Vorlage an den Landrat des Kantons Basel-Landschaft

Titel: **Tätigkeitsbericht 2014 der Aufsichtsstelle Datenschutz**

Datum: Juni 2015

Nummer: 2015-040_09

Bemerkungen: **Verlauf dieses Geschäfts**

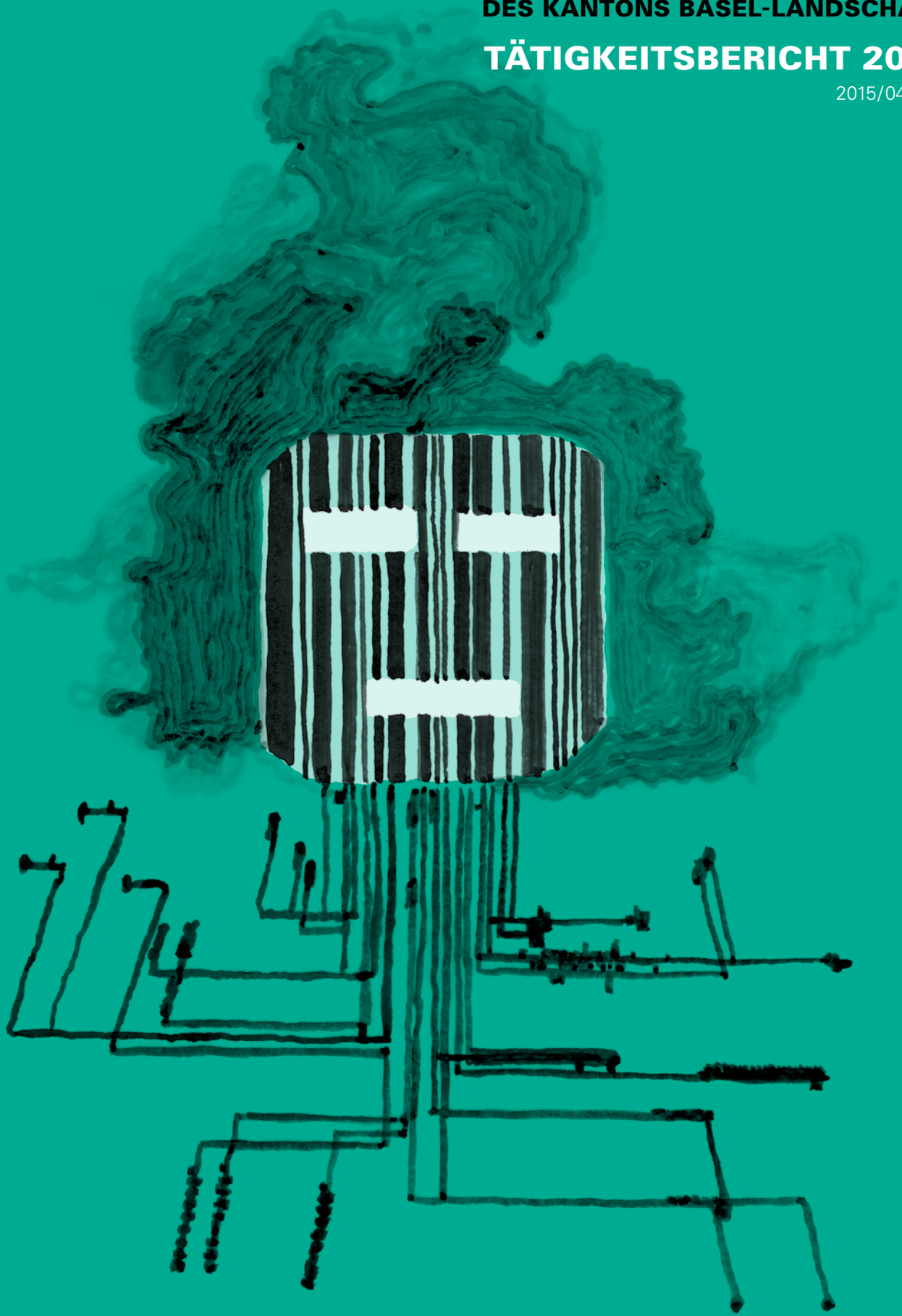
Links:

- 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 2014

2015/040-09



**AUFSICHTSSTELLE DATENSCHUTZ
DES KANTONS BASEL-LANDSCHAFT**

Datenschutzbeauftragte:	Ursula Stucki
Stv. Datenschutzbeauftragter:	Tobias Schnelli
Akademische Mitarbeitende:	Priscilla Dipner-Gerber
	Thomas Held
	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 (IDG) 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 WESENTLICHE IN KÜRZE

Die Datenschutzbeauftragte[1] hat die Aufgabe, die Grenzen staatlicher Datenbearbeitung beratend und kontrollierend auszuloten. Im Rahmen ihres Beratungsauftrags sucht sie – gemeinsam mit den datenbearbeitenden Behörden – Lösungen, die sowohl eine effiziente Datenbearbeitung als auch den Schutz der Privatheit der Bürgerinnen und Bürger ermöglichen. 2014 erhielt sie 176 Anfragen von Behörden, davon 19 zum Öffentlichkeitsprinzip. Die Anfragen reichten von einfacheren Sachverhalten bis hin zu komplexen Informatikfragen beispielsweise zu Mobile Device Management oder Cloud Computing. Die Datenschutzbeauftragte beriet im Berichtsjahr auch 50 Privatpersonen, davon 3 zum Öffentlichkeitsprinzip. Diese Aufgaben waren vielseitig und anspruchsvoll.

Die Datenschutzbeauftragte schloss im Berichtsjahr drei datenschutzrechtliche Kontrollen ab und startete drei neue. In mehreren Follow-ups überprüfte sie zudem die vereinbarten Massnahmen von früheren Kontrollen. Sie stellte fest, dass die Behörden gewillt sind, die Privatsphäre der Bürgerinnen und Bürger zu schützen. Bei der technischen Umsetzung der rechtlichen Anforderungen stiessen sie indessen manchmal an ihre Grenzen. So fehlte beispielsweise das Know-how, oder angeschaffte Applikationen waren mangelhaft.

Datenschutz und Informationssicherheit sind untrennbar miteinander verbunden. Die Datenschutzbeauftragte stellte bereits früher fest, dass Entscheidungsträger die Informationssicherheit oft nicht ausreichend berücksichtigen. Dass dies teuer werden kann, zeigte sich im Berichtsjahr bei der Umstellung der IT-Arbeitsplätze auf eine neue Plattform (Projekt CliZ). Die mangelhafte Inventarisierung der Soft- und Hardware verursachte erhebliche Mehrkosten.

Personendaten werden heute vorwiegend elektronisch bearbeitet, was fundierte Informatikressourcen der Kontrollbehörde bedingt. Im Berichtsjahr konnte die Datenschutzbeauftragte das IT-Know-how mit einer neuen Informatikstelle substanziell erweitern. Damit ist sie jetzt fachlich und personell in der Lage, anstehende Informatikfragen adäquat anzugehen, IT-Kontrollen zu begleiten und die präventive Vorabkontrolle aufzubauen.

