



Vorlage an den Landrat des Kantons Basel-Landschaft

Titel: **Tätigkeitsbericht 2009 der Aufsichtsstelle Datenschutz**

Datum: Oktober 2010

Nummer: 2010-40-09

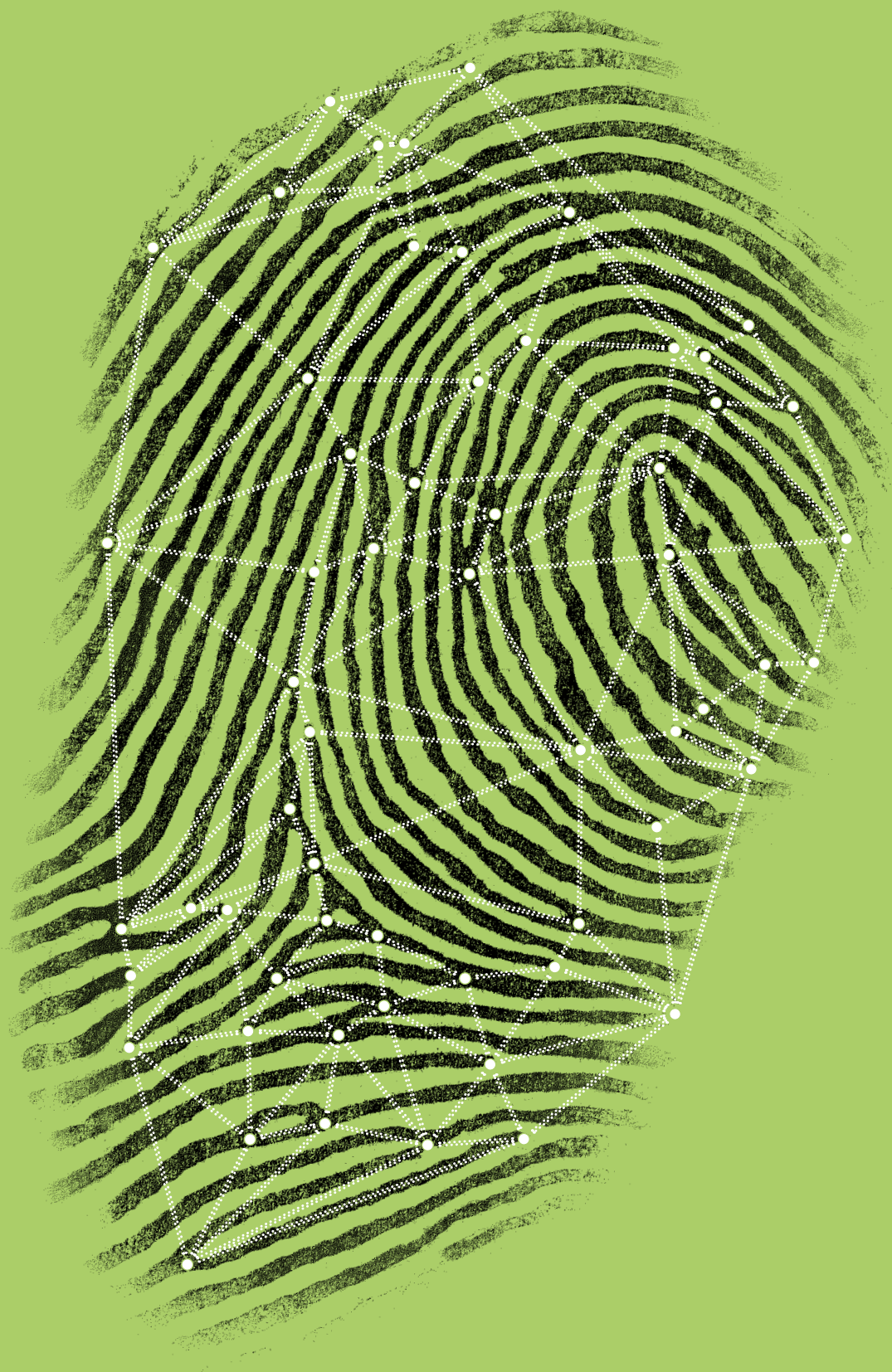
Bemerkungen: [Verlauf dieses Geschäfts](#)

Links: - [Übersicht Geschäfte des Landrats](#)
 - [Hinweise und Erklärungen zu den Geschäften des Landrats](#)
 - [Landrat / Parlament des Kantons Basel-Landschaft](#)
 - [Homepage des Kantons Basel-Landschaft](#)

**AUFSICHTSSTELLE DATENSCHUTZ
DES KANTONS BASEL-LANDSCHAFT**

TÄTIGKEITSBERICHT 2009

2010/040-09



AUFSICHTSSTELLE DATENSCHUTZ
DES KANTONS BASEL-LANDSCHAFT

Datenschutzbeauftragte: Ursula Stucki
Stv. Datenschutzbeauftragter: Michael Schnyder
Juristische Mitarbeitende: Jolanda Peier Vanotti
Philip Glass
Büro: Rathausstrasse 45/4
4410 Liestal
Telefon: 061 552 64 30
Telefax: 061 552 64 31
E-Mail: datenschutz@bl.ch
Internet: www.bl.ch/datenschutz

Gestützt auf § 24 Bst. g Datenschutzgesetz (DSG),
erstattet die Datenschutzbeauftragte dem
Landrat periodisch Bericht über ihre Tätigkeit,
ihre Feststellungen und Erfahrungen.

INHALTSVERZEICHNIS

Seite	3	I.	Das Jahr 2009 in Kürze
	4	II.	Ausgewählte Themen 2009
	4	II.I	Das Legalitätsprinzip
	5	II.II	Umsetzung des teilrevidierten Datenschutz- gesetzes (DSG)
	5	II.II.I	Register der Datensammlungen
	5	II.II.II	Empfehlungen und Weisungen
	5	II.II.III	Kontrollaufgaben
	6	II.II.IV	Kontrollablauf
	6	II.II.V	Nutzen der Kontrolle für die Behörden
	8	III.	Internationales
	8	III.I	Weiterentwicklung der Zusammenarbeit im Schengen-Raum
	8	III.II	Übernahme des Rahmenbeschlusses (RB) 2008/977/JI über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden
	8	IV.	Internet
	9	V.	Beratungstätigkeit
	9	V.I	Fälle aus der Beratungspraxis
	9	V.I.I	Systematische Datenbekanntgabe beim Übertritt in eine neue Schulstufe
	10	V.I.II	Datenbekanntgabe zwischen Sozialhilfebehörden
	12	V.I.III	Vernichtung von unzulässigerweise erhobenen Personendaten
	12	V.I.IV	Datenbekanntgabe zwecks Wissenschaft und Forschung
	12	V.I.V	Wahrung des Berufsgeheimnisses versus Transparenz
	13	V.I.VI	Unvollständig anonymisiertes Urteil im Internet
	14	V.I.VII	Überwachung der Internetnutzung
	14	VI.	Kontrolltätigkeit
	14	VI.I	Kontrolle des sog. kantonalen Staatsschutzes
	16	VII.	Stellungnahmen
	17	VIII.	Informationstätigkeit
	17	VIII.I	Medien
	17	VIII.II	Publikationen
	17	VIII.III	Kurse und Referate
	17	IX.	Zusammenarbeit national und international
	17	IX.I	Zusammenarbeit der kantonalen Datenschutz- behörden
	18	IX.II	Zusammenarbeit mit dem Eidg. Datenschutz- und Öffentlichkeitsbeauftragten (EDEOB)
	18	IX.III	Grenzüberschreitende Zusammenarbeit
	18	IX.III.I	Rücktritt aus den europäischen Arbeitsgruppen
	19	IX.III.II	Case Handling Workshop
	19	X.	Ausblick
	20		Anhang

I. DAS JAHR 2009 IN KÜRZE

2009 war ein arbeitsintensives und abwechslungsreiches Jahr. Ob einfach oder komplex, ob kommunal oder international, im Zentrum unserer Tätigkeiten stand auch im vergangenen Jahr der Mensch und sein Recht auf informationelle Selbstbestimmung.

Das stetige Wachstum des elektronischen Datenaustausches, die rasante Entwicklung neuer Technologien sowie die damit zusammenhängenden neuen Kommunikationsformen haben uns thematisch gefordert. Es hat uns einmal mehr gezeigt, dass die stete Auseinandersetzung mit neuen Entwicklungen aus den Bereichen Technik und Recht für jede Datenschutzbehörde unabdingbar ist.

Die kantonalen Behörden nutzen die neuen Technologien auch, denn schliesslich sind sie verpflichtet, ihre Datenbearbeitungsprozesse möglichst wirkungsvoll und effizient zu gestalten. Für staatliche Behörden kann Effizienz jedoch nur so lange Leitlinie sein, als auch gleichzeitig die Grundrechte und die rechtsstaatlichen Prinzipien Beachtung finden. Im Berichtsjahr mussten wir feststellen, dass diese Zusammenhänge nicht überall bekannt sind und Projekte zuweilen vorangetrieben werden, ohne dass die rechtlichen Rahmenbedingungen zuvor geprüft worden sind.

