Vorlage an den Landrat des Kantons Basel-Landschaft

Titel: **Tätigkeitsbericht 2013 der Aufsichtsstelle Datenschutz**

Datum: Juni 2014

Nummer: 2014-040_09

Bemerkungen: **Verlauf dieses Geschäfts**

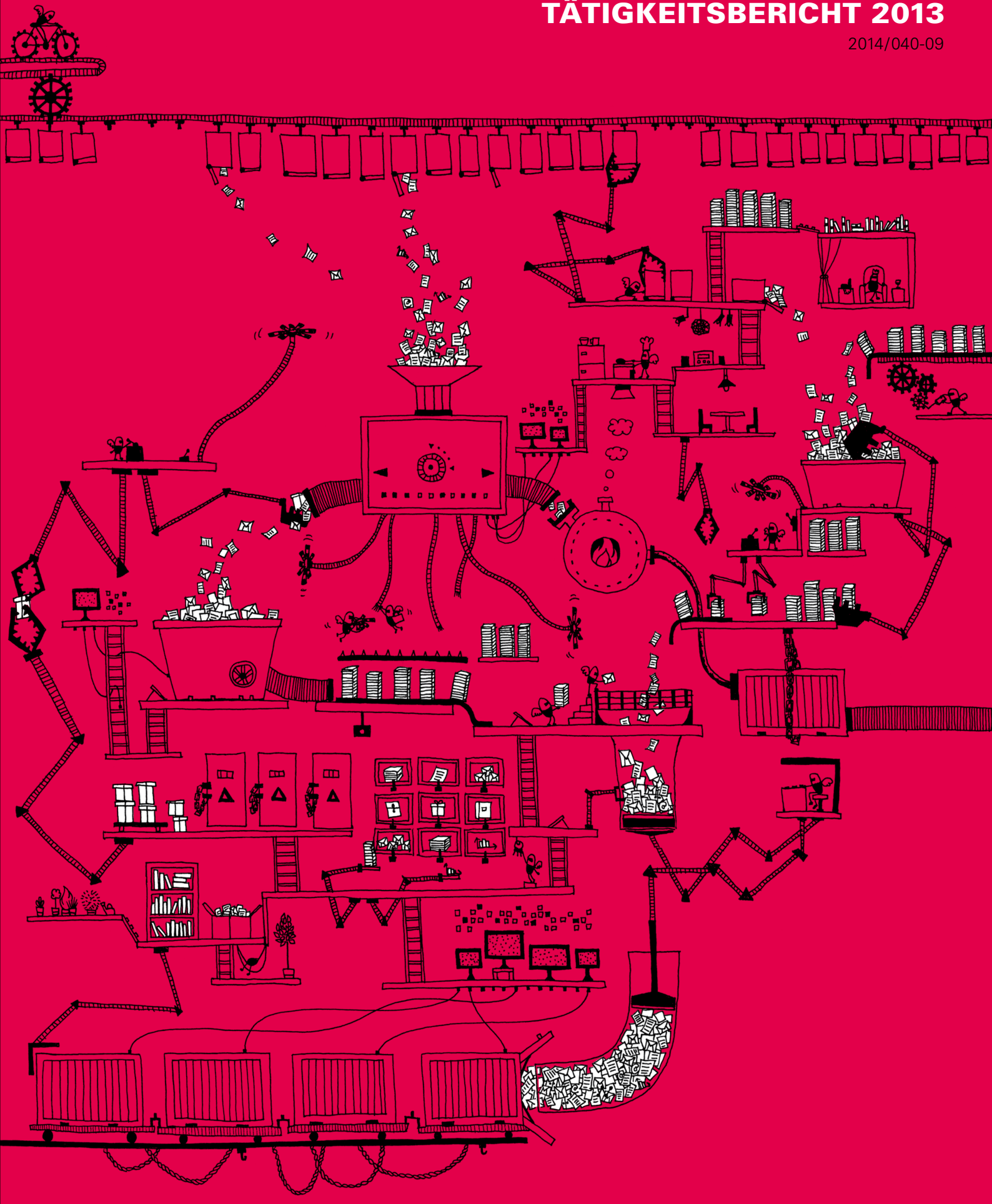
Links:

- 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 2013

2014/040-09



**AUFSICHTSSTELLE DATENSCHUTZ
DES KANTONS BASEL-LANDSCHAFT**

Datenschutzbeauftragte:	Ursula Stucki
Stv. Datenschutzbeauftragter:	Tobias Schnelli
Juristische Mitarbeitende:	Jolanda Peier Vanotti
	Michael Schnyder
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 § 47 Informations- und Datenschutzgesetz erstattet die Datenschutzbeauftragte dem Landrat Bericht über ihre Tätigkeit sowie über wichtige Feststellungen und Beurteilungen.

Gestaltung/Illustration: Neeser & Müller, Basel; Druck: Schaub Medien AG, Liestal

INHALTSVERZEICHNIS

I. DAS JAHR 2013 IN KÜRZE

Datenschutz ist Teil der persönlichen Freiheit, und jedem Mensch steht das Recht auf Privatheit zu. Die Datenschutzbeauftragte und ihr Team haben sich 2013 erneut für dieses liberale Anliegen eingesetzt. Erstmals konnte sie sich auch für das Recht der Bürgerinnen und Bürger auf Zugang zu amtlichen Informationen engagieren. Die Frage, wie die Balance zwischen Informationszugang und Datenschutz gehalten werden kann, war neu und vielschichtig.

Die Datenschutzbeauftragte[1] befasste sich 2013 mit einer Vielfalt an Datenschutzthemen, wie ausgewählte Stichwörter dazu beispielhaft aufzeigen: Amtsgeheimnis, Arbeitnehmerdatenschutz, Autohalter-Auskunft, Big Data, Datensperre, Datenschutz durch Technik, Datenschutz und Schule, Cloud Computing, Client Infrastruktur, E-Learning, E-Health, E-Recruiting, elektronisches Amtsblatt, EU-Datenschutzrecht, GIS, Gebühren, Grundbuchdaten, Informationszugang, Internet, IT-Strategie, IT-Systemgestaltung, Kindes- und Erwachsenenschutz, Kontrolle, Mail, N-SIS, Patientendaten, zentrales Personenregister, Polizeigesetz, Protokollierung von Zugriffen, Recht am eigenen Bild, RIPOL, Teilrevision IDG, SAP/ERP, Schengener Durchführungsübereinkommen, Social Media, Sozialversicherung, Staatsschutz, Steuerpranger, Vereinheitlichung der schweizerischen Datenschutzgesetzgebung, Vertrag zum Universitätskinderspital beider Basel, Videoaufnahmen, Vorabkontrolle sowie offene Zustellung von Zahlungsbefehlen.

Das neue Öffentlichkeitsprinzip führte zu siebzehn Anfragen von Behörden sowie sechs Rechtsberatungen für Private, die Zugang zu amtlichen Informationen einforderten. Das Öffentlichkeitsprinzip im ganzen Kanton Basel-Landschaft umzusetzen und dadurch Transparenz für die Bürgerinnen und Bürger zu schaffen, ohne die Privatsphäre der betroffenen Personen zu verletzen, bleibt eine Herausforderung – auch für die Datenschutzbeauftragte.

Zusätzlich zur Beratung startete die Datenschutzbeauftragte fünf datenschutzrechtliche Kontrollen von öffentlichen Organen und beendete deren vier. Sie prüfte ausserdem über 80 Mitberichte und Vernehmlassungen auf deren datenschutzrechtliche Relevanz und schrieb 14 Stellungnahmen. Ferner beantwortete sie diverse Medienanfragen und Fragen der Politik, schulte Mitarbeitende, hielt Referate und verfasste den Tätigkeitsbericht sowie weitere Publikationen.

Im Bereich Datensicherheit konstatierte die Datenschutzbeauftragte mehrere Sicherheitsbestrebungen für die zahlreichen Informationsbestände des Kantons. Allerdings stellte sie auch im Berichtsjahr fest, dass die Umsetzung der Datensicherheit in der Verwaltung noch deutlich verbessert werden muss. Trotz öffentlicher Debatte über NSA, Datenlecks und Datenklau ist den öffentlichen Organen vielfach wenig bewusst, dass sie über sehr viele Daten verfügen, die es aus finanziellen und rechtlichen Gründen zu schützen gilt.

Im Rahmen der parlamentarischen Oberaufsicht der landrätlichen Geschäftsprüfungskommission wurde die Datenschutzbeauftragte im Herbst von der Subkommission 4 zu ihrer Arbeitsweise befragt. Sie informierte die Subkommission über aktuelle Fragestellungen und orientierte sie über ihr immer breiteres und komplexeres Aufgabengebiet und das entsprechend gestiegene Arbeitsvolumen.

