

3. Tätigkeitsbericht Datenschutzbeauftragter 2018

Antrag der Geschäftsleitung vom 29. August 2019

KR-Nr. 282/2019

Ratspräsident Dieter Kläy: Zu diesem Geschäft begrüsse ich ganz herzlich den Datenschutzbeauftragten Bruno Baeriswyl. Der Behandlungsablauf für den Tätigkeitsbericht des Datenschutzbeauftragten sieht wie folgt aus: Die Eröffnung macht der Referent der Geschäftsleitung, Roman Schmid, während zehn Minuten. Danach hat der Datenschutzbeauftragte, Bruno Baeriswyl, ebenfalls für zehn Minuten das Wort. Danach folgen die Fraktionssprecherinnen und -sprecher mit ebenfalls je zehn Minuten Redezeit. Darauffolgend haben die übrigen Mitglieder des Rates je fünf Minuten Redezeit. Danach schliessen der Datenschutzbeauftragte und der Referent der Geschäftsleitung mit einer Replik die Debatte.

Roman Schmid (SVP, Opfikon), Referent der Geschäftsleitung: Im Berichtsjahr 2018 konnten 600 Beratungen durchgeführt werden. Dies entspricht einer Zunahme von 40 Fällen oder knapp 7 Prozent. Aufgrund der weiter angestiegenen Zahl der Beratungen und der dadurch gebundenen Ressourcen konnte das angestrebte Ziel von 40 Kontrollen nicht eingehalten werden. Beim Abarbeiten von Pendenzen und bei der Durchführung von Kontrollen wird nach einer Prioritätenliste vorgegangen.

Mit Blick in die Zukunft kann davon ausgegangen werden, dass sich die Beratungs- und Kontrolltätigkeit des Datenschutzbeauftragten weiter erhöhen wird. Der Kantonsrat sollte sich Gedanken darüber machen, wie viele Ressourcen er aufgrund der fortschreitenden Digitalisierung dem Datenschutzbeauftragten bereitstellen möchte.

Erstmals konnte im Jahr 2018 an der ZHAW (*Zürcher Hochschule für Angewandte Wissenschaften*) ein CAS-Weiterbildungskurs (*Certificate of Advanced Studies*) für Datenschutzverantwortliche angeboten und durchgeführt werden. Rund 25 Teilnehmerinnen und Teilnehmer wurden in einem kompakten Lehrgang von rund vier Monaten in Datenschutzrecht, IT-Risiken und Informationssicherheit, in Informations-Governance, Datenschutz-Compliance und Datenschutz-Management geschult. Die Kursteilnehmerinnen und -teilnehmer bestanden je zur Hälfte aus Verwaltungsangestellten und aus Angestellten der Privatwirtschaft.

Aufgrund der Mitgliedschaft der Schweiz bei Schengen-Dublin muss auch der Kanton Zürich Anpassungen der Gesetzgebung an die EU-Richtlinien im kantonalen IDG (*Gesetz über die Information und den Datenschutz*) vornehmen. Dies hauptsächlich in den Bereichen Polizei und Justiz. Die regierungsrätliche Vorlage beinhaltete vor allem Ergänzungen, welche in die Wegleitung der Konferenz der Kantonsregierungen (*KdK*) aufgenommen wurden. Die Anforderungen des KdK-Leitfadens wurden gemäss der Stellungnahme des Datenschutzbeauftragten gut aufgenommen und pragmatisch umgesetzt. In der kantonsrätlichen Vorlage wurden allerdings materielle Änderungen vorgenommen, welche nicht konform zu

den Vorgaben der Richtlinien sind. Es fehlt die verpflichtende Bestimmung, dass sich eine Bürgerin oder ein Bürger mit einer Beschwerde an den Datenschutzbeauftragten wenden kann, der sich damit in einem förmlichen Verfahren zu befassen hat. Eine Verfügung zur Anpassung der Datenbearbeitung soll nur bei einer erheblichen Verletzung möglich sein. Zudem hat der Kantonsrat die Möglichkeit gestrichen, dass der Datenschutzbeauftragte vorsorgliche Massnahmen erlassen kann. Dies sind drei wichtige Bestimmungen, um die Freiheitsrechte der Bürgerinnen und Bürger in Sachen Digitalisierung zu schützen und Datenschutzprobleme effizient zu behandeln. Die Vorlage – Sie wissen es – wurde diesen Monat in diesem Rat behandelt und die erste Lesung abgeschlossen.