2009 waren wir wieder mehrheitlich beratend tätig. 163 Behördenanfragen und 75 Anfragen von Privaten sind bei uns eingegangen, und zur Beantwortung der vielfältigen Fragen haben wir vom Gemeinderecht bis hin zum Europarecht unterschiedlichste Erlasse konsultiert.

Neben der Beratungstätigkeit haben wir unsere Kontrolltätigkeit weiter aufgebaut und bewegen uns in kleinen Schritten in Richtung einer professionellen Kontrollbehörde. Der Prozess kommt langsam, aber stetig voran. Dazu gehört die Auseinandersetzung mit effizienten Kontrollmethoden, die im schweizerischen Datenschutz erst im Aufbau sind. Anlässlich einer Kontrolle des sog. «kantonalen Staatsschutzes» konnten wir erste wertvolle Erfahrungen sammeln. Darüber hinaus haben wir, mit externer Unterstützung, eine umfangreichere Kontrolle gestartet, die die Nutzung des Schengener Informationssystems (SIS) zum Gegenstand hat. Das Ergebnis dieser Kontrolle sollte im ersten Quartal 2010 vorliegen.

Ferner hat die Aufsichtsstelle wissenschaftliche Studien auf ihre Datenschutzkonformität geprüft und konnte in allen Fällen einer Datenbekanntgabe gemäss § 12 Abs. 4 DSG zustimmen.

Wir verfassten zudem Stellungnahmen zu unterschiedlichsten Rechtsetzungsvorhaben. Dabei stand der Entwurf zu einem Informations- und Datenschutzgesetz (IDG) im Vordergrund. Aber auch die Weiterentwicklung des sog. Schengen-Besitzstandes war mit grösseren Gesetzesanpassungen verbunden.

Im Rahmen von mehreren Zeitungs- und Radioberichten hatten wir Gelegenheit, uns zu datenschutzrechtlichen Fragen zu äussern. Die Themen Google Street View und Videoüberwachung waren dabei die thematischen Spitzenreiter.

Ein weiterer wichtiger Pfeiler unserer Arbeit war und ist die Aus- und Weiterbildung. Im Berichtsjahr konnten wir Lernende des KV und Polizeiaspirantinnen und -aspiranten im Datenschutzrecht ausbilden. Ferner haben wir sechs Referate vor unterschiedlichem Publikum gehalten.

Die Aufsichtsstelle Datenschutz pflegte auch 2009 den fachlichen Austausch mit Datenschutzbehörden im In- und Ausland und durfte in verschiedenen Arbeitsgruppen mitwirken.

Das letzte Jahr war sehr vielseitig und unsere Jahresplanung wurde – der Macht des Faktischen gehorchend – durch unplanbare Ereignisse relativiert. Die Abhängigkeit von äusseren Faktoren ist typisch für Datenschutzbehörden und erschwert zuweilen eine solide Arbeits- und Ressourcenplanung. Nicht alles, was wir uns vorgenommen hatten, konnten wir auch umsetzen. Zu kurz gekommen sind vor allem proaktive Tätigkeiten wie z. B. der Aufbau eines modularen Schulungskonzepts oder das Verfassen von Merkblättern.

II. AUSGEWÄHLTE THEMEN 2009

Das Berichtsjahr war wieder äusserst abwechslungsreich, die Themenvielfalt spannend und herausfordernd zugleich. Die im Folgenden beschriebenen Themenbereiche, Feststellungen und Erläuterungen beziehen sich nur auf einen kleinen Ausschnitt unserer Tätigkeit.

Das Legalitätsprinzip war leider wieder ein Thema. Es scheint nach wie vor noch nicht in genügendem Mass bekannt zu sein, dass staatliche Organe Daten der Bürgerinnen und Bürger nur bearbeiten dürfen, wenn eine gesetzliche Grundlage die Bearbeitung vorsieht.

Innerbetrieblich haben wir uns mit der Umsetzung der neuen datenschutzrechtlichen Vorgaben beschäftigt. Wir haben dabei unsere Priorität auf den erwähnten Aufbau unserer Kontrolltätigkeit gelegt und mit der Einführung des Instruments der Vorabkontrolle begonnen.

Ferner hat der grenzüberschreitende Datenaustausch zu teilweise umfassenden Gesetzgebungsprojekten in Bund und Kanton geführt.

Und schliesslich haben wir uns erneut mit der Entwicklung neuer Informationstechnologien und deren Einsatz in der Datenbearbeitung beschäftigt. Neben dem Dauerthema Videoüberwachung haben auch das Internet und seine mannigfaltigen Nutzungsmöglichkeiten einige Datenschutzfragen aufgeworfen.

II.I. DAS LEGALITÄTSPRINZIP

Das Legalitätsprinzip wird auch Prinzip der Gesetzmässigkeit genannt. Es besagt, dass sich ein staatlicher Akt auf einen generell-abstrakten Erlass (Gesetz, Dekret, Verordnung etc.) stützen muss, der

hinreichend bestimmt und vom zuständigen Organ (Stimmvolk, Landrat, Regierung) erlassen worden ist.¹

In der Kantonsverfassung Basel-Landschaft (KVBL) finden sich Normen, die das Legalitätsprinzip widerspiegeln. So statuiert z. B. § 4 KVBL «Alle Behörden sind an Verfassung und Gesetz gebunden. Ihr Handeln muss im öffentlichen Interesse liegen und verhältnismässig sein. Behörden und Private verhalten sich nach Treu und Glauben.» Ferner besagt § 15 KVBL, dass Einschränkungen der Grundrechte einer gesetzlichen Grundlage bedürfen und dass schwerwiegende Einschränkungen im Gesetz ausdrücklich vorgesehen sein müssen. Eine Abweichung von diesem Prinzip bleibt für Fälle ernster, unmittelbarer und offensichtlicher Gefahr vorbehalten. Vereinfacht gesagt bedeutet das Legalitätsprinzip, dass staatliche Behörden nur gestützt auf entsprechende gesetzliche Grundlagen tätig werden dürfen.²

Trotz dieser klaren verfassungsmässigen Vorgaben mussten wir wieder feststellen, dass Projekte ohne genügende gesetzliche Grundlage weit vorangetrieben oder gar gestartet wurden. Projektverantwortliche stellten zwar Mittel für Technisches oder Organisatorisches ein, die notwendigen Ressourcen für die Prüfung der rechtlichen Rahmenbedingungen wurden dagegen oft vergessen.

Entgegen einer weitverbreiteten Auffassung ist es in solchen Fällen nicht «der Datenschutz», der das Projekt verzögert, sondern vielmehr das Nichtbeachten der rechtsstaatlichen Rahmenbedingungen. Wird das Legalitätsprinzip erst berücksichtigt, wenn die Aufsichtsstelle interveniert, ist dies zu spät und letztlich für alle Beteiligten unbefriedigend.

1) Vgl. Häfelin/Müller/Uhlmann: Allgemeines Verwaltungsrecht, 5. Aufl., 2006, Seite 79.

2) Vgl. § 6 ff. DSG.

II.II. UMSETZUNG DES TEILREVIDIERTEN DATENSCHUTZGESETZES (DSG)

Die Umsetzung der neuen datenschutzrechtlichen Vorgaben entwickelt sich unterschiedlich. Während wir uns im Berichtsjahr mit den Bedingungen der neuen Vorabkontrolle befasst haben, weil wir 2010 ein entsprechendes Merkblatt herausgeben möchten, ist die Einführung des Verzeichnisses der Datensammlungen ins Stocken geraten und aufgrund der diskutierten Einführung des Öffentlichkeitsprinzips zurückgestellt worden.

II.II.I. REGISTER DER DATENSAMMLUNGEN³

Das Verzeichnis der Datensammlungen dient der Transparenz und ist Teil des datenschutzrechtlichen Auskunftsrechts. Bürgerinnen und Bürger sollen mit einfachen Mitteln erkennen können, welche Datensammlungen im Kanton und in den Gemeinden vorhanden sind. Dies bedingt zumindest eine Inventarisierung der Datenbestände durch die verantwortliche Behörde. Entsprechende Softwareprogramme existieren seit einigen Jahren und werden von anderen Kantonen eingesetzt. Wir haben deshalb im Berichtsjahr eine Veranstaltung mit den IT-Verantwortlichen des Kantons organisiert, an der ein derartiges Programm vorgestellt wurde, das – auf Wunsch – auch eine Anbindung der Gemeinden ermöglicht hätte. Es hat nicht erstaunt, dass die Pflicht zur Führung eines Registers der Datensammlungen nicht auf grosse Akzeptanz gestossen ist, ist doch bereits in den 1990er-Jahren ein erster Versuch gescheitert.