Der Landrat beschloss im Berichtsjahr, die Datenschutzbehörde administrativ der Landeskanzlei zuzuordnen. Sie wird dadurch mit den anderen sogenannten besonderen Behörden gleichgestellt, und ihre Unabhängigkeit wird betont. Nach 22 Jahren bei der Sicherheitsdirektion bereitete die Datenschutzbeauftragte daraufhin die administrative Zuordnung zur Landeskanzlei vor.

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

II. THEMEN 2014

II.I. EINMAL IM NETZ – IMMER IM NETZ

Im Internet geben Menschen ihre Ansichten, Bilder und weitere sensitive Daten preis und teilen selbst Intimstes mit «Freunden» aus dem Netz. Im Rahmen ihrer Schulungen stellte die Datenschutzbeauftragte fest, dass sich die wenigsten Nutzenden bewusst sind, dass sie im Internet eine Datenspur hinterlassen und dass ihre Daten kaum mehr löschbar sind. Unbekannte Dritte können die Daten auswerten oder zu einem Persönlichkeitsprofil hinzufügen. Sich nachträglich dagegen zu wehren oder die Daten löschen zu lassen, ist schwierig bis unmöglich.

Öffentliche Organe, die via Internet die Bevölkerung informieren, veröffentlichen Personendaten in der Regel zurückhaltend. Die Datenschutzbeauftragte stellte im Berichtsjahr fest, dass einige Schulen neue Wege gefunden haben, um zum Beispiel Bilder der Schülerinnen und Schüler datenschutzkonform zu publizieren. So verfügen ihre Websites beispielsweise über eine geschlossene Benutzergruppe, oder sie zeigen Fotos passwortgeschützt[2]. Datenschutz verunmöglicht somit nicht, dass beispielsweise Fotos elektronisch zugänglich werden, sondern gibt Denkanstösse, wie sich Informationsbedürfnisse mit zeitgemässer Technologie realisieren lassen, ohne die Persönlichkeitsrechte der Schülerschaft zu vernachlässigen.

2] Statt vieler: Website der Primarschule Muttenz www.primar-muttenz.ch

II.II. DATEN-BEARBEITUNG DURCH EXTERNE DIENSTLEISTER

Ein öffentliches Organ bleibt auch dann für den Datenschutz verantwortlich, wenn es Aufgaben auslagert und Daten durch Dritte bearbeiten lässt. Wichtig sind deshalb die Vorarbeiten vor dem Vertragsschluss. Zunächst muss geklärt sein, wer welche Daten bearbeiten soll. Werden besondere Daten wie Angaben zur Gesundheit, das Erbgut oder politische Ansichten bearbeitet oder ganze Persönlichkeitsprofile erstellt, sind höhere Sicherheitsmassnahmen erforderlich. Der externe Vertragspartner muss die Massnahmen aufzeigen, mit denen er die Informationssicherheit gewährleistet. Er muss auch nachweisen, dass die Daten nur in einem Land mit adäquatem Datenschutz bearbeitet werden. Zudem sollte ein Gerichtsstand in der Schweiz vereinbart werden. Eine Auslagerung von Datenbearbeitungen darf nicht dazu führen, dass Kontrollen durch staatliche Organe verunmöglicht werden.

Einzelne Verträge verpflichten externe Dienstleister, ihre Unterlagen an Revisionsfirmen herauszugeben, soweit diese ebenfalls zur Geheimhaltung verpflichtet worden sind. Ähnliche Regelungen für den Bereich der datenschutzrechtlichen Kontrolle fehlen hingegen weitgehend, und die Rechte der Datenschutzbeauftragten müssen aus dem Gesetz abgeleitet werden. Das kann unnötigen Aufwand generieren. Im Berichtsjahr führten bei einer Kontrolle der Datenschutzbeauftragten die fehlenden vertraglichen Regelungen zu erheblichen Verzögerungen und damit auch zu Mehrkosten.

II.III. DATENSCHUTZ UND INFORMATIONSSICHERHEIT

Die Datenschutzbeauftragte beriet im Berichtsjahr Behörden, die Personendaten elektronisch bearbeiten. So befasste sie sich mit einem webbasierten Instrument für die Bedarfserfassung im Behindertenbereich, den Applikationen Cari und Tribuna, dem e-Personaldossier, dem Mobile Device Management sowie der Schuladministrationslösung.

Sie stellte dabei fest, dass Informatikprojekte nicht konsequent nach der im Kanton geltenden Methodik (Hermes)[3] durchgeführt wurden und dadurch wichtige Aspekte unberücksichtigt blieben. So wurden die rechtlichen Rahmenbedingungen nicht frühzeitig analysiert, die Informationseigner bei der Abklärung des Schutzbedarfs nicht involviert und die Prozesse und Rollen nicht beschrieben, wodurch die Zugriffsberechtigungen nicht funktionsbezogen festgelegt werden konnten. In vielen Projekten fehlte zudem ein Konzept für die behördeninterne Regelung zur Archivierung und Löschung der Daten. Dass diese wichtigen Projektdokumente fehlten, war nicht zuletzt auf Ressourcendruck in den Projekten zurückzuführen. Eine weitere Herausforderung bleibt die Regelung der Verantwortung für dezentral erhobene und zentral gehaltene Daten.

Im Berichtsjahr nahm die Datenschutzbeauftragte zur Kenntnis, dass der Kanton über kein aktuelles Inventar der Hard- und Software verfügte. So zeigte das Projekt CliZ 400 nicht inventarisierte Geräte und zahlreiche nicht erfasste Applikationen, zum Teil auch ohne definierte Anwendungsverantwortliche. Dies führte bei CliZ zu einem erhöhten Zeitaufwand für die Informationsbeschaffung und zu erheblichen Mehrkosten[4]. Glücklicherweise entstand neben den finanziellen Folgen kein weiterer Schaden. Ob die Lehren aus dem Projekt gezogen werden, wird sich zeigen. Dass das kantonale Inventar der Hard- und Software aktuell und vollständig gepflegt wird, ist nicht nur für künftige Migrationsprojekte unabdingbar, sondern auch für das Risikomanagement der Informationssicherheit. Die dazu erforderlichen Beschaffungs- und Projektprozesse bedingen indessen entsprechende Ressourcen.