Um die Einhaltung der Anforderungen beim Datenschutz in rechtlicher, organisatorischer und sicherheitstechnischer Hinsicht zu beurteilen, wurden auch im Berichtsjahr 2018 verschiedene Datenschutz-Reviews durchgeführt. Geprüft wurden Gemeinden, Spitäler und IT-Dienstleister. Daneben erfolgten Checks von Webseiten. Diese Kontrollen sind wichtig, zumal sich erneut gezeigt hat, dass Mängel in der Informationssicherheit bestehen. Im Kanton ist ein einheitliches und ausreichendes Sicherheitsniveau anzustreben.

Neu wurde ab dem Berichtsjahr 2018 ein Nachkontrollprozess eingeführt, womit die Wirkung der durchgeführten Kontrollen zeitnah und vertieft evaluiert werden kann. Die Umsetzung wird monatlich kontrolliert, indem die geprüften Organe mit einem Schreiben auf die fälligen Massnahmen hingewiesen werden. Somit kann dem Umstand entgegengewirkt werden, dass die vorgeschlagenen Massnahmen in der Vergangenheit bei gerade mal 50 Prozent umgesetzt wurden.

Bürgerinnen und Bürger wollen sich immer mehr über ihr digitalisiertes Umfeld informieren. Aus diesem Grund veröffentlichte der Datenschutzbeauftragte auch im Berichtsjahr wieder einige Informationen und Hilfsmittel, wie zum Beispiel die Broschüre «Meine Rechte und Pflichten – Informationen zum Spitalaufenthalt».

Der jetzige Stelleninhaber Bruno Baeriswyl wird im Frühjahr 2020 pensioniert werden. Aus diesem Grund hat die Geschäftsleitung des Kantonsrates eine Findungskommission eingesetzt, welche geeignete Kandidatinnen und Kandidaten für die Wahl der Nachfolge vorschlagen soll. Die öffentliche Wahl soll im Dezember dieses Jahres stattfinden.

Eine weitere Änderung ist der Totalrevision des Kantonsratsgesetzes geschuldet. Gemäss heutigem Gesetz übt die Geschäftsleitung die Oberaufsicht über den Datenschutzbeauftragten aus. Neu ist ab 1. Mai 2020 die Geschäftsprüfungskommission zuständig.

Die Geschäftsleitung dankt dem Datenschutzbeauftragten und seinen Mitarbeitenden für ihren Einsatz und die gute, informative Zusammenarbeit. Im Namen der einstimmigen Geschäftsleitung beantrage ich Ihnen, den Tätigkeitsbericht 2018 des Datenschutzbeauftragten zu genehmigen.

Bruno Baeriswyl, Datenschutzbeauftragter des Kantons Zürich: Ich danke Ihnen für Ihr Interesse für den Datenschutz. Auch im vergangenen Jahr hat uns insbesondere die Digitalisierung der kantonalen Verwaltung wie auch der Gemeinden

sehr stark beschäftigt. Sie bringt zusätzliche Risiken für die persönliche Freiheit und die Privatsphäre der Bürgerinnen und Bürger. Und wir sehen aus Umfragen, dass sich die Bürgerinnen und Bürger immer mehr Sorgen machen, wie mit ihren persönlichen Daten beim Staat umgegangen wird.

Die Gesetze legen die Leitplanken, wie beim Datenschutz und bei der Informationssicherheit vorzugehen ist. Doch obwohl immer mehr sensitive Daten bearbeitet werden, müssen wir leider feststellen, dass vielfach die notwendigen Massnahmen zum Schutz dieser Daten fehlen. Fast täglich kann man in den Zeitungen lesen, dass wieder irgendwelche Personendaten im Internet frei verfügbar sind, beispielsweise letzte Woche Gesundheitsdaten: 16 Millionen Datensätze in 52 Ländern, davon auch 1500 Datensätze in der Schweiz. Unsere Kontrollen im Jahr 2018 haben gezeigt, dass auch im Kanton Zürich solche Vorfälle nicht auszuschliessen sind.