Weil die Datenschutzbeauftragte ihr immer grösseres Aufgabengebiet mit den zur Verfügung gestellten Mitteln nachweislich nicht mehr erfüllen konnte, beantragte sie dem Landrat zusätzliche Mittel. Das Parlament genehmigte 2013 die Erhöhung des Sollstellenplans von drei auf vier Stellen. Dies ermöglicht es der Datenschutzbeauftragten und ihrem Team, beispielsweise weiterhin Anfragen von Privaten und Behörden zu beantworten. Zudem kann sie das erforderliche IT-Know-how intern aufbauen, um IT-Kontrollen teilweise selber durchzuführen und Behörden bei Fragen zum technischen Datenschutz bedarfsgerecht zu beraten. Die Weiterentwicklung des Teams zu einer kleinen interdisziplinären Organisationseinheit ist eine Herausforderung, der sich die Datenschutzbeauftragte gerne stellt. Sie tut dies mit Blick auf die Rechte der Bürgerinnen und Bürger, in deren Interesse sie ihr Mandat letztlich erfüllt.

1] Der Begriff «Datenschutzbeauftragte» bezeichnet sowohl die Behörde als auch die Funktion.

II. THEMEN 2013

II.I. DAS ÖFFENTLICHKEITSPRINZIP

Im Berichtsjahr behandelte die Datenschutzbeauftragte 23 Anfragen zum Öffentlichkeitsprinzip, was rund 10% aller Anfragen entsprach. 17 dieser Anfragen stammten von Behörden und beinhalteten hauptsächlich die Offenlegung von Protokollen und Kommissionsberichten. Die Datenschutzbeauftragte klärte zudem Fragen zu den Spesen des Landrats, ein Gesuch eines Politikers um Einsicht in ein Strafgerichtsurteil und Fragen im Zusammenhang mit Landerwerbspreisen. Die sechs Privatpersonen, die sich zum Öffentlichkeitsprinzip an die Datenschutzbeauftragte wandten, was 10% der Privatanfragen entsprach, erwarteten teils von ihr die Anweisung der Behörden, ihnen den Informationszugang pauschal zu gewähren. Derart weitgehende Kompetenzen stehen der Datenschutzbeauftragten berechtigterweise nicht zu. Bei den für alle Beteiligten neuartigen Fragen zum Öffentlichkeitsprinzip musste die Datenschutzbeauftragte die Grenzen im Gespräch mit den Ratsuchenden und unter Beizug der Rechtsprechung des Bundes und anderer Kantone ausloten. Eine Praxis zum Öffentlichkeitsprinzip, wie sie im Datenschutzrecht seit Jahren existiert, muss sich im Kanton Basel-Landschaft und in den Gemeinden erst noch etablieren.

Die Datenschutzbeauftragte stellte fest, dass im Alltag noch keine direktionsübergreifende Koordination besteht. Zwar tauschen sich die Generalsekretäre anlässlich ihrer ordentlichen Sitzungen über die Gesuche aus, es fehlt jedoch eine Projektorganisation, die u. a. eine einheitliche und speditive Erledigung der Gesuche sowie einen regelmässigen fachlichen Austausch der von den Direktionen nominierten Verantwortlichen[2] zum Ziel hat. Die Datenschutzbeauftragte wird sich dafür einsetzen, dass die Direktionen, die für die Umsetzung des IDG verantwortlich sind, koordiniert eine einheitliche Praxis erarbeiten. Aufgrund erster Erfahrungen der Verwaltung sollen zudem Prozesse definiert werden, mit denen Gesuche innert der gesetzlichen Frist (30 Tage) behandelt und Reklamationen wegen nicht eingehaltener Fristen vermieden werden können. Die Datenschutzbeauftragte wird die Verantwortlichen gerne bei den anstehenden Umsetzungsarbeiten unterstützen.

2] § 13 Abs. 3 IDG: Die Direktionen der kantonalen Verwaltung und die Landeskanzlei bezeichnen je eine Stelle, die mit der Umsetzung des Öffentlichkeitsprinzips in der Direktion respektive in der Landeskanzlei betraut ist.

II.II. DATENSCHUTZ UND DATENSICHERHEIT IN DER VERWALTUNG

Obwohl die Medien 2013 Datenschutzthemen wie die Überwachung durch die NSA, den Verkauf von Steuerdaten oder die Datensammlungen von Google und Facebook breit aufgriffen, wurde nur am Rande erwähnt, dass auch der Staat immer mehr Daten seiner Bürgerinnen und Bürger sammelt und sie zunehmend zentral und mit immer komplexeren Systemen bearbeitet. Die Vertraulichkeit auch dieser Daten kann durch höhere Gewalt, organisatorische Mängel, menschliches Fehlverhalten und technisches Versagen gefährdet sein.

Die zunehmende Zentralisierung der Datenbestände - und damit verbunden der elektronische Abruf der Daten nach dem Selbstbedienungsprinzip - ist ein weiteres Risiko für die Datensicherheit. Die Datenabfrage wird dadurch zwar immer effizienter, die bekanntgebende Stelle kann jedoch kaum mehr prüfen, ob die rechtlichen Voraussetzungen für die elektronischen Abfragen gegeben sind. Im Gegensatz zu Papierakten: Wer regelmässig Papierakten aus den Büros eines öffentlichen Organs mitnehmen möchte, muss dies begründen können. Um auch bei elektronischen Datenbeständen den Datenschutz und die Datensicherheit zu gewährleisten, müssen die öffentlichen Organe bei geplanten Datenbearbeitungsprozessen u. a. die Zugriffsrechte gesetzeskonform definieren, den Schutzbedarf regelmässig risikobasiert prüfen, die Systeme und Anwendungen inventarisieren und die Anwendungsverantwortlichkeit klären. Dies mag aufwendig erscheinen. Wer jedoch verhindern möchte, dass weitgehend unbemerkt in IT-Systeme eingedrungen wird und grosse Datenmengen kopieren oder verändern werden, sollte die Fragen der Datensicherheit in IT-Projekten trotz des damit verbundene Aufwandes nicht vernachlässigen.

Die Datenschutzbeauftragte stellte im Berichtsjahr bei zahlreichen IT-Projekten fest, dass die datenschutzrechtlichen Vorgaben des Kantons[3] teilweise vernachlässigt wurden: In einigen Projekten fehlten die für die Datensicherheit erforderlichen Fragen und Prüfschritte, andere Projekte enthielten unvollständige Prozesse oder Mängel im Systemmanagement. Auch im Beschaffungswesen wurde die IT-Sicherheit vernachlässigt: Die Datenschutzbeauftragte stiess auf angeschaffte Applikationen, die nicht dem Stand der Technik entsprachen und Vorgaben der IT-Sicherheit stark vernachlässigten.

Mit Sorge beobachtete die Datenschutzbeauftragte zudem den Trend im IT-Bereich, immer mehr IT-Aufgaben an externe Anbieter zu vergeben. Wenn öffentliche Organe darauf verzichten, das erforderliche Know-how intern aufzubauen vergrössert sich ihr Risiko, langfristig von einem einzelnen Anbieter abhängig zu werden.

Die Datenschutzbeauftragte initiierte im Berichtsjahr einen Kurzleitfaden für die Behörden zur Gestaltung der Systeme und Zugriffsberechtigungen. Im Rahmen der ersten Vernehmlassung äusserten sich die operativen Sicherheitsfachleute positiv dazu. Doch die Entscheidungsträger bewerteten den Stellenwert der Datensicherheit und damit auch des Datenschutzes anders: Zwar betrachten sie Datensicherheit grundsätzlich als erforderlich, in der Stellungnahme fehlte jedoch ein klares Bekenntnis, die dazu erforderlichen Massnahmen umzusetzen und entsprechende Mittel einzusetzen.

Trotz der Anstrengungen des Kantons in den Bereichen Datenschutz und Datensicherheit in den vergangenen Jahren und entgegen seiner IT-Strategie stellte die Datenschutzbeauftragte fest, dass zahlreiche Behörden die geltenden Vorgaben nicht oder nur marginal kannten. Zudem beobachtete sie, dass die IT-Sicherheitsfachleute zwar entsprechend ausgebildet und sensibilisiert sind, dass sie ihre aufwändigen Aufgaben aber mangels Ressourcen kaum erfüllen konnten. Die Datenschutzbeauftragte stellt somit weiteren Handlungsbedarf des Kantons für eine flächendeckende Umsetzung seiner IT-Strategie fest.