Aufgrund des übergeordneten Rechts besteht die Informationspflicht der Behörden aber nach wie vor. Wegen der anstehenden Beratung des Entwurfs für ein Informations- und Datenschutzgesetz haben wir das Thema einstweilen zurückgestellt und hoffen, dass eine etwas vereinfachte und effizient umsetzbare Lösung gefunden werden kann.

3) § 16 DSG.

II.II.II. EMPFEHLUNGEN UND WEISUNGEN⁴

Mit der Revision des Datenschutzgesetzes hat die Aufsichtsstelle neue Kompetenzen und Verantwortlichkeiten erhalten. Neben einfachen Beratungen und Stellungnahmen kann die Aufsichtsstelle heute förmliche Empfehlungen erteilen und Weisungen erlassen, die letztlich bis ans Kantonsgericht gezogen werden können. Erfreulicherweise mussten wir 2009 diese Mittel nicht einsetzen und konnten Differenzen einvernehmlich bereinigen.

4) § 25 Abs. 3–5 DSG.

II.II.III. KONTROLLAUFGABEN

Das bis zum 1. Juli 2008 geltende Datenschutzgesetz enthielt die Bestimmung, wonach die Aufsichtsstelle die Anwendung der Bestimmungen des Datenschutzgesetzes überwacht. Diese Bestimmung wurde revidiert und neu formuliert. Nach dem nun geltenden Recht kontrolliert die Aufsichtsstelle nach einem durch sie autonom aufzustellenden Prüfprogramm die Anwendung der Bestimmungen über den Datenschutz.⁵ Damit wird die Unabhängigkeit der Aufsichtsstelle festgehalten und gleichzeitig klargestellt, dass es nicht Aufgabe der Datenschutzbehörde ist, die Rechtmässigkeit der kantonalen Datenbearbeitungsprozesse permanent und lückenlos zu überwachen (was ohnehin nicht möglich wäre). Die Tatsache, dass die Rechtmässigkeit einzelner Datenbearbeitungsprozesse jederzeit kontrolliert werden kann, wird indessen Wirkung zeigen und einiges dazu beitragen, dass das Grundrecht auf informationelle Selbstbestimmung im beruflichen Alltag vermehrt beachtet wird.

Im Rahmen des Aufbaus unserer Kontrolleinheit (zurzeit 20–30 Stellenprozent) haben wir festgestellt, dass Kontrollen grösserer Organisationseinheiten und Systeme nur unter Beizug externer Fachleute zu bewältigen sein werden, denn kleine Datenschutzbehörden verfügen weder über ausgewiesene Betriebswirtschaftler noch über entsprechende IT-Fachleute.

5) § 24 Bst. a DSG.

Kontrollablauf

Im Folgenden soll unser gewählter Kontrollablauf skizziert werden.

- a. Bestimmung der Behörde oder der Organisationseinheit, die geprüft werden soll. Mögliche Auswahlkriterien:
 - Werden besondere Personendaten⁶ bearbeitet?
 - Werden Persönlichkeitsprofile⁷ erstellt?
 - Werden die Daten elektronisch abgerufen?
 - Handelt es sich um ein Pilotprojekt oder eine neue Datenbank?
 - Hat eine Stelle wiederholt datenschutzrechtliche Vorgaben verletzt?
 - Aktueller Anlass.
 - Koordinierte Kontrolle durch mehrere Datenschutzbehörden.
- b. Erste Kontaktaufnahme mit der zu kontrollierenden Behörde.
- c. Evaluation der von der Behörde genutzten Systeme.
- d. Feststellen allfälliger riskanter Datenbearbeitungsprozesse.
- e. Interview mit den Verantwortlichen oder Fragebogen zu Organisation und Art der Bearbeitung sowie zu den rechtlichen Rahmenbedingungen.
- f. Kontrolle vor Ort.
- g. Verfassen eines Kontrollberichts, in dem die relevanten Kontrollpunkte, die Ergebnisse sowie allfällige Empfehlungen festgehalten werden.
- h. Weiterleiten des Berichts an die kontrollierte Behörde zur Stellungnahme.
- i. Besprechung des Berichts mit der kontrollierten Institution sowie der vorgesetzten Behörde.
- j. Abschluss der Kontrolle.
- k. Nachkontrolle der Umsetzung der empfohlenen Massnahmen.

6) § 5 Abs.1 bis DSG.

7) § 5 Abs.1 ter DSG.

Von dieser grob skizzierten Vorgehensweise kann es je nach Situation Abweichungen geben.

Nutzen der Kontrolle für die Behörden

Schon bei der Bestimmung des Kontrollinhalts ist die zu kontrollierende Institution involviert und muss Zeit für die Beantwortung der Fragen aufwenden. Nicht anders ist dies bei den weiteren Schritten. Die Aufsichtsstelle ist sich bewusst, dass der zeitliche Aufwand für die kontrollierte Institution – je nach Kontrollumfang – erheblich sein kann.

Die Kontrolle kann aber dazu dienen, allfällige Schwachstellen bei der Bearbeitung von Personendaten zu erkennen und Massnahmen für deren Behebung zu treffen. So kann u. a. das Risiko einer Anzeige wegen Amtsgeheimnisverletzung oder einer Haftungsklage minimiert werden. Letztlich kann ein gutes Kontrollergebnis aber auch das Vertrauen der Bevölkerung in staatliche Institutionen steigern.



III. INTERNATIONALES

III.I. WEITERENTWICKLUNG DER ZUSAMMENARBEIT IM SCHENGENRAUM

Die Schweiz kann bei jeder Weiterentwicklung des Schengen-Rechts souverän entscheiden, ob sie einen neuen Rechtsakt übernehmen will. Für die Übernahme eines Rahmenbeschlusses in die schweizerische Rechtsordnung beträgt die Frist zwei Jahre.⁸

In einem ersten Schritt werden die Kantone eingeladen, zur Übernahme eines Rechtsakts Stellung zu nehmen. Anschliessend werden sie im Rahmen des Vernehmlassungsverfahrens aufgefordert, sich zu den konkreten Umsetzungsvorhaben zu äussern. Gleichzeitig werden die Kantone verpflichtet, ihren innerkantonalen Handlungsbedarf zu prüfen und entsprechende Anpassungen im kantonalen Recht an die Hand zu nehmen. Der zeitliche Rahmen von zwei Jahren scheint uns in der Praxis u. a. aufgrund der föderalistischen und direkt demokratischen Strukturen der Schweiz eher knapp bemessen.

III.II. ÜBERNAHME DES RAHMENBESCHLUSSES (RB) 2008/977/JI⁹

Der Rahmenbeschluss bezweckt den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit verarbeitet werden. Die im Rahmenbeschluss vorgesehenen Regelungen sind teils direkt anwendbar, teils müssen sie ins innerstaatliche Recht umgesetzt werden. Aufgrund der Organisationshoheit der Kantone sind diese berechtigt und verpflichtet, ihr formelles Datenschutzrecht autonom zu regeln.

Nachdem der Bundesrat die Übernahme dieses Rahmenbeschlusses am 14. Januar 2009 gutgeheissen hatte, hatten wir im Rahmen der kantonsinternen Vernehmlassung Gelegenheit, uns zu den daraus folgenden Gesetzesänderungen zu äussern.¹⁰ Die Übernahme auf Bundesebene sah eine Änderung von sechs Bundesgesetzen¹¹ vor und es war sehr aufwändig, sich einen Überblick über das Umsetzungsvorhaben zu verschaffen.

Die eingehende Überprüfung des Rahmenbeschlusses sowie der Vorlage des Bundes hat ergeben, dass das kantonale Datenschutzrecht in einzelnen Punkten angepasst werden muss. So fehlen z. B. Regelungen über die Weiterverarbeitung empfangener Daten (Art. 13 RB), spezifische Löschfristen (Art. 5 RB) oder spezielle Protokollpflichten (Art. 11 RB). Ob die offenen Punkte im Rahmen des IDG oder in einem separaten kantonalen Erlass geregelt werden, ist noch offen.

8) Art. 7 Abs. 2 lit. b zweiter Satz des Abkommens über die Assozierung der Schweizerischen Eidgenossenschaft bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstandes zwischen der Schweiz und der EU vom 26. Oktober 2004.

9) Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, ABl. 350/2008, S. 60.

10) http://privatim.ch/content/pdf/vernehmlassung_rahmenbeschluss_20090813.pdf.

11) Bundesgesetz vom 16. Dezember 2005 über die Ausländerinnen und Ausländer (AuG); Asylgesetz vom 26. Juni 1998 (AsyIG); Bundesgesetz über den Datenschutz vom 19. Juni 1992 (DSG); Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (StGB); Waffengesetz vom 20. Juni 1997 (WG); Betäubungsmittelgesetz vom 3. Oktober 1951 (BetmG); Bundesgesetz über den Informationsaustausch zwischen den Strafverfolgungsbehörden des Bundes und denjenigen der anderen Schengen-Staaten vom 12. Juni 2009 (SlaG).