Wir haben insbesondere auch Kontrollen im Gesundheitswesen gemacht und haben dort bei grossen Spitälern die Klinikinformationssysteme geprüft. Wir mussten feststellen, dass Daten unverschlüsselt gespeichert werden oder dass sensitive Gesundheitsdaten unverschlüsselt per E-Mail versandt werden. Es gibt auch vielfach keine Vorgaben für sichere Passwörter oder ungeschützte Testsysteme arbeiten mit echten Daten. Vielfach fehlen aber auch Schulungsmassnahmen für das Personal, wie es eben korrekt mit Daten umzugehen hat. Nur dank unseren Kontrollen werden solche Schwachstellen erkannt und hoffentlich auch rechtzeitig beseitigt. Wir haben im letzten Jahr rund 100 Massnahmen mit hoher oder mittlerer Priorität empfohlen und, wie Sie gehört haben, werden nur rund 50 Prozent dieser Massnahmen auch umgesetzt. Dies ist das Ergebnis aus 25 Kontrollen. Es fehlen uns die Ressourcen, um hier mehr Kontrollen zu machen.

Wir erhalten aber auch direkt von Amtsstellen Meldungen über Datenschutzverletzungen. Dies erlaubt es uns, zusammen mit den Amtsstellen auch die notwendigen Massnahmen in die Wege zu leiten. So wurden beispielsweise Rechnungen falsch adressiert oder das Verzeichnis von Bewerberinnen und Bewerbern war offen im Internet zugänglich oder eine fehlerhafte Webkonfiguration hat dazu geführt, dass persönliche Daten während drei Wochen ungeschützt im Internet waren. Neben diesen sicherheitstechnischen Fragen beschäftigen wir uns natürlich auch mit sehr viel datenschutzrechtlichen Fragen. Hier geht es vor allem um die Frage der Verhältnismässigkeit, beispielsweise: Dürfen Gemeinderäte, also Exekutivmitglieder, in die Mitarbeiterbeurteilungen von Gemeindeangestellten Einsicht haben, in diejenigen von allen oder eben nur in diejenigen, die ihrem Ressort zugeteilt sind? Oder zum Beispiel die Schulen: Sie haben definitive Schulausschlüsse von ausländischen Kindern an das Migrationsamt zu melden. Hier stellt sich auch die Frage: Was ist dann der Inhalt einer solchen Meldung? Oder wir haben auch einen Fall gehabt, in dem es um die Publikation von Baugesuchen geht. Hier wird natürlich auch die Adresse des Bauherrn publiziert und die Frage stellt sich: Wie ist es mit der Publikation dieser Adresse, wenn die betroffene Person eine Sperre ihrer Daten bei der Einwohnerkontrolle hinterlegt hat?

Technologie kommt auch in die Haushalte. Mit digitalen Stromzählern, also sogenannten Smartmetern, kann der Einzelne sehr genau überwacht werden, was er

in seinen eigenen vier Wänden tut. Auch hier haben wir Vorgaben erarbeitet, dass solche Daten nur anonymisiert ausgewertet werden dürfen und nur beschränkt im Zugriff von anderen Stellen sein dürfen. Die Digitalisierung in Kanton und Gemeinden bringt komplexere Informatiksysteme. Sie zeigt auch eine immer grössere Abhängigkeit von der Informationstechnologie in der Verwaltung, und die Datenbearbeitungen über die Bürgerinnen und Bürger werden umfassend. Dabei fehlt vielfach das Bewusstsein, dass hier eben auch entsprechende Datenschutz und Sicherheitsmassnahmen zu treffen sind. Darum ist die Erwartungshaltung der Bevölkerung, wie ich es bereits erwähnt habe, sehr klar: Eine Studie im Auftrag der Staatskanzlei und des VZGV (*Verein Zürcher Gemeindeschreiber und Verwaltungsfachleute*) über die Bedarfserhebung über das digitale Leistungsportfolio der Gemeinden hat klar gezeigt, dass die Bürgerinnen und Bürger einen hohen Wert auf den Schutz und die Sicherheit ihrer Daten legen. Dabei können sie durchaus differenzieren. Sie sehen auch, dass zum Beispiel ein digitales Beantragen von Jokertagen eben nicht die gleiche Sensitivität hat wie eine Datenbank mit den Steuerdaten. Auch hier gilt: Um den Ansprüchen der Bevölkerung gerecht zu werden, braucht es bei der Digitalisierung auch die entsprechenden Ressourcen beim Datenschutz. Datenschutz muss kein Thema sein, aber er braucht die volle Aufmerksamkeit. Die Wahrung der Freiheitsrechte auch bei einer umfassenden Digitalisierung muss das Ziel jedes demokratischen Rechtsstaates sein. Die Herausforderungen für den Datenschutz und die Sicherheit der Daten bleiben deshalb auch in Zukunft sehr hoch. In unmittelbarer Zukunft etwa die Einführung des elektronischen Dossiers im Kanton Zürich oder die Frage der Anonymisierung der Daten für die Forschung oder ganz generell das Cloud-Computing, bei dem nicht mehr transparent ist, wo sich die Daten überhaupt befinden. Ich danke Ihnen für Ihre Unterstützung für den Datenschutz und ich danke Ihnen für Ihre Aufmerksamkeit.