3] IT-Strategie des Kantons Basel-Landschaft, S. 13; § 11 der Verordnung über das Projektmanagement (SGS 140.15) sowie § 16 Datenschutzfreundliche Technologien
[1] Bei der Beschaffung von Informatikmitteln zur Verwaltung von Personendaten ist die Datenschutzfreundlichkeit der Technologien angemessen zu berücksichtigen.
[2] Bevor Informatik mittel zu diesem Zweck beschafft werden, ist die zuständige Datenschutzbehörde anzuhören.

II.III. FORMELLES UND MATERIELLES DATENSCHUTZRECHT

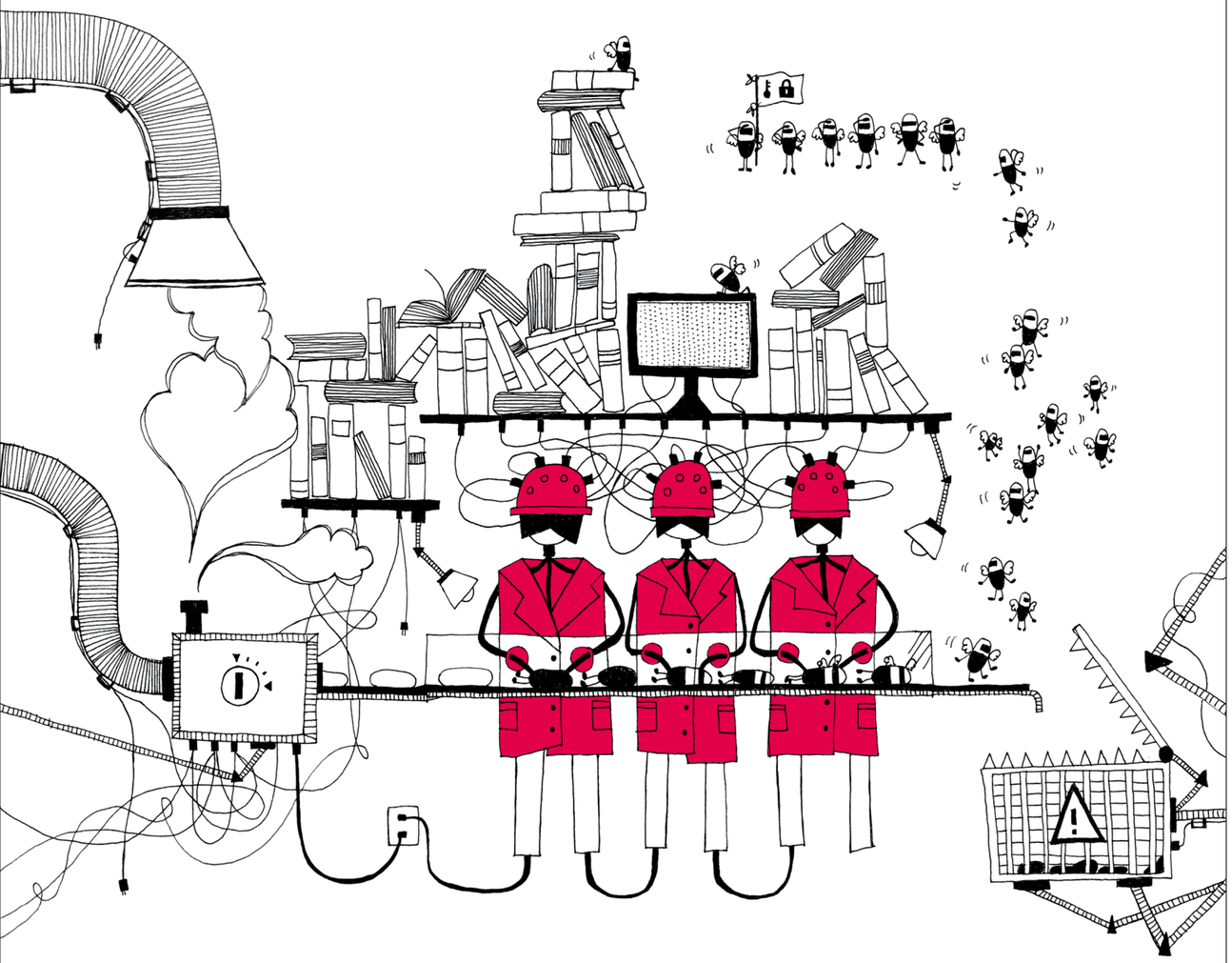
Datenschutzrecht findet sich einerseits in den Datenschutzgesetzen (sog. formelles Datenschutzrecht), andererseits – als materielles Datenschutzrecht – im jeweiligen Fach- und Sachrecht: Die formellen Datenschutzgesetze regeln die Grundprinzipien des Datenschutzes, die Rechte der Betroffenen sowie Stellung und Aufgaben der Datenschutzbehörden. Das materielle Datenschutzrecht beinhaltet die konkreten Regeln der Datenbearbeitung, die sich im jeweiligen Fach- oder Sachrecht finden lassen (z. B. wer welche Daten wie und zu welchem Zweck bearbeiten darf).

Im Kanton Basel-Landschaft findet sich materielles Datenschutzrecht und die entsprechenden Regeln der Datenbearbeitung z. B. im Bildungsrecht, im Steuerrecht oder in den Reglementen zur Videoüberwachung der Gemeinden. Es findet sich aber auch in Bundesgesetzen, z. B. im Bundesgesetz über die Invalidenversicherung, das auch den Datenaustausch unter den involvierten Stellen regelt. Das materielle Datenschutzrecht des Bundes muss von den kantonalen Behörden bei der Umsetzung von Bundesrecht zwar beachtet werden. Die Behörde untersteht deshalb aber nicht der Datenschutzbehörde des Bundes: Die Zuständigkeit der schweizerischen Datenschutzbehörden richtet sich einzig nach dem datenbearbeitenden Organ (Bund, Kanton oder Gemeinde). Wenn eine kantonale Behörde Bundesrecht vollzieht, untersteht sie somit der kantonalen Datenschutzaufsicht.

Die Datenschutzbeauftragte stellte im Berichtsjahr mehrfach fest, dass nicht allen Involvierten die rechtlichen Zuständigkeiten bekannt waren. Dies illustrieren folgende Beispiele:

II.III.a VERTRAG ZUM UNIVERSITÄTSKINDERSPITAL BEIDER BASEL

Die beiden Basel revidierten den Vertrag zum Universitätskinderspital beider Basel (Kinderspitalvertrag) im Herbst 2013. Der Vertragsentwurf wurde den Datenschutzbeauftragten der Kantone Basel-Stadt und Basel-Landschaft zur Stellungnahme unterbreitet.



Diese empfahlen, die Zuständigkeit für den Bereich Datenschutz vertraglich zu regeln und schlugen dazu folgenden Satz vor: «Für den Umgang mit Informationen gilt das Informations- und Datenschutzrecht des Sitzkantons». Die Datenschutzbeauftragte musste darauf der Vorlage an den Landrat entnehmen, dass die Regierungen auf diese Regelung verzichtet hatten und darauf verwiesen, dass im Gesundheitswesen vorrangig übergeordnete Datenschutzbestimmungen aus dem Bundesrecht gelten würden.[4] Die Regierungen verkannten somit die vom Föderalismus geprägten Zuständigkeitsregeln im Datenschutzrecht und verzichteten, ohne Rückfrage bei den beiden Datenschutzbeauftragten, auf eine kurze aber klärende Regelung im Staatsvertrag.

Für die Patientinnen und Patienten der beiden Trägerkantone bedeutet der Verzicht auf eine interkantonale Regelung im Staatsvertrag, dass sie je nach Herkunftsort entweder dem einen oder dem anderen Datenschutzgesetz unterstehen. Wenn zum Beispiel eine Mutter aus dem Baselbiet in der Basler Frauenklinik entbunden hat und ihr Kind anschliessend im benachbarten Kinderspital behandelt wird, gilt gemäss Spitalvertrag für die Mutter das Datenschutzgesetz des Kantons Basel-Stadt, für das Kind das Datenschutzgesetz des Kantons Basel-Landschaft. Auch für die Organisation wird es weiterhin zwei Aufsichtsbehörden geben. Je nach Fragestellung muss eine behandelnde Person zunächst klären, woher eine Patientin oder ein Patient stammt, um sich an die zuständige Datenschutzbehörde richten zu können.

Obwohl das rechtliche Verwirrspiel durch den Staatsvertrag mit dem einen vorgeschlagenen Satz der beiden Datenschutzbeauftragten hätte abgewendet werden können, liegt es nun weiterhin an den beiden Datenschutzbehörden, in jedem Einzelfall gemeinsam praktikable Lösungen zu erarbeiten.