IV. INTERNET

Das Internet gilt als schier unerschöpfliche globale Informationsquelle und weltweite Kommunikationsplattform. Informationen sind rasch abgerufen oder ins Netz gestellt. Man kommuniziert via Mail, diskutiert in Blogs, nutzt Chatrooms, hat teilweise virtuelle Freunde im Social Network oder hat schlicht einen elektronischen Newsletter abonniert. Der Kanton und viele Gemeinden nutzen das Internet als Informationsplattform für ihre Einwohnerinnen und Einwohner.

Ob geschäftlich oder privat, das Internet mit seinen vielfältigen Möglichkeiten lässt sich aus unserem Alltag nicht mehr wegdenken. Die Nutzung des Internets ist aber mit Risiken verbunden, auf die wir im Rahmen unserer Tätigkeit regelmässig hinweisen. Dabei geht es uns nicht darum, die Gefahren im Internet übermässig zu betonen oder gar ein Schreckensszenario aufzuzeichnen. Es geht vielmehr darum, die Nutzerinnen und Nutzer zu informieren, damit sie sich der Risiken bewusst werden und diese selbst einschätzen können.

Wenn wir Behörden in Bezug auf Internetpublikationen zur Zurückhaltung auffordern, wird uns oft entgegengehalten, die Menschen würden ihre

persönlichsten Daten ja freiwillig im Internet offenlegen. Das ist in vielen Fällen tatsächlich so. Man sollte jedoch berücksichtigen, dass öffentliche Organe mit hoheitlich erhobenen Daten von Bürgerinnen und Bürgern arbeiten, die diese in der Regel nicht freiwillig offengelegt haben. Wer diese Daten im Internet publiziert, trägt eine entsprechend erhöhte Verantwortung. Zudem sind staatliche Behörden an das Legalitätsprinzip gebunden. Eine Publikation im weltweiten Internet muss folglich in einer gesetzlichen Grundlage vorgesehen sein.

Das Grundrecht auf informationelle Selbstbestimmung¹² verpflichtet den Staat, die Daten seiner Bürgerinnen und Bürger vor Missbrauch zu schützen. Die Behörden¹³ sind deshalb verpflichtet, die Risiken für den Einzelnen vor einer Internetpublikation zu prüfen. Im Rahmen dieser Risikoanalyse sollte beachtet werden, dass die Daten im Internet weltweit rund um die Uhr von jedermann abrufbar sind. Zudem sollte man wissen, dass Suchmaschinen Daten der Suchenden speichern und Archivierungsprogramme das Netz durchforsten. Die so gewonnenen Daten können ohne Kenntnis der Betroffenen weiterbearbeitet oder auf unbekannte Zeit gespeichert werden. Sind die Daten also einmal im Netz, verlieren die betroffenen Personen und die verantwortliche Behörde die Kontrolle über deren Weiterverwendung.

Wer im Internet Daten von Dritten publiziert, übernimmt die Verantwortung für deren Weiterverwendung und muss im Schadensfall mit Haftungsansprüchen rechnen. Eine Internetpublikation sollte daher nur rechtmässig und mit der erforderlichen Sorgfalt erfolgen (vgl. 5.1.6).

12) Art. 13 Abs. 2 BV § 6 KV.

13) Behörden gemäss § 3 DSG.

V. BERATUNGSTÄTIGKEIT

Um einen Eindruck der Themenvielfalt zu vermitteln, werden an dieser Stelle ein paar spontan zusammengestellte Stichworte aus unserer Geschäftskontrolle aufgezählt: Ahnenforschung, Akteneinsicht, Amtsgeheimnis, Anmeldungs- und Registergesetz, Archivierung, Alkohol- und Suchtberatung, AHV-Nummer, Brandlager, Datenaustausch mit dem Ausland, Diagnose und Befund, Durchbrechung der Datensperre, Durchimpfungsgrad, Gemeinden, Grundbuch, Internet, Jugendstrafrecht, kantonales Personenregister, Kirchen, Mieterdaten, Mitarbeitergespräche, Mitarbeiterüberwachung, Polizeirapporte, Registerharmonisierung, Schuladministration, Schengen, Sozialhilfe, Schulpsychologischer Dienst, Schätzungsprotokolle, Schweinegrippe, Spitex, Tonbandaufnahmen, Verwaltungsorganisationsgesetz, Videoüberwachung, Zustimmungserklärung etc.

Zur Beantwortung der diversen Fragen konsultierten wir ein breites Spektrum von Rechtsvorschriften, vom Gemeinde- bis hin zum Europarecht.

V.I. FÄLLE AUS DER BERATUNGSPRAXIS

Die folgende Darstellung dokumentiert unsere Einzelfallbearbeitung auszugsweise. Die Fälle werden soweit als möglich so dargestellt, dass weder einzelne Behörden noch involvierte Personen erkennbar sind.¹⁴

14) Selbstverständlich stehen unsere Akten der parlamentarischen Aufsicht offen.

V.I.I. SYSTEMATISCHE DATENBEKANNTGABE BEIM ÜBERTRITT IN EINE NEUE SCHULSTUFE

Wir werden immer wieder von Eltern und Lehrpersonen angefragt, welche Personendaten beim Übertritt in eine neue Schulstufe bekanntgegeben werden dürfen.

Schulen bearbeiten viele, zum Teil heikle Daten. Dazu gehören u. a. die Beurteilung von Leistung

und Verhalten der Schülerinnen und Schüler, Angaben zum persönlichen Umfeld, Informationen über die Gesundheit oder über therapeutische Massnahmen. Wir werden deshalb auch regelmässig von Lehrpersonen und Erziehungsberechtigten angefragt, was beim Übertritt in eine neue Schulstufe mit diesen Informationen geschieht.

Als Grundsatz gilt, dass jedes Kind beim Übertritt in eine neue Schulstufe eine Chance für einen Neuanfang erhalten soll. Dies bedeutet, dass die Schulen nicht automatisch ein umfangreiches Dossier der Schülerinnen und Schüler weitergeben dürfen. Der Persönlichkeitsschutz des Kindes hat vielmehr zum Ziel, dass jede neue zuständige Lehrperson sich selbst ein aktuelles Bild über die Schülerin bzw. den Schüler macht.

Von diesem Grundsatz gibt es Ausnahmen. So müssen die Lehrpersonen selbstverständlich alle Informationen erhalten, die für den Schulalltag relevant sind. Dazu gehören:¹⁵

- Personalien: Name, Vorname, Adresse, Geschlecht, Geburtsdatum, Telefon.
- Weitere Angaben zur Person: Nationalität, Erziehungsberechtigte (Namen und Vornamen, Adresse, Telefonnummer).
- Die bisherige Klasse.
- Die Muttersprache bzw. die Fremdsprachigkeit.
- Abgebende Lehrperson mit Namen, Adresse und Telefon.
- Besuch des bisherigen Religionsunterrichtes ja oder nein.
- Der Promotionsentscheid betr. Sekundarstufe I.
- Empfehlung betr. Niveau und Zuteilungsentscheid.
- Empfehlung betr. Regelklasse bzw. Einführungsklasse.
- Nicht abgeschlossener Förderunterricht.

Sind weitere Informationen erforderlich, weil sie für den Schulalltag relevant sind und weil die schulischen Leistungen beeinträchtigt werden können, müssen die Erziehungsberechtigten die Klassenlehrpersonen über Besonderheiten informieren.¹⁶ Dies können z. B. Angaben über Allergien, Krankheiten, Ängste, besondere familiäre Umstände etc. sein. Aufgrund der besonderen Sensibilität dieser Daten sind solche Angaben direkt bei den Erziehungsberechtigten zu erheben.

Zusammenfassend ist festzustellen, dass der Datenaustausch an staatlichen Schulen einer sorgfältigen Interessensabwägung bedarf. Neben den berechtigten Interessen der Lehrerschaft müssen die Rechte der Schülerinnen und Schüler sowie deren Erziehungsberechtigten mitberücksichtigt werden. Dies gilt umso mehr, als einige Daten, die an Schulen erhoben werden, zu den besonders schützenswerten Personendaten zählen (z. B. Angaben zur Gesundheit, über die Intimsphäre etc.).

15) Vgl. Leitfaden Datenschutz für Kindergärten, Schulen und spezielle Schuldienste des Kantons Baselstadt, <http://www.baselstadt.ch/fileadmin/baselstadt/files/docs/jpd/ds/prak/prak-022.pdf>.

16) Die Erziehungsberechtigten sind verpflichtet, die Klassenlehrerin oder den Klassenlehrer frühzeitig über besondere Umstände zu informieren, die ihre Kinder in ihrer schulischen Leistungsfähigkeit beeinträchtigen können (§ 59 der Verordnung für den Kindergarten und die Primarschule vom 13. Mai 2003 [SGS 641.11], § 39 der Verordnung für die Sekundarschule vom 13. Mai 2003 [SGS 642.11]).