Hans-Peter Amrein (SVP, Küsnacht): Ich spreche nicht als Fraktionssprecher, es ist nicht mit meiner Fraktion abgesprochen.

Zuerst ein grosses Dankeschön an den Datenschutzbeauftragten und seine Mitarbeiter für die geleistete Arbeit im Berichtsjahr. Dennoch muss aber festgestellt werden, dass der Datenschutzbeauftragte auch im vergangenen Jahr enorme Sisyphusarbeit geleistet hat. Sinnbildlich kann das Ganze wohl mit einem frustrierten Bauern mit einem Stock in der Hand vor einem Hühnerstall mit zerbrochenen Fenstern verglichen werden. Nur handelt es sich beim Bauern um den Datenschutzbeauftragten des Kantons Zürich und beim Hühnerstall um die zu schützenden Bürger und staatlichen Netzwerke im Kanton Zürich, viele davon mit Apple-Computern und Cloudware ausgerüstet. Doch wer einen Apple-Computer und oder Cloudware benutzt, ist unweigerlich auf einem – meist amerikanischen Server – zu Hause. Und wer auf einem ausländischen oder fremden Server zu Hause ist, muss sich bewusst sein, dass er im Glashaus sitzt.

Gleiches betrifft das Hacken. Wer eine Schnittstelle mit einer fremden Plattform hat, ist den Hackern schlussendlich hilflos ausgeliefert. Und da helfen ultimo ratio auch keine noch so ausgefeilten Abwehr- und Antivirenprogramme, beschäftigen

doch die Grossmächte x tausende oder sogar zehntausende Mitarbeiter, welche tagein und tagaus nur eine Aufgabe haben: in fremde Netzwerke einzudringen und aus Trillionen von Daten für ihre Auftraggeber interessante Daten und Informationen herauszufiltern.

Je ein gröberer Ausreisser ist mir bei der Würdigung des Antrags der GL zu diesem Geschäft und dem Tätigkeitsbericht des Datenschutzbeauftragten über das Jahr 2018 aufgefallen: Im vorliegenden Bericht der Geschäftsleitung, verfasst durch den Referenten der Geschäftsleitung, stellt die GL fest, bei der Revision des IDG im Kanton Zürich seien materielle Änderungen vorgenommen worden, welche nicht konform seien mit der Richtlinie. Welche, sagt er aber nicht. Doch es handelt sich nicht um eine Richtlinie, wie es uns die GL verkaufen will, sondern es handelt sich um eine Wegleitung der Konferenz der Kantonsregierungen, KdK, und solche Wegleitungen sind zum guten Glück in unserem Kanton noch nicht rechtsverbindlich. Beim zweiten gröberen Ausreisser handelt es sich um die Feststellung des DSB (*Datenschutzbeauftragten*) betreffend die Datenschutzaufsicht beim Schengen-Informationen-System, SIS. Eine Stelle der EU verlange, dass die Durchsetzungsbefugnisse der Datenschutzbehörden gestärkt werden müsse. Ihnen solle das Recht verliehen werden, direkt rechtsverbindliche Entscheide zu treffen. Zu was nur schon Empfehlungen des DSB führen können, hat eine Feststellung des DSB zu den polizeilichen Überprüfungen von Neuzuzüglern im Jahre 2013 bewiesen. Die polizeiliche Überprüfung von Neuzuzüglern wurde für rund fünf Jahre im Kanton Zürich enorm erschwert, behindert oder sogar verhindert, bis dann im Jahre 2018, basierend auf einem Vorstoss des Sprechenden und Mitunterzeichnern, die Verordnung zu einem geänderten Polizeigesetz in Kraft trat. Diese beiden Beispiele beweisen, wie wichtig es ist, dass sich der Nachfolger oder die Nachfolgerin des derzeitigen DSB, welcher 2020 in die hoch verdiente Rente geht – er hat trotz aller Kritik enorme, fast unmenschliche Aufbauarbeit geleistet – mit dem Wesentlichen befasst. Der oder die neue Datenschutzbeauftragte soll keine neuen Fenster kitten und sich, wie der heutige DSB über die Herausforderungen der Datensicherheit und Clouds beschwerten, wie er dies im vorliegenden Bericht doziert, sondern darauf hinweisen, dass eine Verwaltung, welche mit Apple-Computern arbeitet und mit Clouds operiert, nie sicher arbeiten kann. Und Empfehlungen einer bürokratisierten EU-Behörde, welche mit einem löchrigen System arbeitet, können und dürfen nicht ernst genommen werden. Konzentration auf das Wesentliche, die Daten der Bürger und der Verwaltung schützen, das ist angesagt – und nicht weiter bürokratisieren und ausbauen.