4] Vorlage 2013-020. S. 7: *«Die Regierungen der Trägerkantone lehnen die Aufnahme einer solchen Bestimmung ab, da im Gesundheitswesen vorrangig übergeordnete Datenschutzbestimmungen aus dem Bundesrecht gelten (Sozialversicherungsrecht, Datenschutzgesetz, Krankenversicherungsgesetz, Gesetz über den Versicherungsvertrag)»*

II.III.b E-LEARNING-TOOL DATENSCHUTZ

Im Berichtsjahr setzte der Kanton zur Schulung der Mitarbeitenden ein E-Learning-Tool für IT-Sicherheit und Datenschutz ein. Die Inhalte zu IT-Sicherheit und Datenschutz wurden bei derselben externen Firma eingekauft, die auch das Tool lieferte. Der Inhalt zum Datenschutz wurde nachträglich der Datenschutzbeauftragten zur Stellungnahme unterbreitet. Sie stellte fest, dass das E-Learning-Tool auf dem Datenschutzgesetz des Bundes basierte, das im Kanton praktisch nicht angewendet wird. Die Datenschutzbeauftragte musste deshalb den gesamten Inhalt umschreiben und an die kantonalen Bedingungen anpassen. Sie nahm dies gleich zum Anlass, auch die Sicherheitsverantwortlichen im Datenschutzrecht zu schulen.

II.IV. STELLUNG DER DATENSCHUTZ-BEHÖRDE

Die unabhängige Datenschutzbehörde ist im staatlichen Gefüge ein Sonderfall: Sie ist weder ein Verfassungsorgan wie der Ombudsman, noch ein parlamentarisches Fachorgan wie die Finanzkontrolle. Ihre Unabhängigkeit hat ihren rechtlichen Ursprung im internationalen Recht: Da sich die Schweiz am internationalen Datenaustausch beteiligt, muss sie gewissen völkerrechtlichen Anforderungen gerecht werden[5]. So wird u. a. verlangt, dass die Einhaltung der innerstaatlichen datenschutzrechtlichen Vorgaben von Aufsichtsbehörden überwacht wird, die ihre Aufgabe in «völliger» Unabhängigkeit wahrnehmen[6].

Der Kanton Basel-Landschaft hat am 1. Juli 2008 das geforderte Kontrollorgan eingeführt[7]. Die Rechtsnormen des damaligen Datenschutzgesetzes wurden 2013 unverändert ins IDG übernommen. Somit führt der Kanton eine unabhängige Aufsichtsstelle[8], die ihre Aufgabe weisungsunabhängig erfüllt[9]. Die Datenschutzbeauftragte untersteht selbstverständlich der parlamentarischen Oberaufsicht[10] und ist verpflichtet, dem Wahlorgan sowie der Öffentlichkeit periodisch über ihre Tätigkeit und ihre Feststellungen zu berichten[11].

Die von Gesetzgebern in Bund und Kanton eingesetzten unabhängigen Datenschutzbehörden beraten Private und Behörden und kontrollieren die Datenbearbeiter. Sie stellen sicher, dass die grundrechtlichen Interessen der Bürgerinnen und Bürger im Gesetzgebungsverfahren oder bei der Schaffung neuer Datenbearbeitungsprozesse angemessen berücksichtigt werden. Für diese Aufgaben benötigen die Datenschutzbehörden Personal mit fundierten Kenntnissen im

5] Im Bereich Datenschutz stehen dabei das Zusatzprotokoll zur Datenschutzkonvention des Europarats (DSK, SR 0.235.11), die EG-Datenschutzrichtlinie (RL 95/46) und das Schengener Durchführungsübereinkommen (SDÜ, SR 0.362.31) im Vordergrund.

6] Art. 1 DSK und Art. 28 RL 95/46

7] GS 36.709

8] § 35 Abs. 1 IDG

9] § 36 Abs. 1 IDG

10] § 36 IDG

11] § 47 IDG

Datenschutzrecht und – aufgrund der technikgestützten Datenbearbeitungen – auch in den Bereichen Informatik und Revision.

Die Datenschutzbeauftragte des Kantons Basel-Landschaft verfügte im Berichtsjahr über einen Sollstellenplan von drei Stellen, die sich vier Personen teilen. In den ersten sieben Monaten beschäftigte sie zudem ein Volontariat. In der zweiten Jahreshälfte musste darauf verzichtet werden, weil das Geschäftsvolumen keine Zeit mehr für die Betreuung eines Volontariats zuliess.

Die Datenschutzbeauftragte beantragte 2013 zum zweiten Mal in Folge und mit der gleichen Begründung eine Erhöhung des Sollstellenplans von drei auf vier Stellen, weil weiterhin eine Fachperson im Bereich Revision und IT-Sicherheit fehlte. Doch auch im Bereich Recht bestand dringender Bedarf an zusätzlichen Ressourcen, weil sowohl das neu eingeführte Recht auf Informationszugang als auch die grössere Komplexität der Datenschutzfragen das Arbeitsvolumen deutlich vergrösserten (vgl. II.I.). Ein Budgetpostulat gegen den Antrag der Datenschutzbeauftragten wurde am 12. Dezember 2013 knapp abgelehnt, so dass sie die zusätzliche Stelle mit zwei Teilzeitmitarbeitenden besetzen kann.

Dass die Aufgaben einer Kontrollbehörde, die sich für den Datenschutz und den Informationszugang der Bürgerinnen und Bürger einsetzt, nicht ganz den derzeit im Vordergrund stehenden finanziellen Interessen untergeordnet wurden, motiviert und verpflichtet die Datenschutzbeauftragte, ihre gesetzlichen Aufgaben weiterhin engagiert zu erfüllen.

III. FÄLLE AUS DEM BERATUNGS-ALLTAG

2013 führte die Datenschutzbeauftragte 242 Beratungen durch. Zusätzlich beantwortete sie viele kurze telefonische Anfragen. Weil das Erfassen dieser kurzen Telefonanfragen in der Geschäftskontrolle länger dauern würde als deren Beantwortung, wurden sie nicht erfasst. Rund drei Viertel der erfassten Beratungen stammten von Behörden, ein Viertel von Privaten. Etwas mehr als jede zehnte Anfrage betraf nur das Öffentlichkeitsprinzip. Alle weiteren Anfragen betrafen den Datenschutz oder beide Gebiete. Die im Folgenden beschriebenen einfachen Fälle sind typisch für den Beratungsalltag der Datenschutzbeauftragten.

III.I. ELTERN NEHMEN ELTERNGESPRÄCH MIT SMARTPHONE AUF

Eine Lehrperson wandte sich an die Datenschutzbeauftragte, weil Eltern das Elterngespräch aufgenommen hatten. Die Lehrerin hatte die Eltern nach diesem Gespräch schriftlich gebeten, die Aufnahme nicht an Dritte weiterzugeben. Von den Eltern erhielt sie jedoch keine Bestätigung, sondern lediglich den Hinweis, man habe ihre Bitte zur Kenntnis genommen.

Unbefugtes Aufnehmen von Gesprächen ist ein Antragsdelikt, das mit Freiheitsstrafe bis zu einem Jahr oder einer Geldstrafe bestraft wird[12]. In Rücksprache mit der Bildungs-, Kultur und Sportdirektion (BKSD) empfahl die Datenschutzbeauftragte der Lehrperson, den Sachverhalt der Schulleitung zu unterbreiten, damit diese die erforderlichen Schritte zum Schutz der Lehrperson ergreifen konnte. Für die weitere rechtliche Unterstützung der Schulleitung stand der Rechtsdienst der BKSD zu Verfügung.

12] Art. 179ter des Schweizerischen Strafgesetzbuchs (StGB)

III.II. PUBLIKATION VON EINWOHNER-DATEN IM GEMEINDEBLATT

Eine Gemeinde fragte die Datenschutzbeauftragte, ob sie Zu- und Wegzug sowie runde Geburtstage im Gemeindeblatt veröffentlichen dürfe. Die Datenschutzbeauftragte wies die Gemeinde darauf hin, dass die Veröffentlichung dieser Angaben zur Erfüllung ihrer gesetzlichen Aufgabe kaum erforderlich sei. Mit dem Einverständnis der betroffenen Personen sei eine Publikation jedoch möglich.

III.III. PERSÖNLICH-KEITSTEST UN-VERSCHLÜSSELT GEMAILT

Eine Person bewarb sich um eine Stelle beim Kanton Basel-Landschaft. Im Rahmen der Rekrutierung wurde ein Persönlichkeitstest durchgeführt. Die Testresultate wurden dem potenziellen Vorgesetzten unverschlüsselt via Mail zugestellt. Aufgrund der Einstellungen im Mailprogramm erhielten auch Drittpersonen Kenntnis von diesem Persönlichkeitstest und sprachen die bewerbende Person darauf an. Die Datenschutzbeauftragte stellte einmal mehr fest, dass trotz ihrer zahlreichen Hinweise noch immer Vertrauliches unverschlüsselt per Mail verschickt wird. Auf Wunsch der betroffenen Person hat die Datenschutzbeauftragte darauf verzichtet, bei der Behörde direkt zu intervenieren.