V.I.II. DATENBEKANNTGABE ZWISCHEN SOZIALHILFEBEHÖRDEN

Wir wurden von einem Bürger angefragt, ob es zulässig sei, dass die Sozialberatung seiner jetzigen Wohngemeinde seiner früher zuständigen ausserkantonalen Sozialhilfebehörde melde, dass er seit einiger Zeit eine Rente beziehe.

Wir haben mit der Sozialberatung Kontakt aufgenommen und um eine Stellungnahme gebeten. Aufgrund der eingegangenen Informationen und ergänzender rechtlicher Abklärungen kamen wir zum Schluss, dass die Mitteilung der Sozialberatung an die auswärtige Sozialhilfebehörde rechtmässig war.

Die Sozialberatung hatte den Fragesteller aufgefordert, mit seiner ehemaligen Sozialhilfebehörde Kontakt aufzunehmen, da er aufgrund einer zugesprochenen Rente gewisse Leistungen hätte rückerstatten müssen. Da der Fragesteller jedoch keinen Kontakt mit der auswärtigen Sozialhilfebehörde aufgenommen hatte, hegte die Sozialberatung den Verdacht, dass er den Rentenbezug verheimlichen wollte, um dadurch doppelte Leistungen zu beziehen.

Das Sozialhilfegesetz des Kantons Basel-Landschaft sieht in § 42 Abs. 3 vor, dass die Gemeinden und der Kanton den Missbrauch von Sozialhilfe bekämpfen. Aufgrund des Umstandes, dass der Rentenbezug nicht gemeldet wurde, bestand der Verdacht auf Missbrauch der Sozialhilfe. Dies berechnete die Sozialberatung im vorliegenden Einzelfall, den Rentenbezug der auswärtigen Gemeinde zu melden, damit diese den Rückerstattungsanspruch geltend machen konnte.



V.I.III. VERNICHTUNG VON UNZULÄSSIGER-WEISE ERHOBENEN PERSONENDATEN

Eine kantonale Amtsstelle führte eine in ihren gesetzlichen Aufgabenbereich fallende Umfrage bei basellandschaftlichen Arbeitgebern durch. Dabei mussten die Arbeitgeber diverse Angaben zu Arbeitnehmern machen. Nebst Angaben zu Geburtsdatum, Nationalität, Lohn, Geschlecht etc. verlangte die kantonale Amtsstelle auch die Herausgabe von Namen und Vornamen der Angestellten.

Abklärungen der Aufsichtsstelle ergaben, dass die Erhebung von Namen und Vornamen der Angestellten für die Erfüllung des Zweckes der Umfrage zum damaligen Zeitpunkt nicht erforderlich war. Die notwendigen Erkenntnisse aus der Umfrage konnten auch aus den anonymisierten restlichen Angaben gewonnen werden. Die Erhebung von Namen und Vornamen erwies sich aus datenschutzrechtlicher Sicht als unverhältnismässig und war somit unzulässig, denn einer der Grundsätze bei der Bearbeitung von Personendaten lautet: Die Bearbeitung von Personendaten hat nach Treu und Glauben zu erfolgen und muss verhältnismässig sein (§ 6 Abs. 3 DSG BL).

Mit der kantonalen Amtsstelle wurden folgende Massnahmen vereinbart:

- Die bereits erhobenen Namen und Vornamen werden umgehend vernichtet.
- Zukünftige Datenerhebungen sind mit einem Hinweis auf die gesetzlichen Grundlagen dieser Datenerhebung zu versehen. Dies erleichtert es dem angefragten Dateninhaber, über die Zulässigkeit seiner Datenweitergabe zu entscheiden.

V.I.IV. DATENBEKANNTGABE ZWECKS WISSENSCHAFT UND FORSCHUNG

Datenschutz soll Wissenschaft und Forschung nicht unnötig einschränken. Das Datenschutzgesetz sieht daher in § 12 Abs. 4 vor, dass Personendaten Privaten für Zwecke der Wissenschaft und Forschung bekanntgegeben werden dürfen, sofern

u. a. die Zustimmung der Aufsichtsstelle vorliegt. Im Berichtsjahr haben wir drei Studienkonzepte aus dem medizinischen und sozialmedizinischen Bereich u. a. auf ihre Wissenschaftlichkeit hin geprüft und der Datenbekanntgabe zustimmen können.

Eine Zustimmung nach § 14 Abs. 4 DSG kann erteilt werden, wenn die Wissenschaftlichkeit der Arbeit aufgrund der eingereichten Unterlagen erwiesen ist und wenn keine besonderen Geheimhaltungsbestimmungen gegen eine Datenbekanntgabe sprechen. Bevor die Zustimmung erfolgt, verpflichten sich die Wissenschaftler schriftlich, u. a. die Daten nur für den angegebenen Zweck zu verwenden, keine Personendaten an Dritte weiterzugeben, die Daten rasch möglichst zu anonymisieren und die Ergebnisse der wissenschaftlichen Arbeit nur so bekanntzugeben, dass die betroffenen Personen nicht mehr bestimmbar sind. Die Wissenschaftler verpflichten sich zudem ausdrücklich, für die Datensicherheit inkl. der Löschung der Daten zu sorgen.

Die Datenschutzbehörde überprüft die Wissenschaftlichkeit und trägt für diese Beurteilung die Verantwortung. Die Behörde, die die Personendaten bekanntgibt, bleibt aber – wie bei anderen Datenbekanntgaben auch – für die Einhaltung der weiteren datenschutzrechtlichen Vorgaben weiterhin verantwortlich (§ 4 DSG).

V.I.V. WAHRUNG DES BERUFSGEHEIMNISSES VERSUS TRANSPARENZ

Ein Institut der Universität Bern wollte die Zustimmung der Aufsichtsstelle für das Einholen von bestimmten Personendaten für Forschungszwecke (§ 12 Abs. 4 DSG BL). Benötigt wurden Daten von Kindern, die an Krebs erkrankt waren. Die Daten

wurden einerseits zum Zwecke der Forschung für bereits definierte Projekte benötigt und andererseits zum Zwecke der Vervollständigung der Datenbank des Kinderkrebsregisters. Erhoben werden sollten die Daten bei den Einwohnerdiensten der Gemeinden. Eine Prüfung der Voraussetzungen für die

Datenbekanntgabe an das Institut ergab, dass diese datenschutzrechtlich zulässig war.

Im Zusammenhang mit der Anfrage des Instituts bei den Einwohnerdiensten stellte sich aber die Frage nach der Vereinbarkeit der Wahrung der ärztlichen Schweigepflicht (Berufsgeheimnis) mit dem Erfordernis der Transparenz gegenüber den Einwohnerdiensten. Fragte das Institut mit seiner vollständigen Bezeichnung und unter Angabe des Zweckes (Forschung resp. Vervollständigung des Kinderkrebsregisters) die Einwohnerdienste an, war klar, dass das Kind, dessen Daten abgefragt wurden, an Krebs leidet. Die Preisgabe dieser Tatsache stellt eine Verletzung des Berufsgeheimnisses dar. Damit die Einwohnerdienste, die für den Datenschutz verantwortlich sind, entscheiden können, ob sie die Auskunft erteilen dürfen, müssen sie wissen, wem sie die Daten bekanntgeben. Wie sollen sie den Entscheid treffen können, wenn sie nicht einmal wissen dürfen, wer anfragt? Um richtig entscheiden zu können, müssen die Einwohnerdienste also wissen, wer anfragt und zu welchem Zweck die Daten erhoben werden.

Für die Lösung dieses Interessenkonfliktes gibt es verschiedene Ansätze:

- Eine Institution, die einem Berufsgeheimnis unterliegt, gelangt zuerst an die Aufsichtsstelle. Diese prüft die Zulässigkeit der verlangten Datenbekanntgabe. Ist die Datenbekanntgabe zulässig, teilt sie den Behörden, die die Daten bekanntgeben sollen, mit, dass sie dies tun können. Dabei ist der Empfänger gegenüber der bekanntgebenden Behörde so weit zu anonymisieren, dass keine Rückschlüsse auf Umstände, die dem Berufsgeheimnis unterliegen, gemacht werden können. Diese Lösung hat den Nachteil, dass die Verantwortung für die Datenweitergabe von den eigentlichen Entscheidungsträgern weggenommen und auf die Aufsichtsstelle übertragen wird. Dies widerspricht einerseits dem Grundsatz von § 4 DSG. Andererseits wäre der Aufwand, jede Anfrage einer Institution durch die Aufsichtsstelle bearbeiten zu lassen, unverhältnismässig gross.
- Die anfragende Institution erhält einen direkten (Online-)Zugriff auf die Daten. Es müsste klar definiert werden, auf welche Daten zugegriffen werden kann und wer zugriffsberechtigt ist. Das System sollte zudem eine Protokollierung ermöglichen, die für Kontrollen der Aufsichtsstelle aktiviert werden könnte. Eine dauerhafte Protokollierung wäre dagegen kritisch, weil aus den Protokollen letztlich auch wieder erkennbar würde, welche Kinder an Krebs erkrankt sind.