Esther Guyer (Grüne, Zürich): Ich konzentriere mich jetzt auf das Unwesentliche: Dies ist ja jetzt der letzte Jahresbericht des Datenschutzbeauftragten Bruno Baeriswyl. Es wird ja sicher viele Verabschiedungen geben, aber für uns als Partei ist das wohl die einzige Möglichkeit, um ihm für seinen grossen Einsatz zu danken. Seine Tätigkeit fiel ja in eine extrem bewegte Zeit des digitalen Wandels. Mit dem Öffentlichkeitsprinzip musste ein zentrales und sehr wichtiges Recht unserer Bürgerinnen und Bürger umgesetzt werden. Die Digitalisierung stellt besondere Ansprüche an dieses Amt: Gute Vernetzung, ständige Weiterbildung und

sehr, sehr gute Kenntnisse der aktuellen internationalen Entwicklungen sowohl im rechtlichen als auch im Anwenderbereich sind dazu nötig. Bruno Baeriswyl erfüllt diese Anforderungen bestens. Er warnte die Schulen vor digitalen Medien, wie WhatsApp und Drop Box und machte Schülerinnen und Schüler auf die Gefahren beispielsweise durch den Kontrollverlust aufmerksam. Er hat begriffen, dass es mehr bringt, wenn ein Fachmann zu den Schülern spricht, als wenn die Eltern ständig mahnen oder gar verbieten. Anstatt ein Blättchen zu schicken, wie das die meisten machen, ist er persönlich hingegangen. Das unterstreicht die Ernsthaftigkeit seines Anliegens.

Für diese grossen und ständig wachsenden Aufgaben hat ihm die bürgerliche Mehrheit des Kantonsrates das Leben nicht gerade erleichtert. Das Stellenbegehren wurde jedes Jahr abgelehnt – jedes Jahr –, ja, nicht einmal befristete Stellen hat man ihm gesprochen. Dabei wäre es bitter nötig – Sie haben es gehört –, es fehlt in der Verwaltung an Sensibilität für die Datensicherheit. Und vor allem fehlt es auch in der Regierung an Sensibilität für die Datensicherheit. Man hat die Zusammenarbeit mit dem Datenschutzbeauftragten nicht gepflegt, sondern ihn eher missachtet. Das ist ein grosser Fehler, und man muss verlangen, dass sich das in Zukunft ändert.

Trotzdem wurde eine grosse Arbeit von hoher und höchster Qualität geliefert. Dafür danken wir Bruno Baeriswyl und wünschen ihm für die Zukunft alles Gute. Und ich persönlich hoffe, dass er weiterhin publiziert und sich einmischt und sich vernehmen lässt. Ich danke Ihnen.

Bruno Baeriswyl, Datenschutzbeauftragter des Kantons Zürich: Eigentlich wollte ich nichts mehr sagen, aber ich bedanke mich natürlich für das Votum von Esther Guyer. Und Herrn Amrein möchte ich beruhigen: Also bis April 2020 bin ich noch voll da (*Heiterkeit*).

Abstimmung

Der Kantonsrat beschliesst mit 168 : 0 Stimmen (bei 1 Enthaltung), dem Antrag der Geschäftsleitung zuzustimmen und den Tätigkeitsbericht 2018 des Datenschutzbeauftragten zu genehmigen.

Das Geschäft ist erledigt.