III.IV. ZUGANG ZU INFORMATIONEN

Die Einführung des Öffentlichkeitsprinzips im Berichtsjahr führte zu diversen Anfragen bei der Datenschutzbeauftragten (vgl. I.II.). Die Behörden waren vor allem verunsichert, wie das generelle Recht auf Zugang zu Informationen umzusetzen sei. Neu mussten drei Arten der Akteneinsicht unterschieden werden. Zugang zu Informationen im Allgemeinen, Akteneinsicht nach Verfahrensrecht oder Einsicht in die eigenen Personendaten. Die Datenschutzbeauftragte machte die Behörden im Einzelfall darauf aufmerksam, dass die Einsicht in die eigenen Personendaten bereits im alten Datenschutzgesetz geregelt war und nach wie vor kostenlos gewährt werden müsse. Zudem informierte sie, dass in laufenden Verfahren der Rechtspflege nicht das IDG, sondern das Verfahrensrecht anwendbar sei. Für Zugangsgesuche gemäss Öffent-

lichkeitsprinzip verwies die Datenschutzbeauftragte die Behörden auf ihren Leitfaden und ihre Merkblätter. Sie wies wiederholt darauf hin, dass das Öffentlichkeitsprinzip nichts am Datenschutzrecht und am Recht der Einzelnen auf Privatheit geändert habe.

III.V. ÖFFENTLICHKEITSPRINZIP BEI SCHULRATSPROTOKOLLEN

Ein Schulrat fragte die Datenschutzbeauftragte an, ob mit dem Öffentlichkeitsprinzip die Schulratsprotokolle nun öffentlich einsehbar und zugänglich sein müssen, und ob dies gegebenenfalls eine Hol- oder eine Bringschuld sei.

Schulratsprotokolle fallen unter das Öffentlichkeitsprinzip. Jede Person kann ein Gesuch stellen und Zugang zu den Protokollen verlangen. Der Schulrat muss jeweils im Einzelfall beurteilen, ob es überwiegende öffentliche oder private Gründe gibt, die gegen eine Offenlegung eines Protokolls sprechen. Kommt der Schulrat zum Schluss, dass ein Protokoll offengelegt werden kann, muss er die Personendaten im Protokoll anonymisieren und der gesuchstellenden Person den Zugang innert 30 Tage gewähren. Kommt er zum Schluss, ein Protokoll könne nicht offengelegt werden, muss er dies der gesuchstellenden Person ebenfalls innert 30 Tagen mitteilen und sie informieren, dass sie eine anfechtbare Verfügung verlangen könne.

Die Datenschutzbeauftragte verwies diese und andere Schulbehörden auf ihren Leitfaden zum IDG, der dieses Vorgehen erläutert[13]. Sie stellte indessen fest, dass die Umsetzung für Milizbehörden noch sehr anspruchsvoll ist.

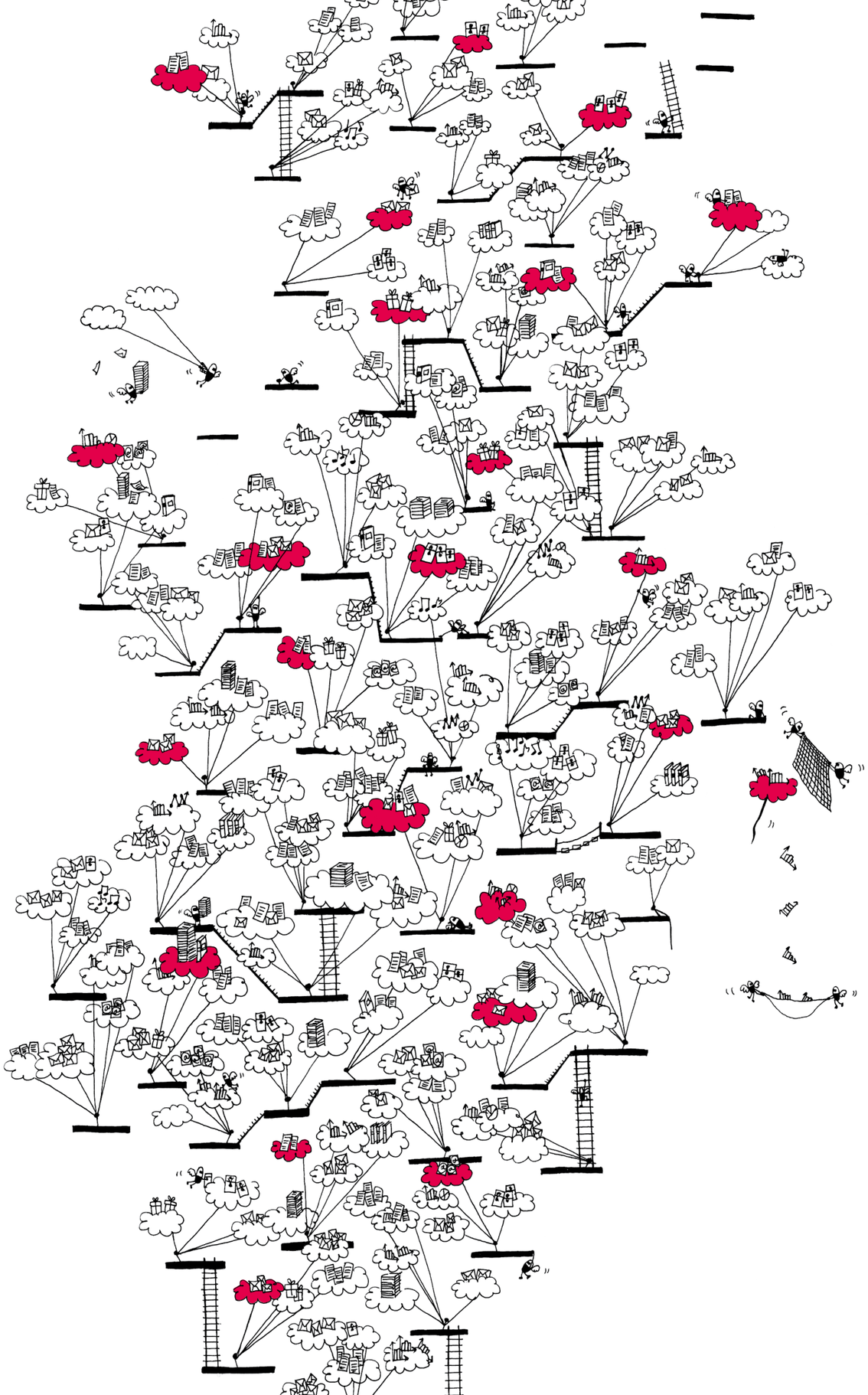
13] www.baselland.ch/fileadmin/baselland/files/docs/jpd/ds/daten/anhang-1_pruefungsschema.pdf

III.VI. LEBENSLAUFVORLAGE NICHT VOLLSTÄNDIG ANONYMISIERT

Eine Person meldete sich bei der Datenschutzbeauftragten, weil ihr ein Regionales Arbeitsvermittlungszentrum (RAV) einen nur unvollständig anonymisierten Lebenslauf einer anderen Person als Vorlage ausgehändigt hatte. Die Datenschutzbeauftragte forderte die Verantwortlichen des RAV auf, mit den Daten von Stellenlosen sorgfältig umzugehen und deren Persönlichkeitsrechte zu respektieren.

III.VII. HANDSCHRIFTLICHE NOTIZEN

Die Datenschutzbeauftragte wurde auch im Berichtsjahr gefragt, ob Handnotizen zu den Akten gehören und ob man diese bei einem entsprechenden Gesuch offenlegen müsse. Die Datenschutzbeauftragte wies darauf hin, dass nicht die Form, sondern der Inhalt einer Notiz entscheidend sei. Auch handschriftliche Notizen können relevante Inhalte haben und für die Entscheidfindung wichtig sein. Die Tatsache, dass etwas von Hand geschrieben wurde, schliesst den Zugang zu Informationen somit nicht aus.