Sobald das kantonale Personenregister¹⁷ vorliegt, könnte die zweite Variante als Lösung geprüft und gegebenenfalls ein gut gesicherter direkter Zugriff gewährt werden.

V.I.VI. UNVOLLSTÄNDIG ANONYMISIERTES URTEIL IM INTERNET

Eine Person beschwerte sich bei der Aufsichtsstelle, weil ein Gerichtsurteil im Internet publiziert wurde, ohne dass zuvor die Namen von Zeugen gelöscht wurden. Gab man die Namen der Zeugen in einer Suchmaschine ein, so erhielt man einen

Link auf das vollständig publizierte Urteil. Dieses Suchergebnis liess letztlich auch einen Rückschluss auf die Parteien selbst zu.

Das Publizieren von Gerichtsurteilen im Internet ist heute alltäglich und dient vor allem den juristisch Interessierten als wertvolle Informationsquelle über die Rechtsprechung. So publizieren neben dem Bundesgericht auch kantonale Gerichte regelmässig ihre Urteile. Zum Schutz der betroffenen Personen werden die Entscheide jedoch nur anonymisiert publiziert. Eine Veröffentlichung von korrekt anonymisierten Urteilen ist datenschutzrechtlich unproblematisch.

Im vorliegenden Fall wurden die Namen der Zeugen (Personendaten) unbeabsichtigt im weltweiten Netz veröffentlicht. Nach Bekanntwerden des Fehlers und entsprechender Intervention der Aufsichtsstelle wurde das Ur-

¹⁷) § 9 Anmeldungs- und Registergesetz vom 19. Juni 2008 (SR 111, ARG).

teil unverzüglich von der Seite des Kantons Basel-Landschaft entfernt. Via Suchmaschinen waren die Daten aber weiterhin weltweit zugänglich. Nachdem das Urteil auch noch auf den Servern der grossen Suchmaschinen (Google, Yahoo etc.) gelöscht worden war, war es noch auf kleineren, relativ unbekannten Suchmaschinen und in Internetarchiven vorhanden. Eine vollständige Löschung der Daten im Internet war nicht mehr möglich.

Einmal im Netz, immer im Netz. Dieser Spruch gilt immer noch. Personendaten lassen sich aus dem Internet kaum mehr eliminieren. Bei Publikationen im Internet ist deshalb grösste Vorsicht geboten. Nicht alles, was in Papierform publiziert wird, sollte auch im Internet veröffentlicht werden. Man könnte Urteile, die die Privatsphäre erheblich tangieren, nur einem bestimmten geschlossenen Benutzerkreis zugänglich machen oder nur auszugsweise publizieren. Auf diese Weise würde die Gefahr eines Datenmissbrauchs erheblich gemindert.

V.I.VII. ÜBERWACHUNG DER INTERNET-NUTZUNG

Wir erhielten einige Anfragen von Beschäftigten, die mehrheitlich anonym bleiben wollten. Sie liessen über eine Drittperson anfragen, ob ihre persönliche Internetnutzung durch die vorgesetzte

Stelle protokolliert und personenbezogen ausgewertet werden dürfe. Wir sind dem Wunsch nach Anonymität natürlich nachgekommen, es hat uns aber irritiert, dass die verwaltungsinternen Fragesteller offenbar befürchteten, ihre Anfrage würde sich negativ für sie auswirken.

Das Benutzungsreglement Informatik-Mittel¹⁸ regelt in § 14 die Kontrolle und Protokollierung der Nutzung der Systeme, Anwendungen, Netzwerke, des E-Mails, der Fernzugriffe und des Internets. Das Reglement verweist auf das Datenschutzgesetz und nennt ausdrücklich den Schutz der Privatsphäre. Es sieht u. a. eine periodische summarische Auswertung der Protokolle vor. Rückschlüsse auf bestimmte Personen sollen dabei nicht möglich sein. Ergibt sich aus der Überprüfung ein Verdacht auf Verstoss gegen dieses Reglement, so bleiben angemessene personenbezogene Prüfungen vorbehalten. Eine präventive personenbezogene Kontrolle ist aufgrund der Persönlichkeitsrechte der Arbeitnehmenden nicht erlaubt.¹⁹ Grundsätzlich müssen die Mitarbeitenden im Voraus über eine personenbezogene Prüfung informiert werden.²⁰

Eine personenbezogene Kontrolle ist also möglich, sofern sie verhältnismässig ist. Die Verhältnismässigkeit bezieht sich einerseits auf Zahl der überprüften Personen, andererseits aber auch auf die Dauer der personenbezogenen Prüfung. In einem Fall kamen wir zum Schluss, dass die Überwachung einer grösseren Organisationseinheit über einen Zeitraum von sechs Monaten unverhältnismässig lange ist und dass man einem allfälligen Missbrauch des Internets mit Führungsmitteln begegnen sollte, die weniger stark in die Grundrechte aller Mitarbeiterinnen und Mitarbeiter eingreift.

18] Benutzungsreglement Informatik-Mittel (BI) vom 17. Dezember (SGS 140.551).

19] § 14 Abs. 3 BI.

120] § 14 Abs. 4 BI.

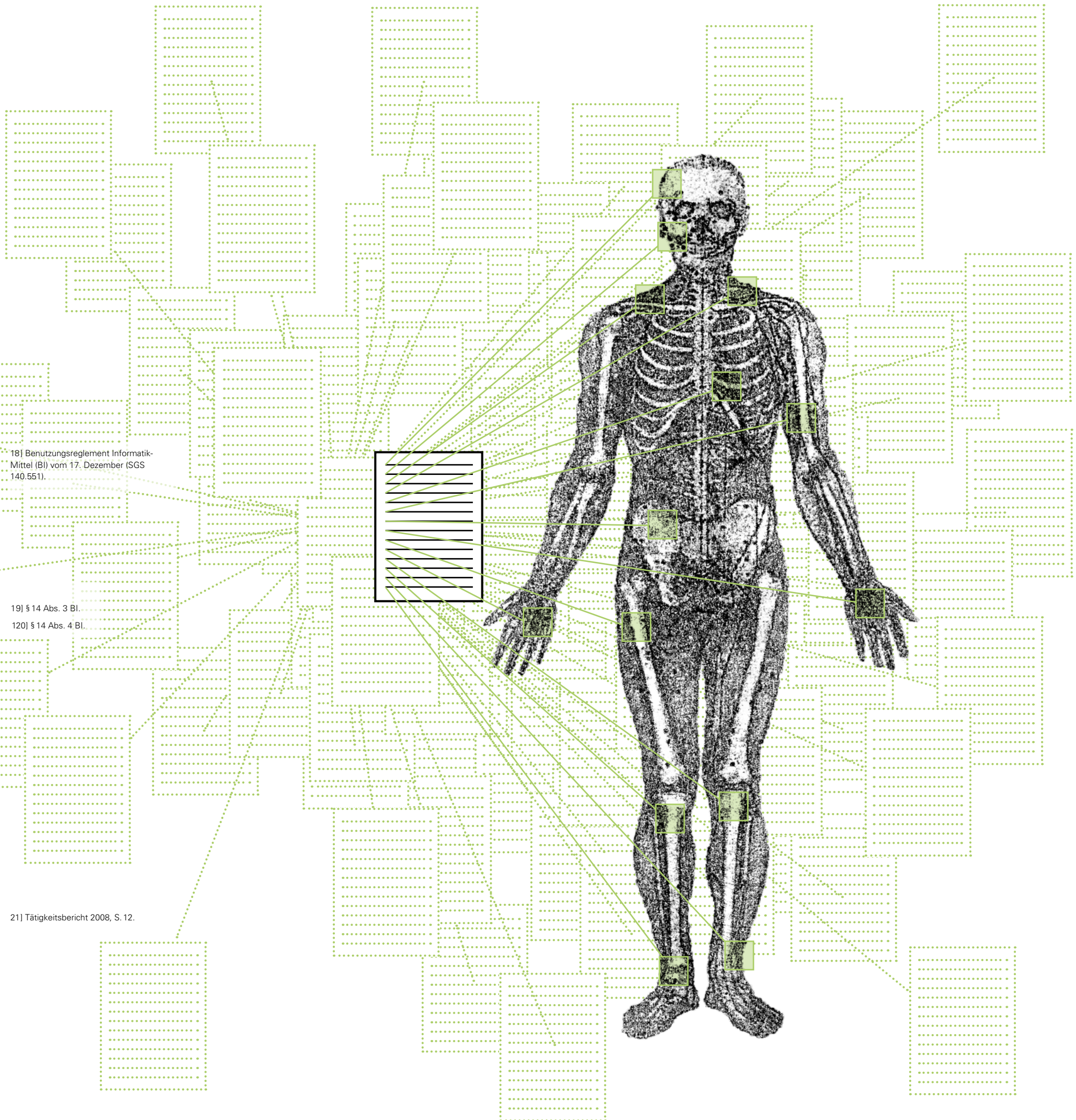
21] Tätigkeitsbericht 2008, S. 12.