Pannen lassen sich im komplexer werdenden Geschäftsalltag kaum verhindern. Mit einer risikobasierten Planung des Mitteleinsatzes liessen sich deren Häufigkeit und Auswirkungen jedoch begrenzen. Zwar kosten beispielsweise die Definition eines IT-Grundschutzes, die Implementation von IT-Sicherheitskonzepten, die Klassifizierung der Ressourcen und die Schulung von Mitarbeitenden Zeit und Geld. Weil die IT immer stärker in die Geschäftsprozesse integriert wird

3] § 12 Verordnung über die Informationssicherheit (VIS) vom 11. März 2008 (SGS 162.51)

4] LR-Vorlage 2014/135: Nachtragskredit zur Umstellung der IT-Arbeitsplätze in der kantonalen Verwaltung auf eine neue Plattform, S. 5

und dadurch die Abhängigkeit von ihr zunimmt, kann es sich zwar durchaus lohnen, in die Prävention zu investieren.

II.IV. VORAB-KONTROLLE

Der Informationsaustausch nimmt mengenmässig rasant zu und wird technisch immer komplexer: unter Behörden, zwischen Behörden und Privaten sowie zwischen Behörden und der Wirtschaft. Staatliche Aufgaben werden häufiger an Externe delegiert, und auch neue E-Government-Prozesse setzen auf neue Technologien und Plattformen. Der Schutz der ausgetauschten Informationen hängt somit zunehmend von den elektronischen Verfahren und Mitteln ab. Gegen aktuelle Bedrohungen (Systemausfall, Hacking etc.) sind risikobasierte Schutzmassnahmen notwendig.

Im Rahmen der Vorabkontrolle prüft die Datenschutzbeauftragte, ob öffentliche Organe Informationen gestützt auf einer Rechtsgrundlage und mit angemessenen organisatorischen und technischen Schutzmassnahmen bearbeiten (§12 IDG).

Wenn die spezifischen Rechte und Freiheiten der betroffenen Personen bereits vor der realisierten oder geänderten Datenbearbeitung abgeschätzt und minimiert werden, lassen sich aufwendigere Nachbesserungen bei der Umsetzung vermeiden. Trotzdem legten im Berichtsjahr die öffentlichen Organe der Datenschutzbeauftragten ihre Projekte erst vereinzelt und oft zu spät zur Vorabkontrolle vor. Das lag auch daran, dass die Datenschutzbeauftragte aufgrund mangelnder Ressourcen für die Vorabkontrolle die Organe lange nicht ausreichend sensibilisieren und mit methodischen Grundlagen unterstützen konnte. Ab Mitte 2014 konnte sie diese Lücke mit zusätzlichen personellen Ressourcen schliessen. Bereits erstellte sie einen Leitfaden für die Vorabkontrolle, der 2015 veröffentlicht wird. Er soll die Qualitätssicherung, die Informationssicherheit und das gesamte Informatikvorhaben erleichtern und so dazu beitragen, die Vorabkontrolle bei den öffentlichen Organen durchzusetzen.

III. FÄLLE AUS DEM BERATUNGS-ALLTAG

Die Datenschutzbeauftragte erhielt im Berichtsjahr 226 Anfragen: 176 Anfragen stammten von Behörden, davon betrafen 19 das Öffentlichkeitsprinzip. Zudem wandten sich 50 Privatpersonen an die Datenschutzbeauftragte, wovon 3 Anfragen das Öffentlichkeitsprinzip betrafen. Kurze telefonische Anfragen erfasst die Datenschutzbeauftragte weiterhin nicht in der Statistik, wenn das Erfassen länger als die Beantwortung dauern würde.

III.I. DATENSCHUTZ

III.I.a «GESUNDHEITS-ERKLÄRUNG» DER PENSIONSKASSE BASEL-LANDSCHAFT

Die Pensionskasse Basel-Landschaft (PKBL) darf von neu zu versichernden Personen oder von bereits versicherten Personen, die ihr Pensum erhöhen, Angaben zur Gesundheit einfordern. Weil die sogenannte «Gesundheitserklärung» der PKBL persönliche Fragen enthielt, wandten sich Betroffene an die Datenschutzbeauftragte. Sie prüfte den Fragenkatalog der «Gesundheitserklärung» auf seine Rechtmässigkeit und stellte fest, dass er auch Fragen zu Krankheiten bei Eltern oder Geschwistern enthielt, beispielsweise zu Herz- und Kreislaufleiden oder zu psychischen Störungen.

Die Datenschutzbeauftragte bat die PKBL und den vertrauensärztlichen Dienst der Pensionskasse um eine Stellungnahme zum Fragenkatalog. Der Vertrauensarzt stellte fest, dass Angaben zu Krankheiten der Eltern und der Geschwister für die Prüfung des Gesundheitszustands der Versicherungsnehmenden nicht nötig sind und die entsprechenden Fragen somit ersatzlos gestrichen werden können.

Die PKBL war mit diesen Ausführungen einverstanden und passte den Fragebogen entsprechend an.

III.I.b **EINWOHNERREGISTER-DATEN FÜR DAS PATIENTENARCHIV DES KANTONSSPITALS**

Um ihr Patientenarchiv zu aktualisieren, liess eine Abteilung des Kantonsspitals einer Gemeinde eine Liste mit Personendaten zukommen. Sie wollte von der Gemeinde wissen, ob die aufgeführten Personen leben oder verstorben sind.

Mit dem Versand der Patientenlisten an die Gemeinden gab das Kantonsspital bekannt, welche in der Gemeinde wohnhaften Personen es behandelte. Die von der Gemeinde eingeschaltete Datenschutzbeauftragte stellte fest, dass eine Legitimation für diese Bekanntgabe fehlte. Zudem dürfen Daten der Patientinnen und Patienten nach Abschluss einer Behandlung nicht weiter bearbeitet werden. Krankengeschichten sollten frühestens 10 Jahre nach der letzten Behandlung archiviert oder vernichtet werden. Diese Aufbewahrungsfrist basiert auf der Verjährungsfrist, die im Schadensfall zu beachten ist. Da auch Erben von Verstorbenen eine Schadenersatzforderung geltend machen können, gab es keinen ersichtlichen Grund, weshalb das Todesdatum von ehemaligen Patientinnen und Patienten für die Archivierung in Erfahrung gebracht werden müsste.

Die Datenschutzbeauftragte teilte der Gemeinde mit, dass die Voraussetzungen für die vom Spital gewünschte Datenbekanntgabe nicht erfüllt sind. Da sich die Archivierung an der gesetzlichen Aufbewahrungsfrist von 10 Jahren orientieren kann, sind Angaben zum genauen Todesdatum weder erforderlich noch geeignet um ein Spitalarchiv zu organisieren.

III.I.c **E-MAILS MIT PROTOKOLLEN DER GEMEINDERATSSITZUNGEN**

Eine Gemeinde fragte die Datenschutzbeauftragte, ob es aus datenschutzrechtlicher Sicht problematisch sei, die Protokolle der Gemeinderatssitzungen den Mitgliedern des Gemeinderats und der Geschäftsprüfungskommission unverschlüsselt per E-Mail zu senden.