IV. KONTROLL-TÄTIGKEIT

Zum gesetzlichen Auftrag der Datenschutzbeauftragten gehören Kontrollen bei öffentlichen Organen des Kantons und der Gemeinden. Bei diesen Kontrollen prüft die Datenschutzbeauftragte, ob sich die öffentlichen Organe an das IDG halten. Gemäss ihrer Erfahrung führen ihre angekündigten Kontrollen bei den Behörden auch dazu, dass diese sich im Vorfeld mit dem Thema beschäftigen und selbst Mängel erkennen und beheben lassen. Im Berichtsjahr hat die Datenschutzbeauftragte fünf Kontrollen begonnen und vier beendet:

IV.I. NUTZUNG DES SCHENGENER INFORMATIONS-SYSTEMS

Die Datenschutzbeauftragte schloss im Berichtsjahr die Kontrolle bei der Polizei Basel-Landschaft zur Nutzung des Abrufverfahrens des Schengener Informationssystems (SIS) ab. Die Datenschutzbeauftragte wertete die von den Angestellten der Polizei angegebenen Gründe für deren Abfragen im SIS aus. Der Schlussbericht wird im Januar 2014 erstellt werden[14].

14] Vgl. Tätigkeitsbericht 2012

Die Auswertung der Datenschutzbeauftragten zu den Gründen der SIS-Abfragen führte zu einer rechtlichen Diskussion mit der Polizei Basel-Landschaft, dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDOEB) und dem Bundesamt für Polizei (Fedpol), wie Art. 15 resp. 16 des Bundesgesetzes über die polizeilichen Informationssysteme des Bundes (BPI) auszulegen seien. Diese Bestimmungen regeln im polizeilichen Bereich, zu welchen Zwecken auf die beiden technisch verbundenen Systeme von Ripol (automatisiertes Polizeifahndungssystem) und N-SIS (Nationaler Teil des SIS) zugegriffen werden darf. Polizei, EDOEB und Fedpol stellten sich auf den Standpunkt, dass Abfragen durch zugangsberechtigte Angestellte der Polizei zu Zwecken, die mit der Polizeiarbeit im Zusammenhang stehen, grundsätzlich rechtmässig sind. Sie begründeten dies mit allgemeinen Grundsätzen der Polizeiarbeit, der Strafprozessordnung, des kantonalen Polizeigesetzes sowie anhand von internationalen Verträgen. Nicht berücksichtigt wurde von ihnen Art. 16 BPI zum N-SIS sowie die in Art. 15 BPI zum Ripol gesetzlich verankerten Abfragegründe. Gemäss Botschaft des Bundesrates zum Bundesgesetz über die polizeilichen Informationssysteme des Bundes regelt indessen das BPI «für jedes Informationssystem die Art der Daten und den Zweck, zu dem sie bearbeitet werden dürfen» (BBL 2006 5069). Die Datenschutzbeauftragte wertet dies als klares Zeichen dafür, dass die Abfragegründe von Art. 15 und 16 BPI bei der Beurteilung der Frage der Rechtmässigkeit der Abfragen heranzuziehen sind. Weder die Polizei, noch der EDOEB, noch Fedpol konnten rechtlich darlegen, weshalb von den im BPI aufgelisteten Abfragegründen, die § 95 des Schengener Durchführungsabkommen entsprechen, abzuweichen ist. Die Datenschutzbeauftragte machte sie darauf aufmerksam, dass die heutige Praxis einer richterlichen Überprüfung allenfalls nicht standhalten würde. Aufgrund der internationalen Vorgaben regte die Datenschutzbeauftragte an, dass die Frage der Anwendbarkeit des BPI nicht kantonal, sondern gesamtschweizerisch angegangen werden sollte. Der EDOEB, als Präsident der N-SIS-Koordinationsgruppe, als Aufsichtsorgan von Fedpol und als Mitglied europäischer Arbeitsgruppen wäre zuständig, derartige Fragestellungen unter Beachtung des übergeordneten Rechts umfassend zu klären.

IV.II. SCHULPSYCHOLOGISCHER DIENST, KREISSTELLE 1 IN LIESTAL

Der Schulpsychologische Dienst bearbeitet zahlreiche sensitive Daten, z. B. von Schülerinnen und Schülern in speziellen Lebenssituationen, und tauscht sie mit anderen Institutionen aus. Die Datenschutzbeauftragte bereitete deshalb im Berichtsjahr eine Kontrolle vor, die im ersten Quartal 2014 mit Unterstützung einer externen Firma durchgeführt wird.

IV.III. OPEN SYSTEM INVALIDEN-VERSICHERUNG

Bei einer Kontrolle einer IV-Stelle eines anderen Kantons wurden bei der Applikation Open System Invaliden-Versicherung (OSIV) Mängel in der Umsetzung von datenschutzrechtlichen Vorgaben festgestellt. Da OSIV auch im Kanton Basel-Landschaft und in anderen Kantonen von IV-Stellen angewendet wird, wählten die Datenschutzbeauftragte und andere kantonalen Datenschutzbehörden ein gemeinsames Vorgehen. Die beteiligten Datenschutzbeauftragten stellten ihren IV-Stellen gleichlautende Fragen, zu deren OSIV-Anwendung. Eine erste Auswertung der Antworten ergab, dass sich bei allen IV-Stellen ähnliche Problemstellungen abzeichneten. Die Datenschutzbeauftragen der beteiligten Kantone werden 2014 das weitere Vorgehen festlegen.

IV.IV. AMT FÜR MIGRATION

Das Amt für Migration (AfM) bearbeitet zahlreiche Daten von ausländischen Personen. Als Geschäftskontrolle dieser Datenbearbeitung wendet es unter anderem das IT-System Tribuna 2000 ein.

Im Auftrag der Datenschutzbeauftragten kontrollierte im Berichtsjahr eine externe Firma beim AfM das IT-System Tribuna 2000 sowie ausgewählte Geschäftsprozesse. Die Kontrolle ergab, dass die gesetzlichen Vorgaben zu Informationssicherheit und Datenschutz in den untersuchten Gebieten mehrheitlich gut erfüllt sind und insgesamt ein gutes Bewusstsein im Bereich Datenschutz besteht. Bei der Anwendung des IT-Systems Tribuna 2000 zeigte die Kontrolle indessen Handlungsbedarf beim Datenschutz und im Bereich der Informationssicherheit. Die Datenschutzbeauftragte zeigte Verbesserungsmassnahmen auf. Weil das System Tribuna 2000 von der neuen Version 3 abgelöst werden soll, könnten die Verbesserungsmassnahmen bereits bei der Ablösung umgesetzt werden. Die Datenschutzbeauftragte plant 2014 ein Follow-up der empfohlenen Massnahmen.

IV.V. PERSONALDIENST DER GERICHTS-VERWALTUNG

Nach den Kontrollen von zwei kantonalen Personaldiensten im Vorjahr[15] kontrollierte die Datenschutzbeauftragte im Berichtsjahr den Personaldienst der Gerichtsverwaltung auf datenschutzrechtliche Themen: Sie kontrollierte Führung und Aufbewahrung der Personaldossiers, Bewerbungsverfahren, Eintritt und Austritt aus dem Staatsdienst und weitere Bearbeitungsprozesse im Zusammenhang mit Personaldossiers. Aus Ressourcengründen verzichtete sie darauf, die elektronische Bearbeitung der Personaldaten zu kontrollieren.

15] Vgl. Tätigkeitsbericht 2012

Die Kontrolle der Datenschutzbeauftragte ergab, dass die datenschutzrechtlichen Vorgaben im Wesentlichen gut eingehalten wurden und dass sich die Mitarbeitenden des Personaldienstes der Sensitivität der Daten bewusst waren. Handlungsbedarf zeigte sich hingegen bei der Aufbewahrung der Personaldossiers. Dieser wurde von den Verantwortlichen erkannt.

IV.VI. NEUE ELEKTRONISCHE PERSONAL-DOSSIERS BEIM PERSONALAMT

Die zahlreichen Personaldossiers innerhalb der Kantonalen Verwaltung können besondere Personendaten (Gesundheitsdaten, Angaben zu Krisensituationen etc.) enthalten; ein Missbrauch dieser Daten könnte für die Betroffenen eine erhebliche Verletzung der Persönlichkeitsrechte bedeuten. Die Angestellten haben kaum Möglichkeiten, den Umgang mit ihren Daten zu überprüfen.

Im Rahmen von SAP HR wurden sämtliche Papierdossiers in elektronische Dossiers überführt. Eine spezialisierte Firma scannte dazu die meisten Papierdossiers ein. Die Datenschutzbeauftragte prüfte den Auftrag und die Umsetzung des Scanning-Prozesses anhand eines Fragebogens.