VI. KONTROLLTÄTIGKEIT

VI.I. KONTROLLE DES SOG. KANTONALEN STAATSSCHUTZES

Im Tätigkeitsbericht 2008 wurde darauf hingewiesen, dass die Vereinigung der schweizerischen Datenschutzbeauftragten (PRIVATIM) eine koordinierte Kontrolle der kantonalen Staatsschutzaktivitäten initiiert hat.²¹ Als erster Schritt erarbeitete die Arbeitsgruppe innere Sicherheit (AGIS) einen Fragebogen, der den in PRIVATIM organisierten kantonalen Datenschutzbehörden zur Weiternutzung zur Verfügung gestellt wurde. Im Kanton Basel-Landschaft wurde der Fragebogen den zuständigen Polizeibehörden weitergeleitet.

Nach der Auswertung der Antworten fanden weitere Gespräche mit den Polizeibehörden statt. Daraufhin wurde entschieden, dass eine Kontrolle des sog. kantonalen Staatsschutzes durchgeführt werden sollte. Die Aufsichts-



stelle erhielt bei der Durchführung der Kontrolle die uneingeschränkte Unterstützung der zuständigen Mitarbeitenden.

Dennoch blieb letztlich ein Graubereich bestehen, den wir – ohne Verschulden der kantonalen Behörden – nicht kontrollieren durften. Hätten wir nämlich kontrollieren wollen, ob Datenbearbeitungen durch die kantonalen Staatsschutzorgane rechtmässig erfolgt sind (z. B. Löschung unnötiger Daten), wäre aufgrund der geltenden Bundesgesetzgebung eine Zustimmung des DAP (Dienst für Analyse und Prävention) zur Einsicht in die entsprechenden Dossiers notwendig gewesen. Eine Zustimmung wäre aber nur im Einzelfall auf Gesuch hin erteilt oder eben nicht erteilt worden. Ein Umstand, der einer unabhängigen und annähernd repräsentativen Kontrolle entgegensteht.

Konkret bedeutete dies, dass Datenbearbeitungsprozesse, die den DAP involvierten, unkontrolliert bleiben mussten.

In der Folge wurde eine Auswahl von Dossiers des sog. kantonalen Staatsschutzes einer datenschutzrechtlichen Kontrolle unterzogen. Dabei wurden die Dossiers nach formellen (Datensicherheit/Aufbewahrung der Dossiers, Zugriffsberechtigungen sowie Löschung/Archivierung) und materiellen Kriterien (Rechtsgrundlage sowie Verhältnismässigkeit und Erforderlichkeit der Datenbearbeitung) geprüft.

Keines der kontrollierten Dossiers enthielt Daten, die aufgrund des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit (BWIS) erhoben wurden und somit im eigentlichen Sinne staatsschutzrelevant sind. Kontrolliert wurden vielmehr Datenbearbeitungen, die gestützt auf das Polizeigesetz erfolgt waren. Alle von uns geprüften Datenbearbeitungen erfolgten rechtmässig, d. h. gestützt auf eine genügende gesetzliche Grundlage und waren verhältnismässig.

Unsere Feststellungen haben wir der Subkommission 4 der Geschäftsprüfungskommission bekanntgegeben, da sich diese Kommission ebenfalls mit dem Thema Staatsschutzkontrolle beschäftigt. Der Austausch war für uns äusserst wertvoll.

Die Frage, wer die Rechtmässigkeit der Bearbeitung von Staatsschutzdaten in Kantonen kontrollieren soll, ist nach wie vor in Diskussion. Wir hoffen auf eine Lösung, die zwischen der parlamentarischen Kontrolle und der Kontrolle der autonomen kantonalen Datenschutzbehörden unterscheidet und die die föderalistisch geprägte Kompetenzordnung im Bereich Datenschutz mitberücksichtigt.

VII. STELLUNGNAHMEN

Die Aufsichtsstelle nimmt Stellung zu Erlassen, die für den Datenschutz erheblich sind.²² 2009 haben wir im Wesentlichen zu folgenden Themen Stellung genommen:

- Datenbekanntgabe im Rahmen des SuissePol-Index
- Follow-up-Bericht Schengen-Evaluation
- Verordnung über die Videoüberwachung im öffentlichen Verkehr
- Vernehmlassung zum Notenaustausch zwischen der Schweiz und der EU betreffend Übernahme des Rahmenbeschlusses 2008/977/JI
- Entwurf einer Änderung der Verordnung zum Polizeigesetz (Vermissten-suche)
- Stellungnahme zum Entwurf Landratsvorlage «Zentralisierung der Verlustscheinbewirtschaftung» und Revision Steuergesetz
- Vernehmlassungsverfahren des Bundes: Stellungnahme zur Änderung des StGB (Online-Zugriff VOSTRA)
- Vernehmlassung zur Revision des Regierungs- und Verwaltungsorganisationsgesetzes (VwOG) des Bundes betreffend der Nutzung der elektronischen Infrastruktur des Bundes
- Stellungnahme zu §§ 21 und 22 des Entwurfs zum Polizeireglement der Stadt Liestal; Empfehlung gemäss § 25 Abs. 3 DSG
- Vorabkontrolle des Reglements über die Videoüberwachung der Gemeinde Füllinsdorf

22] § 24 Bst. f DSG.

VIII. INFORMATIONSTÄTIGKEIT

VIII.I. MEDIEN

Im vergangenen Jahr hatten wir 16 Medienkontakte und nahmen die Gelegenheit gerne wahr, uns via Radio oder Printmedien zu Fragen des Datenschutzes zu äussern. Es liegt in der Natur der Sache, dass diese Anfragen jeweils recht überraschend kommen und je nach Gegenstand viel Zeit in Anspruch nehmen. Im Berichtsjahr waren die Themen Videoüberwachung und Google Street View Spitzenreiter.

VIII.II. PUBLIKATIONEN

Im Berichtsjahr wurde ein Teil unseres Webauftritts aktualisiert. Im Weiteren haben wir einen Newsletter «Datenschutz.konkret» sowie den Tätigkeitsbericht verfasst und beides im Internet publiziert. Weitere wünschenswerte Publikationen (Merkblätter, Leitfaden, Fachartikel) konnten aus Ressourcengründen nicht erstellt werden.

VIII.III. KURSE UND REFERATE

Im Berichtsjahr haben wir erneut die Polizeiaspirantinnen und -aspiranten über das Datenschutzrecht informieren dürfen und dabei erste Kontakte zu unseren zukünftigen Leistungsempfängern geknüpft. Ferner haben wir wieder die Lernenden des KV (Branchenkunde für kantonale und kommunale Verwaltung) im Datenschutzrecht unterrichten dürfen. Der Austausch mit jungen Menschen, die mit den neuen Technologien gross geworden sind, scheint uns sehr wichtig und gibt uns regelmässig neue Impulse. Ebenfalls wichtig sind die Kurzreferate, die wir anlässlich der Einführungstage für neue Mitarbeitende halten.

Im Weiteren haben wir an einer gut besuchten Informationsveranstaltung des Staatsarchivs teilgenommen und konnten die Anwesenden u. a. über ihre Verantwortung für den Datenschutz aufklären. Auf Einladung der Forschungsgemeinschaft «Mensch im Recht» konnten wir zum Thema Social Networking referieren und schliesslich orientierten wir die in das Projekt «Berufswegbegleitung» involvierten Behördenmitglieder über die datenschutzrechtlichen Rahmenbedingungen.

Im Sinne einer proaktiven Strategie hätten wir gerne mehr Zeit in die Ausbildung und Sensibilisierung gesteckt. Leider war uns dies 2009 aufgrund weiterer Aufgaben nicht möglich.

IX. ZUSAMMENARBEIT NATIONAL UND INTERNATIONAL²³

Interkantonale Institutionen wie etwa die Fachhochschule Nordwestschweiz (FHNW) oder die Universitätskinderklinik beider Basel machen einen Austausch mit anderen Datenschutzbehörden unverzichtbar.

Darüber hinaus können einzelne Datenschutzbehörden das rechtliche und technische Fachwissen nicht für alle Bereiche stets vollumfänglich bereithalten. Dies gilt umso mehr, als

personenbezogene Daten über die Kantons- und Landesgrenzen hinaus ausgetauscht werden. Datenschutzfragen müssen folglich ebenfalls grenzüberschreitend und gemeinschaftlich gelöst werden.