Die Datenschutzbeauftragte teilte der Gemeinde mit, dass Vertrauliches grundsätzlich nicht unverschlüsselt in E-Mails gehört. Gemeinderatsprotokolle enthalten in der Regel nicht nur schützenswerte Personendaten, sondern auch politisch heikle Inhalte, die nur von einem bestimmten Personenkreis gelesen werden sollten. Sie empfahl dem Gemeinderat, Vertrauliches nur verschlüsselt via E-Mail zu versenden, und machte einmal mehr auf die Möglichkeit einer geschlossene Benutzergruppe aufmerksam. Der Entscheid, welches Risiko er eingehen will, liegt letztlich beim Gemeinderat.

III.I.d **PERSONENDATEN DES SOZIALDIENSTS FÜR DIE EINWOHNERKONTROLLE**

Die Einwohnerkontrolle einer Gemeinde forderte vom Sozialdienst der gleichen Gemeinde die aktuellen Adressen von Personen, die in Pflegeheimen untergebracht worden sind. Der Sozialdienst weigerte sich unter Berufung auf den Datenschutz, die entsprechenden Adressen bekannt zu geben, und wandte sich an die Datenschutzbeauftragte.

Die Datenschutzbeauftragte teilte der Einwohnerkontrolle mit, dass der Datenschutz auch innerhalb einer Gemeinde gilt und eine Datenbekanntgabe dann zulässig ist, wenn ein Gesetz dies vorsieht oder die Angaben zur Erfüllung einer gesetzlichen Aufgabe erforderlich sind. Soweit die Einwohnerkontrolle erläutern konnte, für welche gesetzliche Aufgabe sie die Daten benötigte, konnte die Datenbekanntgabe als rechtmässig erachtet werden.

III.I.e **BEKANNTGABE VON GESPERRTEN PERSONENDATEN DURCH EINE GEMEINDE**

Eine Gemeinde fragte die Datenschutzbeauftragte an, ob sie die Adresse einer Person, die bei der Einwohnergemeinde eine Adresssperre hinterlegt hatte, einer Firma bekannt geben dürfe. Die Firma benötigte die Adresse, weil sie gegen diese Person eine offene Rechnung geltend machen wollte.

Die Datenschutzbeauftragte klärte die Einwohnerkontrolle über den Ablauf und über die Voraussetzungen für eine Durchbrechung einer Datensperre auf. Eine Gemeinde muss bei einer solchen Anfrage abklären, ob die um Bekanntgabe ersuchende Person glaubhaft machen kann, dass die Personendaten erforderlich sind, um ihre Rechtsansprüche durchzusetzen. Der Person, die ihre

Daten hatte sperren lassen, sollte das rechtliche Gehör gewährt werden. Die Gemeinde hat sodann eine Interessenabwägung vorzunehmen und zu verfügen, ob sie das Begehren auf Bekanntgabe der gesperrten Personendaten gutheisst oder abweist. Dieses Vorgehen mag zwar aufwendig erscheinen, entspricht aber gängigem Verwaltungsrecht. Zudem schützt es die Gemeinde davor, gesperrte Daten irrtümlicherweise unberechtigten Dritten bekanntzugeben und dadurch einen Schaden zu verursachen.

III.I.f AN- UND ABMELDUNG BEI DER EINWOHNER-GEMEINDE VIA FACEBOOK

Eine Gemeinde plante, zu- und wegziehende Personen, die sie auf keine andere Weise kontaktieren konnte, via Facebook zu bitten, sich an- oder abzumelden. Die Gemeinde bat die Datenschutzbeauftragte, dieses Vorgehen aus datenschutzrechtlicher Sicht zu beurteilen.

Die Datenschutzbeauftragte hielt Folgendes fest: Die Gemeindeverwaltung nimmt die An-, Um- oder Abmeldung per Verfügung vor, wenn eine zu- oder wegziehende Person dies fristgerecht unterlassen hat (§ 6 kantonales Anmeldungs- und Registergesetz). Der Gemeinde obliegt somit eine selbstständige Handlungspflicht; sie muss der an-, um- oder abmeldepflichtigen Person nicht nachforschen. Eine säumige Person per Facebook zu kontaktieren, ist deshalb nicht nötig. Falls die Person auf dem Schriftweg nicht erreichbar ist, kann die Verfügung der Abmeldung auch im kantonalen Amtsblatt publiziert werden (§ 19 kantonales Verwaltungsverfahrensgesetz).

III.I.g LISTENAUSKUNFT AN STADTRATS-KANDIDIERENDE

Einige Gemeinden wurden im Berichtsjahr von Kandidierenden für ein Exekutiv- oder ein Legislativamt um Daten für einen einmaligen Versand von Wahlinformationen gebeten. Die Gemeinden sollten ihnen einen Auszug aus dem Einwohnerregister mit Name und Adresse aller Einwohnerinnen und Einwohner zukommen lassen, die bestimmte Kriterien erfüllten (z. B. nicht älter als dreissig Jahre alt). Mehrere Gemeinden wandten sich dazu an die Datenschutzbeauftragte.

Die Datenschutzbeauftragte teilte den Gemeinden mit, dass es sich bei den gewünschten Daten um eine sogenannte Listenbekanntgabe handelt (§ 3 Absatz 3 kantonales Anmeldungs- und Registergesetz). Damit eine solche Listenbekanntgabe erlaubt ist, müssen die Personendaten, nach denen gefragt wird, für einen schützenswerten ideellen Zweck verwendet werden. Der Gesetzgeber will damit vor allem das politische Leben und die Vereinstätigkeit erleichtern. Die Anfragen der Kandidierenden erfüllten somit die Anforderungen an eine Listenbekanntgabe. Die Gemeinden mussten beachten, dass keine gesperrten Daten bekanntgegeben und die Adressen nur einmalig und nur für den angegebenen Zweck genutzt wurden. Sie stellten dies mit einer Verpflichtungserklärung der Datenempfänger sicher.

III.I.h GEBÜHREN FÜR ADRESS-AUSKÜNFTE UND EIGENE PERSONENDATEN

Die Datenschutzbeauftragte wurde im Berichtsjahr erneut mehrfach gefragt, ob für Adressauskünfte oder für die Herausgabe eigener Daten Gebühren erhoben werden dürfen.

Ob Gebühren verlangt werden dürfen, hängt von der Information ab, die herausgegeben werden soll. Gemäss IDG sind unter Informationen sämtliche Aufzeichnungen zu verstehen, welche die Erfüllung einer öffentlichen Aufgabe betreffen, unabhängig von ihrer Darstellungsform und ihrem Informationsträger. Damit eine Information verlangt werden kann, muss sie in irgendeiner Form aufgezeichnet oder verkörpert sein (z. B. als Akte, USB-Stick oder Film). Unter Informationen fallen aber auch Personendaten und somit alle Daten, die sich auf eine bestimmte oder bestimmbare natürliche oder juristische Person beziehen.