Anhand der Fragebogen und der weiteren Unterlagen des Personalamts stellte die Datenschutzbeauftragte fest, dass im Scanning-Prozess den datenschutzrechtlichen Anliegen, insbesondere der Datensicherheit und der Vertrau-

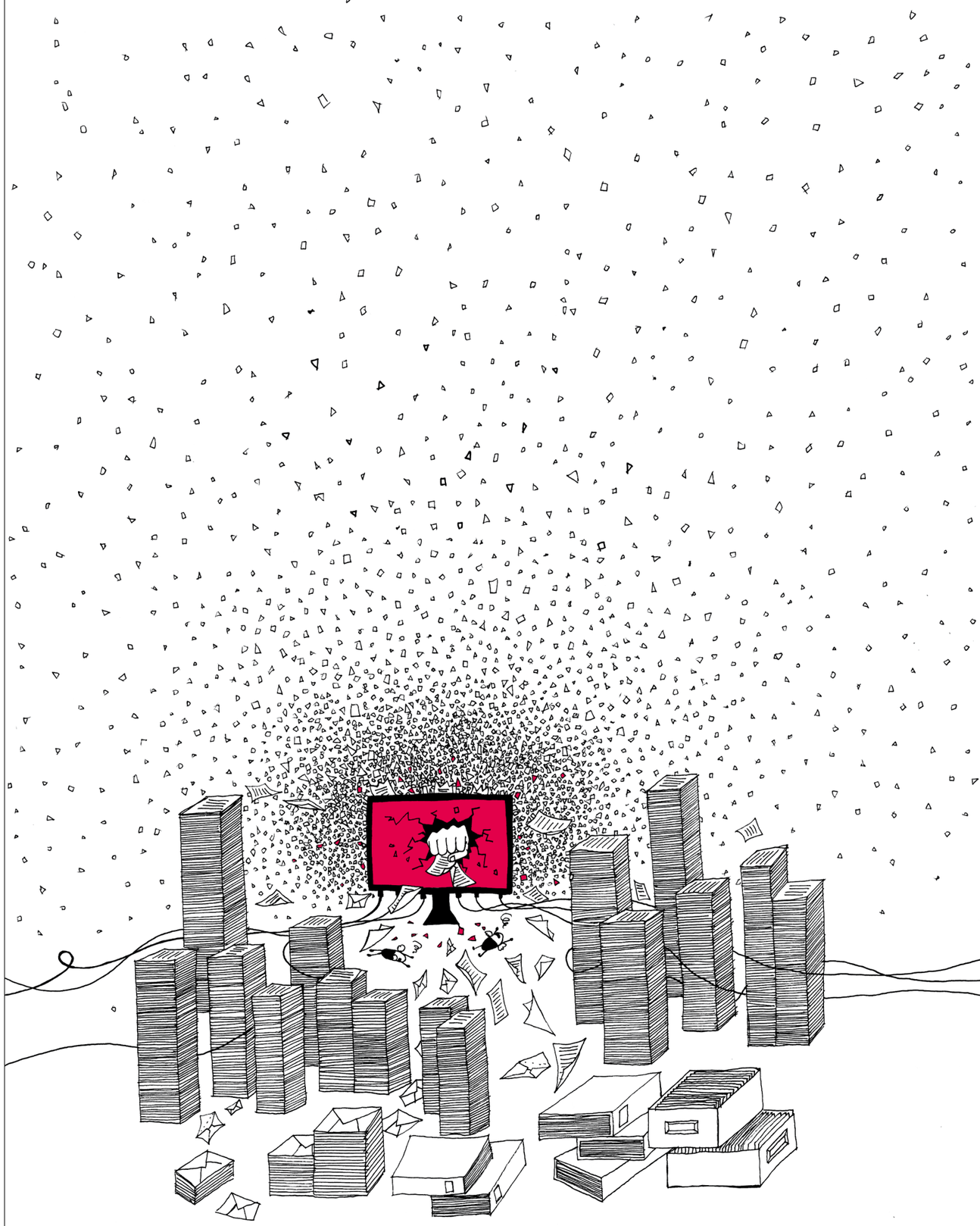
lichkeit, angemessen Rechnung getragen wurde. Sie verzichtete darauf, den Prozess vor Ort in der Ostschweiz zu kontrollieren, behielt sich aber vor, den Bereich E-Dossier im Folgejahr beim Personalamt zu prüfen.

IV.VII. KONTROLLE: ONLINE-ZUGRIFFE AUF DAS EDV-GRUNDBUCH

Das EDV-Grundbuch enthält auch vertrauliche Angaben, beispielsweise über Hypotheken und andere Belastungen von Immobilien. Die Grundeigentümerinnen und Grundeigentümer haben deshalb das Recht, dass ihre Daten nach den geltenden Standards vor Missbrauch geschützt werden.

Die Datenschutzbeauftragte kontrollierte plangemäss [16], ob der Bereich Zivilrecht, wie gesetzlich vorgesehen, den Online-Zugriff auf das EDV-Grundbuch geprüft hatte. Dabei musste sie erneut feststellen, dass die Zugriffe nicht kontrolliert wurden. Der Bereich Zivilrecht anerkannte den Mangel und leitete – mit Unterstützung externer Fachleute – Massnahmen ein, die 2014 umgesetzt werden sollen.

16] Vgl. Tätigkeitsbericht 2012



V. STELLUNGNAHMEN

Die Datenschutzbeauftragte erhält Mitberichte zur Prüfung und Stellungnahme. Im Berichtsjahr waren es 82 Mitberichte, von denen allerdings nur 17 datenschutzrelevante Inhalte enthielten, die eine Stellungnahme erforderten. Aufgrund der kurzen Fristen beschränkte sich die Datenschutzbeauftragte meistens auf summarische Prüfungen. Sie äusserte sich unter anderem zu folgenden Themen: ICT und IT-Strategie der Schulen, Anmelde- und Registergesetz, Liste säumiger Prämienzahlenden von Krankenkassen, elektronisches Amtsblatt, Kinderspitalvertrag (vgl. II.III.a), Umgang mit Mitarbeitendengesprächen, Onlinezugriffen auf Daten der Motorfahrzeugkontrolle, dritte Etappe von Enterprise Resource Planning (ERP) und Laufbahnverordnung. Die rechtlichen Beurteilungen der Datenschutzbeauftragten wurden teilweise berücksichtigt. Insbesondere bei der Stellungnahme zum Kinderspitalvertrag und zu personalrechtlichen Themen (vgl. V.I.) wurden ihre rechtlichen Bedenken kaum beachtet.

V.I. UMGANG MIT PERSONALDATEN

Die Datenschutzbeauftragte befasste sich wiederholt mit der zentralen Bearbeitung von Personaldaten im SAP (vgl. auch IV.VI.). Dessen Regelungen sehen vor, dass die Mitarbeitenden, die Papierakten scannen, permanent und umfassend Zugriff auf die E-Dossiers erhalten, während die Vorgesetzten, die die Personaldossiers zur Aufgabenerfüllung benötigten, nur eingeschränkt darauf zugreifen können. Die Datenschutzbeauftragte wies in einer Stellungnahme darauf hin, dass diese Zugriffsregelungen weder organisatorisch noch rechtlich nachvollziehbar seien. Trotz ihrer Stellungnahme blieben die Zugriffsberechtigungen 2013 unverändert. Inwieweit die sich daraus ergebende Praxis rechtmässig ist, wird eine Prüfung vor Ort zeigen.

V.II. EINHEITLICHES SCHWEIZERISCHES DATENSCHUTZRECHT

Die Konferenz der Kantonsregierungen fragte die Kantone, ob sie eine Änderung der Bundesverfassung unterstützen, die dem Bund die Kompetenz erteilt, die «allgemeine Datenschutzgesetzgebung» zu vereinheitlichen. Anlass für die geplante Änderung war eine interne Evaluation des Datenschutzgesetzes des Bundes; aufgrund dieser Evaluation beauftragte der Bundesrat eine Arbeitsgruppe des Eidgenössischen Polizei- und Justizdepartements, bis Ende 2014 Vorschläge für eine Revision vorzulegen, die den Datenschutz effizienter machen könnte. Dabei wurde die Idee diskutiert, den Anwendungsbereich des Bundesdatenschutzgesetzes auf die Kantone auszudehnen.

In der föderalistisch aufgebauten Schweiz gibt es neben dem Datenschutzgesetz des Bundes auch in allen Kantonen Datenschutzgesetze (oder Informations- und Datenschutzgesetze). Die Kantone sind zuständig, allgemeine Grundsätze des Bearbeitens von Personendaten durch kantonale (und kommunale) öffentliche Organe zu erlassen. Die 26 kantonalen Datenschutzgesetze sind aufgrund der Schengen-Assoziierung weitgehend harmonisiert. Sie enthalten u. a. alle relevanten Datenschutzprinzipien und verlangen, dass Datenbearbeitungen auf einer gesetzlichen Grundlage basieren und verhältnismässig sein müssen. Unterschiede finden sich vor allem zur Organisation der Datenschutzbehörde, die von den Kantonen im Rahmen des übergeordneten Rechts frei gestaltet werden kann.

