanntgabe an Dritte ist eine Vereinbarung abzuschliessen. Es kann eine Konventionalstrafe vorgesehen werden für den Fall, dass die Datenschutzbestimmungen nicht eingehalten werden.

[4] In diesen Fällen finden Art. 4 Abs. 4 sowie Art. 5 und 8 keine Anwendung.

Art. 16a

Vorabkontrolle

[1] Ein automatisiertes Verfahren zur Verarbeitung von personenbezogenen Daten, das mit besonderen Risiken für die Rechte und Freiheit der betroffenen Personen verbunden sind, insbesondere auf Grund der Art und Zweckbestimmung, darf erst eingesetzt oder wesentlich geändert werden, wenn sichergestellt ist, dass diese Risiken nicht bestehen oder durch technische oder organisatorische Massnahmen verhindert werden.

[2] Diese Bearbeitung ist vorgängig durch die kantonale Aufsichtsstelle zu kontrollieren und genehmigen zu lassen.

Art. 18

Auskunftsrecht; Grundsatz der Transparenz und Informationsanspruch

[1] Jede Person hat das Recht, Auskunft über das Vorhandensein einer Datensammlung, ihre Hauptzwecke sowie das verantwortliche öffentliche Organ zu erhalten.

[2] Jede Person erhält auf Verlangen in allgemein verständlicher Form Auskunft darüber, ob und wenn ja welche Daten über sie in einer bestimmten Datensammlung bearbeitet werden. Die Auskunft erfolgt in der Regel schriftlich, in Form eines Ausdrucks oder einer Fotokopie. Jede Person erhält auf Verlangen Einsicht in ihre Daten.

[3] Die Auskunft erfolgt in der Regel kostenlos. Sofern mit der Auskunft ein grosser administrativer Aufwand verbunden ist oder in derselben Angelegenheit wiederholt Auskunft verlangt wird, kann eine angemessene Gebühr verlangt werden.

Art. 23

[1] Der Regierungsrat wählt als verwaltungsunabhängige Aufsichtsstelle eine kantonale Datenschutzbeauftragte oder einen kantonalen Datenschutzbeauftragten mit entsprechender fachlicher Qualifikation für eine Amtsdauer von vier Jahren.

[2] Es kann nur aus wichtigen sachlichen Gründen eine Abwahl erfolgen.

[3] Die Aufsichtsstelle erfüllt ihre Aufgaben in völliger Unabhängigkeit; sie verfügt über ein eigenes Budget.

[4] Vorbehältlich der nachfolgenden Bestimmungen wird das Nähere in einer Verordnung festgelegt.

Art. 25 Abs. 1 lit. d, e, f und g

[1] Die Aufsichtsstelle

d) behandelt Eingaben von betroffenen Personen und gibt Empfehlungen gemäss Art. 26 Abs. 2 ab;

e) berät die verantwortlichen Organe in Fragen des Datenschutzes und der Datensicherheit, nimmt Stellung zu Erlassen, die für den Datenschutz erheblich sind und ist nach eigenem Ermessen berechtigt, diese Stellungnahmen zu veröffentlichen;

f) arbeitet zur Erfüllung der Kontrollaufgabe mit den Kontrollorganen der anderen Kantone, des Bundes und des Auslandes zusammen;

g) ist kantonales Kontrollorgan bei der bundesrechtlichen Aufgabenerfüllung im Sinne der Bundesdatenschutzgesetzgebung[1)].

Art. 26

[1] Die Aufsichtsstelle ist befugt, ungeachtet allfälliger Geheimhaltungspflichten Untersuchungen über die Einhaltung der Datenschutzbestimmungen durchzuführen, alle für die Erfüllung des Kontrollauftrages erforderlichen Informationen über Datenbearbeitungen einzuholen, Einsicht in alle Unterlagen zu nehmen, Besichtigungen durchzuführen und sich Bearbeitungen vorführen zu lassen.

[2] Stellt die Aufsichtsstelle die Verletzung von Datenschutzvorschriften fest, so kann sie dem verantwortlichen Organ eine Empfehlung abgeben. Die anzeigende Person ist über das Ergebnis der Untersuchung und über den Inhalt der Empfehlung zu informieren.

[3] Das verantwortliche Organ nimmt innert 30 Tagen zur Empfehlung Stellung. Diese ist an keine Form gebunden. Lehnt es die Empfehlung teilweise oder vollständig ab, so kann die Aufsichtsstelle eine Empfehlung in der Form einer begründeten Verfügung erlassen.

[4] Die Aufsichtsstelle kann zudem

a) ein vorläufiges Verbot einer Datenverarbeitung anordnen;
b) die Sperrung, Löschung oder Vernichtung von Daten anordnen;
c) dem Regierungsrat oder dem Kantonsrat über datenschutzrelevante Mängel oder bei Verletzung von datenschutzrechtlichen Vorschriften Bericht erstatten.

Art. 26a

Rechtsmittel

[1] Gegen Verfügungen gemäss Art. 26 Abs. 3 und Abs. 4 lit. a und b kann vom verantwortlichen Organ beim Regierungsrat Rekurs erhoben werden.

[2] Gegen Rekursentscheide des Regierungsrates kann die Aufsichtsstelle beim Obergericht Verwaltungsgerichtsbeschwerde erheben.

[3] Soweit dieses Gesetz nichts anderes bestimmt, richtet sich das Verfahren und der Rechtsschutz nach den Bestimmungen des Verwaltungsrechtspflegegesetzes.

Art. 26b

Beschwerde- und Anzeigebefugnis

[1] Stellt die Aufsichtsstelle grobe Verletzungen von Datenschutzvorschriften durch ein öffentliches Organ fest, so erhebt sie Aufsichtsbeschwerde gemäss Art. 30 des Verwaltungsrechtspflegegesetzes.

[2] Ergeben sich Hinweise auf eine strafbare Handlung, meldet die Aufsichtsstelle dies den Strafverfolgungsbehörden.

II.

[1] Dieses Gesetz untersteht dem Referendum.

[2] Der Regierungsrat bestimmt das In-Kraft-Treten.

[3] Es ist im Amtsblatt zu veröffentlichen und in die kantonale Gesetzessammlung aufzunehmen.

Schaffhausen,

Im Namen des Kantonsrates

Der Präsident:

Die Sekretärin:

Fussnoten:

1) SR 235.1.