Gemäss IDG darf für den Zugang zu den eigenen Personendaten keine Gebühr erhoben werden. Das gilt selbst dann, wenn Kopien von umfangreichen Informationen verlangt werden. Wenn der Zugang zu anderen Informationen

gewährt werden soll, gilt folgende Unterscheidung: Für mündliche Auskünfte und für persönlich ausgehändigte einfache Computerausdrucke aus dem Einwohnerregister dürfen von einer Einwohnergemeinde keine Gebühren erhoben werden (§ 3 Absatz 5 kantonales Anmeldungs- und Registergesetz). Ist der Zugang hingegen mit einem aufwendigen Verfahren verbunden, beispielsweise einer umfangreichen Anonymisierung, oder müssen Kopien oder andere Datenträger erstellt werden, kann dafür eine angemessene Gebühr nach Aufwand erhoben werden. Die Richtlinien für die Höhe der Gebühren sind in der Informations- und Datenschutzverordnung festgelegt.

III.II. ÖFFENTLICHKEITS-PRINZIP

Die Datenschutzbeauftragte befasste sich im Berichtsjahr mit vielfältigen Anfragen zum Öffentlichkeitsprinzip. Mehrfach wurde gefragt, ob Schulratsprotokolle öffentlich sind. Eine andere wiederkehrende Frage war, wie das Öffentlichkeitsprinzip an der Schnittstelle von Privaten und Staat auszulegen sei, beispielsweise wenn sich eine Gemeinde als Aktionär an einem privaten Unternehmen beteiligt. Dazu kamen eher technische Fragen wie nach der Zuständigkeit oder nach der Berechnung der im Öffentlichkeitsprinzip vorgesehenen Gebühren.

Die Datenschutzbeauftragte stellte fest, dass den Behörden nicht immer klar war, dass Gesuche um Informationszugang und Gesuche um Zugang zu den eigenen Daten unterschiedlichen Zwecken dienen. Der allgemeine Informationszugang soll das Verwaltungshandeln transparenter machen. Der Zugang zu den eigenen Personendaten ist hingegen ein datenschutzrechtliches Instrument, das den Bürgerinnen und Bürgern das Recht einräumt, sich über die staatliche Bearbeitung ihrer eigenen Daten zu informieren und zum Beispiel falsche Inhalte zu berichtigen.

Gemäss der Statistik der Landeskanzlei zum Öffentlichkeitsprinzip in der kantonalen Verwaltung wurden im Berichtsjahr nur wenige Gesuche um Zugang zu Informationen bei der kantonalen Verwaltung eingereicht:

- Direktion für Bildung, Kultur und Sport: 2 (1 gutgeheissen, 1 abgewiesen, noch nicht rechtskräftig)
- Direktion für Bau und Umwelt: 7 (1 gutgeheissen, 1 teilweise gutgeheissen, 5 abgewiesen)
- Direktion für Finanzen und Kirchen: 0
- Direktion für Sicherheit: 4 (2 gutgeheissen, 2 abgewiesen)
- Direktion für Volkswirtschaft und Gesundheit 4 (2 gutgeheissen, 2 abgewiesen)
- Landeskanzlei: 0

Im Falle eines Zugangsgesuchs muss das öffentliche Organ prüfen, ob die im IDG vorgesehenen Einschränkungs- und Verweigerungsgründe einen Zugang zu Informationen ganz oder teilweise verhindern. Je nach Dokument kann diese Abklärung aufwendig sein.

IV. KONTROLL-TÄTIGKEIT

Die Überwachung der datenschutzrechtlichen Vorgaben ist eine Compliance-Aufgabe der datenbearbeitenden Behörden. Neben dieser Selbstkontrolle setzt das Datenschutzrecht unabhängige Aufsichtsbehörden ein, die Kontrollen bei den Behörden durchführen. Diese Kontrollen sind ein Ausgleich dafür, dass die verwaltungsinternen Prozesse der Erfassung, Verarbeitung und Weitergabe von Daten für die betroffenen Bürgerinnen und Bürger häufig nicht transparent sind.

Bei ihren unabhängigen Kontrollen geht die Datenschutzbeauftragte ergebnisoffen vor und orientiert sich an den potenziellen Risiken eines Datenbearbeitungsprozesses. Sie sucht nicht den «Datenskandal», sondern prüft, ob Vorkehrungen getroffen werden, um solche «Skandale» zu vermeiden. Im Berichtsjahr stellte sie erneut fest, dass grundlegende Unterlagen bei den kantonalen Behörden

nicht oder unvollständig vorhanden sind. Dazu gehören beispielsweise eine Dokumentation der Hard- und Software, eine Liste der Datenbestände oder Informationen zu den Applikationsverantwortlichen. Solche Mängel stellen ein Risiko für die Organisation dar und können unnötige Kosten verursachen, wie das Projekt CliZ zeigte (vgl. II.III.). Es bleibt abzuwarten, ob die erforderlichen Inventare und Dokumentationen künftig nachgeführt und aktuell sind.

Die Kontrollen der Datenschutzbeauftragten führen als weitere positive Wirkung zu einer Sensibilisierung der öffentlichen Organe. Bereits kontrollierte Behörden lassen sich eher schon im Vorfeld eines Projekts beraten, oder sie lassen sich von der Datenschutzbeauftragten spezifisch schulen.

IV.I. ONLINE-ZUGRIFFE AUF DAS EDV-GRUNDBUCH

Die Datenschutzbeauftragte stellte 2013 bei einer Kontrolle fest, dass die Zivilrechtsverwaltung die Zugriffe auf das EDV-Grundbuch, das auch vertrauliche Angaben enthält, nicht vorschriftsgemäss kontrollierte (vgl. TB 2013, S. 14). Die Zivilrechtsverwaltung anerkannte den Mangel und leitete Massnahmen ein. Im Berichtsjahr erstellte sie, unterstützt von externen Fachkräften, ein Konzept, das ihr eine Kontrolle der Zugriffe auf das Grundbuch ermöglicht. Wieweit sich die Privatsphäre der Grundeigentümer dadurch schützen lässt, wird die Praxis zeigen.

IV.II. STADTVERWALTUNG LIESTAL: ANMELDUNGS-PROZESS FÜR ZUZIEHENDE

Personen, die in eine Baselbieter Gemeinde zuziehen, sind verpflichtet, sich innerhalb einer bestimmten Frist bei der Einwohnerkontrolle des neuen Wohnortes anzumelden. Bei der Anmeldung erhebt diese zahlreiche Personendaten zu den neuen Einwohnerinnen und Einwohnern und erfasst sie im kommunalen Einwohnerregister und zum Teil auch im kantonalen Personenregister arbo.