Die Datenschutzbeauftragte prüfte deshalb die Folgen eines gesamtschweizerischen Datenschutzgesetzes für den Kanton, die Gemeinden und nicht zuletzt für die von einer behördlichen Datenbearbeitung betroffenen Personen.

Am materiellen Datenschutzrecht und somit am Fach- und Sachrecht der Kantone und Gemeinden, das unter anderem in den kantonalen Polizeigesetzen, Bildungsgesetzen, Gesundheitsgesetzen zu finden ist, würde ein gesamtschweizerisches Datenschutzgesetz kaum etwas ändern (vgl. II.III.). Im materiellen Datenschutzrecht blieben die Unterschiede, die durch den föderalistischen Aufbau der Schweiz bedingt sind, also bestehen. Dazu käme die Zuständigkeit für über 2300 Gemeinden. Ob es tatsächlich effizienter wäre, wenn eine zentrale Bundesdatenschutzbehörde z. B. 26 unterschiedliche Fachgesetze und unzählige Gemeindeerlasse anwenden müsste, darf in Frage gestellt werden. Zu klären wäre ferner, wie weit sich eine zentralistisch organisierte Kontrollbehörde des Bundes in die Belange der autonomen Kantone einmischen dürfte.

In ihrer Stellungnahme wies die Datenschutzbeauftragte darauf hin, dass es für die Kantone keine gewichtigen Vorteile gibt, die eine Änderung der Bundesverfassung rechtfertigen würden. Verloren ginge indessen die Nähe zu den Behörden und zur Bevölkerung. Die Datenschutzbeauftragte hielt zudem fest, dass grundsätzliche Schwierigkeiten der föderalistischen Strukturen sich kaum lösen lassen, indem eine Querschnittsmaterie wie der Datenschutz, die stark vom materiellen Recht geprägt ist, dem Bund übertragen wird.

VI. ÖFFENTLICHKEITSARBEIT

VI.I. MEDIENKONTAKTE UND PUBLIKATIONEN

Die Datenschutzbeauftragte erhielt im Berichtsjahr diverse Medienanfragen zu so unterschiedlichen Themen wie Videoüberwachung in Hallenbädern, Google Streetview in Gemeinden, «Steuerpranger», Fotofallen im Wald und Cloud Computing. Weitere Medienfragen betrafen die Datenschutzbeauftragte: entweder zu Themen ihres Tätigkeitsberichts 2012 oder aufgrund der Budgetdebatte 2013, wobei vor allem deren Ressourcen interessierte.

Aufgrund des grossen Geschäftsvolumens blieb im Berichtsjahr einmal mehr wenig Zeit für Publikationen. Am aufwendigsten war der rechtlich vorgegebene Tätigkeitsbericht 2012. Die Datenschutzbeauftragte verfasste zudem einen Beitrag für die Broschüre «Der Kanton in Kürze» der Landeskanzlei. Im Rahmen des IDG überarbeitete sie – mit Unterstützung des Rechtsdiensts der Bildungs- Kultur- und Sportdirektion – den Leitfaden «Datenschutz für Kindergärten, Schulen und spezielle Schuldienste des Kantons Baselland» sowie diverse Merkblätter.

VI.II. KURSE UND REFERATE

2013 führte die Datenschutzbeauftragte Schulungen zum Datenschutz für folgende Gruppen durch: Polizeiaspirantinnen und -aspiranten, KV-Lernende des Kantons, Lernende der Finanz- und Kirchendirektion sowie Informationssicherheitsbeauftragte des Kantons. Sie referierte zum Thema Öffentlichkeitsprinzip an der Konferenz der Schulratspräsidien und unterrichtete die Absolventinnen und Absolventen des CAS «Öffentliches Gemeinwesen» der Fachhochschule Nordwestschweiz.

VII. KANTONALE, NATIONALE UND INTERNATIONALE ZUSAMMENARBEIT

Wirksamer Datenschutz setzt geeignete Massnahmen zur Informationssicherheit voraus. Die Datenschutzbeauftragte intensivierte dazu im Berichtsjahr den Austausch mit den Mitarbeitenden, die für die Informationssicherheit innerhalb der kantonalen Verwaltung zuständig sind. Sie schulte die kantonalen Sicherheitsbeauftragten (SIBE) und nahm an mehreren SIBE-Sitzungen teil. Aufgrund der positiven Reaktionen wird die Datenschutzbeauftragte diese konstruktive Zusammenarbeit weiterführen.

VII.I. AUSTAUSCH MIT DEN KANTONALEN SICHERHEITSBEAUFTRAGTEN

VII.II. ARBEITSGRUPPE INFORMATION AND COMMUNICATION TECHNOLOGY

Die Datenschutzbeauftragte ist in der Arbeitsgruppe Information and Communication Technology (AG ICT) von Privatim, der Vereinigung der schweizerischen Datenschutzbeauftragten, vertreten. In der AG ICT sind Informatikfachleute der Datenschutzbehörden der Schweiz und Liechtensteins vertreten. Die Arbeitsgruppe dient als Plattform für den fachlichen Austausch und erarbeitete im Berichtsjahr ein Papier über die datenschutzrechtlichen Anforderungen an Krankenhaus-Informationssysteme.

VII.III. PRIVATIM

Die Datenschutzbeauftragte trat 2013 aus dem Vorstand von Privatim, der Vereinigung der Schweizerischen Datenschutzbeauftragten, zurück. Die Vereinsstatuten ermöglichen es jedoch, dass sie weiterhin an den Vorstandssitzungen teilnehmen kann, wenn die Traktanden für die kantonalen Belange relevant sind.

Im Berichtsjahr äusserte sich Privatim zum Bundesgesetz über die Sammlung des Bundesrechts und das Bundesblatt, zum Bundesgesetz über die Registrierung von Krebserkrankungen, zum Bundesgesetz über die Zuständigkeit im Bereich des zivilen Nachrichtendienstes sowie zur Statistikerhebungsverordnung und zur Verordnung über die Datenverknüpfung[17]. Ferner startete Privatim eine Untersuchung zur Frage der Datenbearbeitung im Rahmen der Rechnungskontrolle gemäss Krankenversicherungsgesetz (KVG), an der sich auch die Datenschutzbeauftragte beteiligte.

17] www.privatim.ch/de/themen/category/vernehmlassungen.html

VIII. AUSBLICK

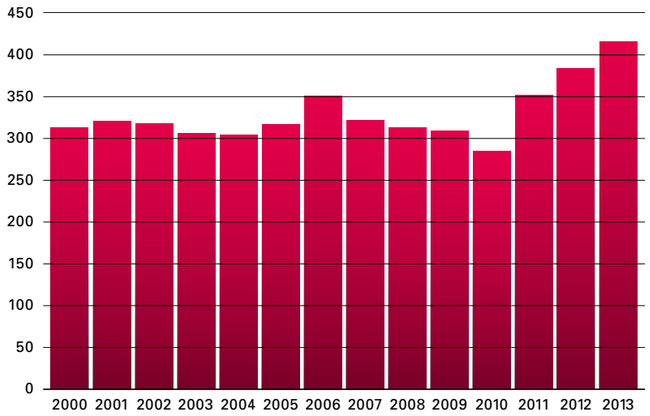
Datenschutz und das Recht auf Informationszugang sind zwei zukunftsorientierte Bereiche, die einem starken Wandel unterworfen sind. Auch im kommenden Jahr wird es darum gehen, das Bewusstsein für diese Themen zu schärfen, Verständnis für die teils komplexe Materie zu schaffen und praxisorientiert Lösungen zu erarbeiten.

Gemeinsam mit dem vergrösserten Team, das sich weiterhin für eine grösstmögliche Wirkung einsetzen wird, wird die Datenschutzbeauftragte die standardisierte Kontrolltätigkeit weiterentwickeln und ein Konzept für die Durchsetzung der Vorabkontrolle erarbeiten. Bei der Beratung wird sie der grossen Themenvielfalt weiterhin mit Professionalität und grosser Fachkenntnis begegnen.

In Zukunft wird es darum gehen, neben dem Datenschutz auch das Recht auf Informationszugang bekannter zu machen. Der Wandel von Amtsgeheimnis zum Öffentlichkeitsprinzip wird aber nicht von heute auf morgen geschehen. Es wird in den nächsten Jahren darum gehen, die Informationsrechte der Bürgerinnen und Bürger zu stärken und die Behörden soweit als möglich in diesem Prozess zu begleiten.

ANHANG

GESCHÄFTE



ART DER GESCHÄFTE