IX.I. ZUSAMMENARBEIT DER KANTONALEN DATENSCHUTZBEHÖRDEN

Im Staatsvertrag über die Fachhochschule Nordwestschweiz (FHNW) fehlen Bestimmungen betreffend die Datenschutzaufsicht. Die Datenschutzbehörden der vier Standortkantone haben daher folgende Abmachung getroffen: Datenschutzfragen von übergeordnetem Interesse, die die ganze FHNW betreffen, werden von der Datenschutzbe-

23] § 24 Bst. i DSG lautet: «Die Aufsichtsstelle arbeitet zur Erfüllung ihrer Aufgaben mit den Datenschutz-Kontrollorganen der Gemeinden, anderer Kantone, des Bundes und des Auslandes zusammen.»

hörde des Kantons Aargau behandelt, da die FHNW dort ihren Sitz hat. Datenschutzfragen, die nur einen Standort betreffen, werden von der entsprechenden Datenschutzbehörde behandelt. Diese Praxis hat sich als praktikabel erwiesen. Eine zur Finanzkontrolle analoge Bestimmung sollte im Rahmen einer nächsten Überarbeitung in den Staatsvertrag aufgenommen werden.

Die Vereinigung der schweizerischen Datenschutzbeauftragten (PRIVATIM) hat sich 2009 mit der Umsetzung der revidierten Datenschutzgesetze beschäftigt und zwei hilfreiche Informationsveranstaltungen durchgeführt. Ferner hat die Vereinigung zur Weiterentwicklung des Schengen-Besitzstandes²⁴ und zum Übereinkommen zum Schutz aller Personen vor dem Verschwindenlassen Stellung²⁵ genommen. Die Aufsichtsstelle hat sich diesen Stellungnahmen gerne angeschlossen.

Die Mitarbeitenden der Aufsichtsstelle arbeiten in den Arbeitsgruppen Innere Sicherheit (AGIS) und Datensicherheit (AG-ICT) von PRIVATIM mit. Diese Gruppen treffen sich in unregelmässigen Abständen und behandeln kantonsübergreifende Fragen wie z. B. die Kontrolle des schweizerischen Staatsschutzes.

24] Übernahme des Rahmenbeschlusses über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden.

25] UN-Erklärung über den Schutz aller Personen vor dem Verschwindenlassen vom 18. Dezember 1992 (Resolution A/RES/47/133 der Generalversammlung).

IX.II. ZUSAMMENARBEIT MIT DEM EIDG. DATENSCHUTZ- UND ÖFFENTLICHKEITSBEAUFTRAGTEN (EDEOB)

Die Durchführung einer koordinierten Aufsicht über den nationalen Teil des Schengener Informationssystems bedingt eine Zusammenarbeit mit dem EDEOB. So ist er für die Kontrolle des Systems und der Bearbeitung der Daten durch Bundesbehörden zuständig. Die kantonalen Datenschutzbehörden sind aufgrund ihrer verfassungsmässigen Kompetenzen und der Organisationsautonomie der Kantone für die Kontrolle ihrer SIS-Nutzungen zuständig. Zur Vorbereitung der Durchführung koordinierter Kontrollen fanden mehrere Sitzungen zwischen dem EDEOB und den kantonalen Datenschutzbehörden statt.

IX.III. GRENZÜBERSCHREITENDE ZUSAMMENARBEIT

Die zunehmende grenzüberschreitende Zusammenarbeit – vor allem in den Bereichen Polizei und Justiz – bedingt auch eine verstärkte grenzüberschreitende Kooperation der zuständigen Datenschutzbehörden. Die Schweiz und damit auch der Kanton Basel-Landschaft haben sich im Rahmen

des grenzüberschreitenden Datentransfers verpflichtet, europäische Datenschutzstandards zu übernehmen, soweit Daten mit dem europäischen Ausland ausgetauscht werden. Dies führt dazu, dass auch europäisches Recht in unser Rechtssystem einfliesst und unsere tägliche Arbeit beeinflusst. Es ist daher wichtig, im Kontakt und Austausch mit Vertretern europäischer Länder zu stehen.

Als föderalistisch organisierter Staat hat die Schweiz die Möglichkeit, mit zwei Datenschutzbehörden in europäischen Arbeitsgruppen vertreten zu sein. Die Schweiz nutzt diese Möglichkeit und ist regelmässig mit einem Vertreter des Bundes und einer kantonalen Datenschutzbehörde vertreten.

IX.III.I. RÜCKTRITT AUS DEN EUROPÄISCHEN ARBEITSGRUPPEN

Die Aufsichtsstelle Datenschutz des Kantons Basel-Landschaft hat in den vergangenen vier Jahren regelmässig an den Sitzungen der Arbeitsgruppe «Polizei und Justiz» der Europäischen Konferenz der Datenschutzbeauftragten teilgenommen.

Sie hat die Entwicklungen innerhalb der Europäischen Union im Bereich Polizei und Justiz, namentlich in Bezug auf die Entwicklung des Schengen-Besitzstandes, in einem frühen Stadium mitverfolgen und Anliegen der Kantone frühzeitig einbringen können. Per Ende 2009 hat sie dieses Mandat an den Kanton Zürich abgetreten.

Ebenfalls im Berichtsjahr hat sich die Aufsichtsstelle von der Teilnehmerliste der sog. Artikel-29-Gruppe der EU streichen lassen. Bisher wurden die

schweizerischen Datenschutzbehörden allerdings noch nie offiziell zu einer Sitzungsteilnahme eingeladen. Sollte sich daran etwas ändern, wird der Kanton Tessin an den Sitzungen teilnehmen.

IX.III.II. CASE HANDLING WORKSHOP

Im Berichtsjahr hat eine Mitarbeiterin der Datenschutzbehörde am europäischen Case Handling Workshop teilgenommen. Der zweimal jährlich stattfindende Workshop bildet das ideale Forum, sich direkt und unkompliziert mit unseren europäischen Kollegen zu aktuellen datenschutzrechtlichen Problemen auszutauschen und gemeinsam Lösungen zu entwickeln. Anlässlich der Frühjahrsveranstaltung wurden diverse Themen wie Massenmedien und Privatsphäre, Videoüberwachung (anhand von konkreten Beispielen im privaten oder öffentlichen Bereich, aber auch die automatische Registrierung von Kontrollschildern), Bearbeitung von Personendaten des Arbeitnehmers sowie die Situation der elektronischen Datenbearbeitung im Gesundheitswesen besprochen.

Die Herbstveranstaltung befasste sich u. a. mit den Themen Internet (insbesondere auch mit der Notwendigkeit der Sensibilisierung von Jugendlichen hinsichtlich der Gefahren beim Gebrauch des Internets), Überwachung am Arbeitsplatz und Recht der Betroffenen auf Einsicht in unterschiedlichste Daten.

X. AUSBLICK

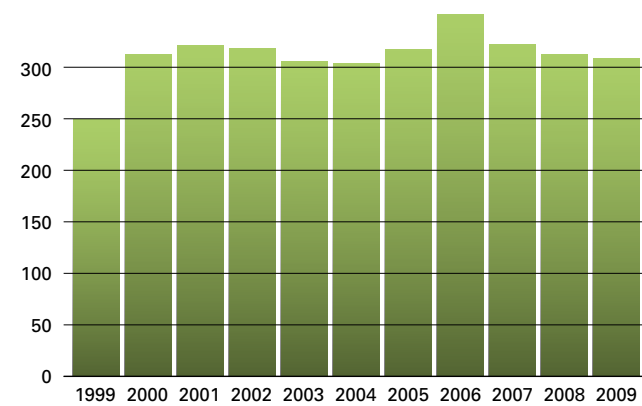
Die Datenschutzbehörde hat viele Aufgaben, die sie mit vergleichsweise bescheidenen Mitteln möglichst effizient erledigen muss. Damit

dies möglich ist, braucht es einerseits einfache interne Abläufe. Andererseits müssen wir aber auch unsere Prioritäten so setzen, dass primär Aufgaben erledigt werden, die einen grossen Wirkungsgrad haben. Dazu gehören Schulung und Information sowie die regelmässigen anlassfreien Kontrollen. In den nächsten Jahren wird es u. a. darum gehen, dass Datenschutzbehörden ihre gesetzlichen Kontrollaufgaben vermehrt wahrnehmen. Die Aufsichtsstelle Datenschutz des Kantons Basel-Landschaft wird sich deshalb als professionelle Kontrollbehörde positionieren müssen. Da Daten zunehmend über die Kantonsgrenzen hinaus ausgetauscht werden, drängt sich eine koordinierte Vorgehensweise mit anderen Datenschutzbehörden auf. Datenschutz ist Persönlichkeitsschutz! Daran wird sich auch in den nächsten Jahren nichts ändern, und der Mensch und seine Grundrechte werden im Zentrum unserer Tätigkeit bleiben.

ANHANG

2009 sind 309 neue Geschäfte eröffnet worden. Wie immer wurden einfache telefonische Anfragen nicht erfasst, da das Erfassen länger dauert, als die Beantwortung selbst. Zudem halten wir unsere Statistik möglichst einfach, damit wir unsere Ressourcen für unsere Kernaufgabe, den Grundrechtsschutz, einsetzen können.

GESCHÄFTE



ART DER GESCHÄFTE