Im Berichtsjahr prüfte die Datenschutzbeauftragte bei der Einwohnerkontrolle der Stadtverwaltung Liestal, ob diese die gesetzlichen Anforderungen an die Datenerhebung beim Zuzug erfüllt. Sie stellte fest, dass die Datenbearbeitung durch die Einwohnerkontrolle in den meisten Punkten gesetzeskonform war und dass sich die Mitarbeitenden der Sensitivität dieser Daten bewusst waren. Die Datenschutzbeauftragte beanstandete indessen, dass Angaben zu Religionszugehörigkeiten und zu beruflichen Tätigkeiten der sich anmeldenden Personen nicht gesetzeskonform erfasst wurden. Sie stellte zudem fest, dass die Betroffenen über das Recht, ihre Daten zu sperren, unzureichend informiert wurden. Die Stadtverwaltung erkannte den Handlungsbedarf und setzte die empfohlenen Massnahmen unverzüglich um.

IV.III. FALLDOSSIERS UND INFORMATIONSSICHERHEIT BEIM SCHULPSYCHOLOGISCHEN DIENST

Der Schulpsychologische Dienst (SPD) bearbeitet zahlreiche sensitive Daten, beispielsweise von Schülerinnen und Schülern in speziellen Lebenssituationen, und tauscht sie mit anderen Institutionen aus. Im Auftrag der Datenschutzbeauftragten kontrollierte im Berichtsjahr eine Firma verschiedene Aspekte der Datenbearbeitung durch den SPD. Im Fokus stand, wie der SPD die personenbezogenen Falldossiers führte und ob eine Applikation zur Bearbeitung von Personendaten die Anforderungen an die Informationssicherheit erfüllte.

Die Kontrolle ergab, dass die gesetzlichen Vorgaben zu Informationssicherheit und Datenschutz in den untersuchten Bereichen mehrheitlich gut erfüllt sind und insgesamt ein gutes Bewusstsein für Datenschutz besteht. Handlungsbedarf zeigte sich bei der Informationssicherheit. Der SPD erkannte diesen und setzte einige der empfohlenen Massnahmen bereits im Berichtsjahr um.

IV.IV. INFORMATIONSSICHERHEIT VON MULTIFUNKTIONSGERÄTEN

Statt dezentrale Drucker, Fotokopierer, Faxgeräte und Scanner verwendet die kantonale Verwaltung zunehmend Multifunktionsgeräte – im Berichtsjahr bereits rund 450. Mit Multifunktionsgeräten lassen sich Druckaufträge und eingescannte Dokumente zwischenspeichern. Je nach Konfiguration werden die zwischengespeicherten Dokumente, die auch vertrauliche Daten beinhalten können, nicht angemessen geschützt und gelöscht. Weil die Multifunktionsgeräte zudem über einen Internetzugang und über Massenspeichermedien verfügen, verschärft sich das Risiko für die Informationssicherheit.

Die Datenschutzbeauftragte prüfte im Berichtsjahr die Informationssicherheit der Multifunktionsgeräte; der Bericht wird 2015 erstellt.

IV.V. INFORMATIONSSICHERHEIT BEI E-PERSONALDOSSIERS

Die Personaldossiers der Kantonsangestellten werden elektronisch geführt, und zwar mit dem SAP-Modul SAP HCM. Personaldossiers enthalten zahlreiche und teilweise sensitive Personendaten. Bei der elektronischen Bearbeitung stellen sich Fragen zur Informationssicherheit und zu den damit verbundenen organisatorischen und technischen Massnahmen zum Schutz der Ressourcen.

Für die Klärung dieser Fragen beauftragte die Datenschutzbeauftragte eine Firma, weil sie nicht über vertieftes SAP-Know-how verfügt.

Wegen der unklaren Zuständigkeiten der zahlreichen Leistungserbringer war es aufwendig, die für die Kontrolle erforderlichen Informationen zu beschaffen. Dies verlängerte die Kontrollarbeit und verursachte Mehrkosten. Die Datenschutzbeauftragte erwartet den Bericht im kommenden Jahr.

IV.VI. SENSITIVE DATEN IN EINEM ALTERS- UND PFLEGEHEIM

Die Gemeinden sind verpflichtet, für eine ausreichende stationäre Betreuungs- und Pflegestruktur ihrer Einwohnerinnen und Einwohner im Alter zu sorgen. Sie können private gemeinnützige Institutionen damit betrauen, so zum Beispiel das Zentrum für Pflege und Betreuung Mülimatt. Weil auch in diesem Alters- und Pflegeheim zahlreiche sensitive Personendaten der Bewohnerinnen und Bewohnern bearbeitet werden, kontrollierte es die Datenschutzbeauftragte im Berichtsjahr gemeinsam mit einer Firma. Im Fokus der Kontrolle standen das elektronische Abklärungssystem BESA, mit dem unter anderem die Pflegestufe ermittelt wird, und die elektronische Pflegedokumentation easyDOK. Der Bericht wird im kommenden Jahr vorliegen.

V. STELLUNGNAHMEN

Im Berichtsjahr verfasste die Datenschutzbeauftragte keine eigenen Vernehmlassungen zu Bundesgesetzen, sondern schloss sich der Meinung von Privatim, der Vereinigung der schweizerischen Datenschutzbeauftragten, an. Privatim äusserte sich zum Bundesgesetz über Geldspiele, zum Erwachsenenschutzrecht und zum Informationssicherheitsgesetz des Bundes[5].

Die Datenschutzbeauftragte äusserte sich aus datenschutzrechtlicher Sicht zu folgenden Themen: Public Private Partnership SAP, Umgang mit Personaldaten, Teilrevision Anmelde- und Registergesetz und -verordnung, Bedrohungsmanagement, Anschluss an das kantonale Personenregister arbo, Mammografie-Screening, Teilrevision Gemeindegesetz, Revision Benutzungsreglement Informatikmittel, Vertrag zur Behindertenhilfe, Verordnung zum Polizeigesetz, Teilrevision Sozialhilfegesetz, Arbeitnehmerschutz, Gewerbeparkkarte, Vorlage zur finanziellen Steuerung, fürsorgerische Unterbringung, Internes Kontrollsystem und Schulsozialdienst.

Die Datenschutzbeauftragte stellte fest, dass ihre rechtlichen Hinweise mehrheitlich berücksichtigt wurden. Ihre Stellungnahmen zum Informatikteil der

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

geplanten Vorhaben wurden indessen oft erst nach mehrmaligem Nachfragen beachtet.

Im Berichtsjahr fand eine Totalrevision des Benutzungsreglements Informatikmittel statt. Die Datenschutzbeauftragte brachte im Mitberichtsverfahren zahlreiche Verbesserungsvorschläge ein, die in der endgültigen Fassung grösstenteils berücksichtigt sind.

In eigener Sache äusserte sich die Datenschutzbeauftragte zum Bericht der landrätlichen Geschäftsprüfungskommission (GPK), die sich mit der Datenschutzbehörde beschäftigte. Wegen ihres gesetzlichen Auftrags und der funktionellen Unabhängigkeit der Datenschutzbehörden[6] konnte sich die Datenschutzbeauftragte nicht mit allen Empfehlungen der GPK einverstanden erklären.

6] Vgl. Gutachten von Prof. Dr. iur. Isabelle Häner, Unabhängigkeit der Aufsichtsbehörden, Umsetzung am Beispiel der Datenschutzaufsicht des Kantons Zürich, Zürich/Basel/Genf 2008

VI. ÖFFENTLICHKEITSARBEIT

Die Datenschutzbeauftragte startete im Berichtsjahr die Überarbeitung älterer Merkblätter. Anlässlich des kantonalen Sicherheitstags zum Thema Cloud Computing (s. VI.II.a) erhielten die Teilnehmenden ihr aktualisiertes Merkblatt zu diesem Thema. Abrufbar ist es auf ihrer Website. Sie stellte insgesamt fest, dass Informationen auf der Website meist nur aufgrund ihrer Hinweise abgerufen werden.

VI.I. MEDIENKONTAKTE UND PUBLIKATIONEN

Im Vergleich zu den Vorjahren unterhielt die Datenschutzbeauftragte im Berichtsjahr weniger Kontakte mit Medienvertretenden. Die Datenschutzbeauftragte beantwortete eine Medienanfrage zur Nutzung von Facebook durch Behörden und eine zum Einsatz von Sicherheitsfirmen in Gemeinden.

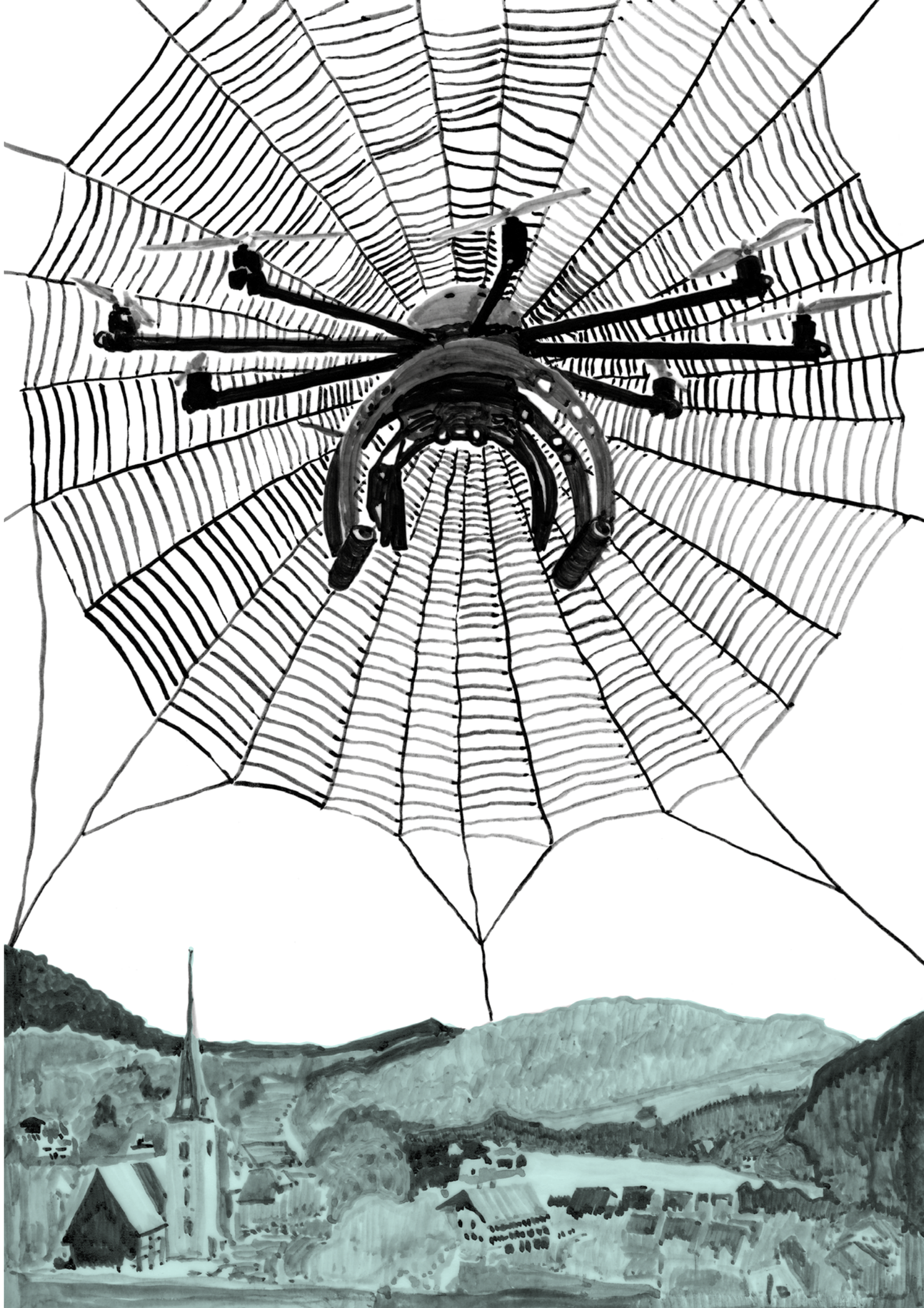
VI.II. KURSE UND REFERATE

Im Berichtsjahr führte die Datenschutzbeauftragte elf Schulungen durch. Dass sie jeweils auf die bereichsspezifischen Fragestellungen eingehen konnte, bedingte zeitintensive Vorbereitungen. Wie jedes Jahr schulte sie Lernende, die beim Kanton eine kaufmännische Ausbildung absolvieren, und pflegte den Austausch mit angehenden Polizistinnen und Polizisten sowie mit Polizeiassistentinnen und -assistenten. Zudem führte sie die Kurse des Personalamts zum Datenschutz und zum Öffentlichkeitsprinzip durch. Dazu kamen Referate vor Schulleitungen, vor Inspektorinnen und Inspektoren im Bereich Schwarzarbeitsbekämpfung sowie vor einer Landratsfraktion. Die Rückmeldungen der Teilnehmenden waren durchwegs positiv, und auch für die Datenschutzbeauftragte war der Austausch mit den unterschiedlichen Gruppen wertvoll.

Die Datenschutzbeauftragte bot erneut an, im Rahmen der Kaderschulung kurz über die Belange des Datenschutzes und der Informationssicherheit zu informieren. Obwohl vom Personalamt gut organisiert, kamen diese Schulungen wegen geringer Anmeldezahlen nicht zustande.

VI.II.a KANTONALER SICHERHEITSTAG

Die Sicherheitsverantwortlichen der Finanz- und Kirchendirektion organisieren jährlich den kantonalen Sicherheitstag, der das Bewusstsein für Informationssicherheit fördern soll. Das Thema im Berichtsjahr war Cloud Computing (vgl. VI.I.). Die Datenschutzbeauftragte bewirkte bei der inhaltlichen Gestaltung, dass zusätzlich zum Nutzen der modernen Technologie die rechtlichen und technischen Sicherheitsaspekte und Risiken angemessen erörtert wurden.



VII. KANTONALE, NATIONALE UND INTERNATIONALE ZUSAMMENARBEIT

Die Datenschutzbeauftragte arbeitet so oft wie möglich mit Gruppen und Behörden zusammen, die sich mit Fragen des Datenschutzes und des Öffentlichkeitsprinzips beschäftigen. Dazu gehört ein regelmässiger Austausch mit Vertretenden der Informatikplanung und -koordination Basel-Landschaft und mit den kantonalen Sicherheitsbeauftragten. Zudem informiert sie beispielsweise die Finanzkontrolle über ihr Prüfprogramm und einzelne Feststellungen. Oberstes Ziel dieser Zusammenarbeit ist die effiziente Nutzung vorhandener Synergien. Angesichts des vielfach grenzüberschreitenden Austauschs kann sich die Datenschutzbeauftragte indessen nicht auf innerkantonale Belange beschränken.

VII.I. AUSTAUSCH MIT DEN KANTONALEN SICHERHEITSBEAUFTRAGTEN

Die Bedeutung der Informationssicherheit für einen wirksamen Datenschutz steigt mit der rasanten technologischen Entwicklung. Die Datenschutzbeauftragte pflegt deshalb mit hoher Priorität den Kontakt und den Austausch mit den für die Informationssicherheit zuständigen Personen im Kanton. Ihre Mitarbeitenden, die sich mit Informatikfragen beschäftigen, beteiligten sich auch im Berichtsjahr an Besprechungen der Informationssicherheitsbeauftragten der Direktionen.

VII.II. PRIVATIM

Die Datenschutzbeauftragte ist Mitglied der Vereinigung der schweizerischen Datenschutzbeauftragten (Privatim). Anlässlich der Frühjahrskonferenz in Winterthur beschäftigte sich Privatim mit der Wirksamkeit und Effizienz von Aufsichtsbehörden. Die Konferenz im Herbst in Zug widmete sich dem Thema «Datenschutz im Gesundheitswesen». Die Datenschutzbeauftragte war an beiden Konferenzen vertreten.

VII.III. EIDGENÖSSISCHER DATENSCHUTZ- UND ÖFFENTLICHKEITSBEAUFTRAGTER

Bei Fragen, die in den Zuständigkeitsbereich des Bundes fallen, pflegt die Datenschutzbeauftragte die Zusammenarbeit mit dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) fallweise und informell.

Die «Koordinationsgruppe der schweizerischen Datenschutzbehörden im Rahmen der Umsetzung des Schengener Assoziierungsabkommens» traf sich im Berichtsjahr beim EDÖB zu zwei Sitzungen. Die Treffen dienten dem Austausch über SIS-Kontrollen des Bundes und der Kantone. Informiert wurde zudem über die aktuellen Entwicklungen des Schengen-Dossiers in Brüssel. Im Berichtsjahr führte eine Expertengruppe der Schengen-Staaten erneut eine Schengen-Evaluation der Schweiz durch, über deren Verlauf grob informiert wurde. Der Kanton Basel-Landschaft musste lediglich schriftliche Fragen beantworten und wurde nicht vor Ort geprüft. Es ist vorgesehen, dass die Kantone 2015 von der Konferenz der Kantonsregierungen über die Ergebnisse der Evaluation informiert werden.

VII.IV. ARBEITSGRUPPE INFORMATION AND COMMUNICATION TECHNOLOGY

Die Arbeitsgruppe Information and Communication Technology (AG ICT) fördert den Austausch zwischen den Informatikspezialistinnen und -spezialisten der schweizerischen Datenschutzbehörden. Im Berichtsjahr beschäftigte sie sich primär mit der Verschlüsselung von E-Mails. Die Verschlüsselung der E-Mail-Kommunikation unter den Mitgliedern wurde erfolgreich mit kostenlosen S/MIME-Zertifikaten auf der bestehenden E-Mail-Infrastruktur – d. h. mit Windows 7 und Outlook 2010 – durchgeführt.

VIII. AUSBLICK

Die Jahresplanung für 2015 der Datenschutzbeauftragten sieht erneut diverse Kontrollen vor. Zudem wird die Implementierung der Vorabkontrolle im Vordergrund stehen. Und schliesslich soll im Sinne der «Hilfe zur Selbsthilfe» der Webauftritt der Datenschutzbeauftragten weiter ausgebaut werden.

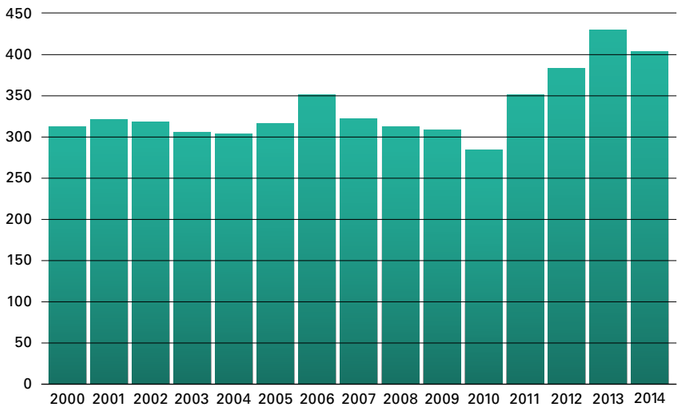
Die rasante Entwicklung der Informationstechnologie, die Veränderung der gesellschaftlichen Rahmenbedingungen und die Internationalisierung sind treibende Kräfte im Umfeld des Datenschutzes. Sie bedingten und bedingen neue Lösungen in den Bereichen Datenschutz und Informationssicherheit. Auf europäischer Ebene wird seit Längerem geprüft, wie das Datenschutzrecht der aktuellen Situation angepasst werden kann. Auf nationaler Ebene prüft der Bundesrat den Revisionsbedarf des Bundesdatenschutzgesetzes. Und die Bundespolitik befasst sich mit parlamentarischen Vorstössen zur digitalisierten Gesellschaft, beispielsweise mit der parlamentarischen Initiative zum Schutz der digitalen Identität der Bürgerinnen und Bürger[7].

Ob und wann die angedachten Änderungen im Datenschutzrecht der Dynamik der technologischen Entwicklung gerecht werden, wird sich zeigen. In der Zwischenzeit müssen die Chancen und Risiken des Einsatzes neuer Technologien anhand der geltenden Regelungen sorgfältig geprüft und grundrechtskonforme Lösungen erarbeitet werden. Die Datenschutzbeauftragte wird die Behörden bei dieser Aufgabe weiterhin unterstützen.

7] Parlamentarische Initiative von NR Fathi Derder (FDP) zum Schutz der digitalen Identität von Bürgerinnen und Bürgern, eingereicht am 20. Juni 2014 (14.434)

ANHANG

GESCHÄFTE



ART DER GESCHÄFTE