2. Tätigkeitsbericht der Datenschutzbeauftragten über das Jahr 2023
Antrag der Geschäftsprüfungskommission vom 22. August 2024
KR-Nr. 136/2024

Ratspräsident Jürg Sulser: Eintreten ist gemäss Paragraf 89 Kantonsratsgesetz obligatorisch. Wir haben freie Debatte beschlossen.
Zu diesem Geschäft begrüsse ich die Datenschutzbeauftragte Dominika Blonski recht herzlich bei uns.
Der Behandlungsablauf für den Tätigkeitsbericht der Datenschutzbeauftragten sieht wie folgt aus: Die Eröffnung macht die Referentin der GPK *(Geschäftsprüfungskommission)*, Edith Häusler, während zehn Minuten, und danach hat die Datenschutzbeauftragte, Dominika Blonski, ebenfalls für zehn Minuten das Wort. Daraufhin folgen die Fraktionssprecherinnen und -sprecher mit ebenfalls je zehn Minuten Redezeit. Darauffolgend haben die übrigen Mitglieder des Rates je fünf Minuten Redezeit. Danach schliessen die Referentin der GPK und die Datenschutzbeauftragte mit einer Replik die Debatte, natürlich nur, wenn sie das wünschen.

Edith Häusler (Grüne, Kilchberg), Referentin der Geschäftsprüfungskommission (GPK): Wie jedes Jahr stand die Datenschutzbeauftragte der GPK an der Sitzung vom 20. Juni 2024 im Rahmen ihres Tätigkeitsberichts Red und Antwort. Ihr umfangreiches Arbeitsfeld wurde ebenfalls öffentlich vorgestellt. Neben der Behandlung des Berichts befragte die GPK die Datenschutzbeauftragte speziell zur Organisation der Datenschutzbehörde, zum Personal, zur Wahrnehmung der Beratungs- und Aussichtstätigkeiten durch die Datenschutzbehörde, zu den KEF-Leistungsindikatoren *(Konsolidierter Entwicklungs- und Finanzplan)* sowie zum Umgang mit den Datenschutzvorfällen.
Die Datenschutzbeauftragten arbeiten online, dadurch können einzelne Themen mit audiovisuellen Inhalten ergänzt und erklärt werden, was zu einer besseren öffentlichen Sensibilisierung für Fragen des Datenschutzes beiträgt. Es wurden auch Kurzvideo-Sequenzen für die Sekundarstufe I und II erstellt, welche zu den verschiedensten Themen rund um den Datenschutz Auskunft geben. Im Berichtsjahr wurden erstmals 60 Kontrollen durchgeführt und damit die Vorgabe des Leistungsindikators gemäss KEF für diese Tätigkeit erfüllt.
Dominika Blonski führte aus, dass die Beratungen der Datenschutzbehörde vor allem Rechtsauskünfte umfassen. Diese können von kleinen, kurzen Anfragen von Bürgerinnen und Bürger bis hin zu langjährigen Begleitungen von einzelnen Institutionen reichen. Jedes Jahr verfolgt die Datenschutzbeauftragte im Rahmen ihrer Kontrolltätigkeit einen Schwerpunkt in einem Bereich, in dem besonders sensitive Daten bearbeitet werden. Im Berichtsjahr lag dieser bei den Alters- und Pflegezentren. Diese Institutionen bearbeiten viele schützenswerte Gesundheitsdaten. Die durchgeführten Kontrollen bei der repräsentativen Auswahl von rund

160 Alters- und Pflegezentren, die im Zuständigkeitsbereich der Datenschutzbeauftragten liegen, brachten einige grundlegende Mängel hervor. So erfolgte der Zugriff auf die Daten teilweise über unpersönliche Accounts mit allgemein bekannten Passwörtern, und starke Identifizierungsmechanismen, die bei der Bearbeitung von besonderen Personendaten Pflicht sind, fehlten.
Ein weiterer Entwicklungsschwerpunkt der Datenschutzbehörde gemäss KEF zielt auf die effiziente und wirksame Unterstützung der Verwaltung bei der Umsetzung von deren Digitalisierungszielen ab. Dazu berät sie die öffentlichen Organe in Datenschutzfragen, beurteilt datenschutzrelevante Vorhaben und nimmt Stellung zu Erlassen. Dabei hat die Zahl von Beratungen und Vorkontrollen in den vergangenen Jahren kontinuierlich zugenommen. Bei den Vorabkontrollen handelt es sich teilweise um sehr komplexe Projekte und sie laufen nach einem klar definierten Prozess ab: Zunächst muss das verantwortliche Organ der Datenschutzbehörde bestimmte Informationen zur Verfügung stellen. Dazu gehört eine Rechtsgrundlageanalyse sowie ein Informations-, Sicherheits- und Datenschutzkonzept. Basierend auf diesen Dokumenten, erarbeitet die Datenschutzbehörde eine Stellungnahme. Im Anschluss führt die Datenschutzbehörde, basierend auf ihren Ergebnissen, eine Beratung beim verantwortlichen Organ durch.
Die Aus- und Weiterbildung konnte auch im letzten Jahr auf hohem Niveau weitergeführt werden. Die Datenschutzbeauftragte stärkt mit ihren Weiterbildungs- und Informationssegmenten die Kompetenzen bei den Mitarbeitern der öffentlichen Organe. Sie werden befähigt, ihre Verantwortung in der Digitalisierung wahrzunehmen und die Anforderungen des Datenschutzes und der Informationssicherheit in ihrem Alltag zu meistern. Ein Beispiel, welches immer wieder zu reden gibt: Öffentliche Organe dürfen nur Personendaten verwenden, welche absolut notwendig sind. Jede Bearbeitung von Daten ist ein Eingriff in die Grundrechte. Bevor Cloud-Dienste benützt werden, muss vorab abgeklärt werden, ob der Eingriff in die Grundrechte verhältnismässig ist.
Im Jahr 2023 legten verschiedene Gemeinde- und Stadtverwaltungen ihre Projekt zur Einführung von «Microsoft 365» *(Softwarepaket)* der Datenschutzbeauftragten zur Vorabkontrolle vor. Und diese zeigte dann eben auch, dass nicht alle Grundrechte geschützt sind. Der Schutz vor Grundrechtsverletzungen ist in den Gemeinden eine wichtige Aufgabe, denn das weckt Vertrauen in der Bevölkerung. Eine Liste von Sozialhilfeempfängerinnen- und -empfängern darf deshalb zum Beispiel nur in der Excel-Cloud-Variante geführt werden, wenn die Personendaten verschlüsselt werden und das Schlüsselmanagement bei den Gemeinden bleibt. Dasselbe gilt, wenn eine Steuerveranlagungsverfügung in Microsoft Exchange online abgelegt werden soll. Die Datenschutzbeauftragte informierte die Gemeinden auch über die Verwendung der Rahmenverträge der schweizerischen Informatikkonferenz mit Microsoft. Der Rahmenvertrag kann allerdings nur ab 250 Nutzerinnen und Nutzern eingesetzt werden, und das ist ein Problem für kleinere Gemeinden.
Es gäbe unzählige Beispiele, die im Tätigkeitsbericht der Datenschutzbeauftragten aufgeführt sind, sehr spannende, interessante Themen, auf die wir vielleicht

im Alltag gar nicht unbedingt kämen. Lesen Sie den Tätigkeitsbericht, wenn Sie es noch nicht gemacht haben, es lohnt sich.
Die kantonale Datenschutzbehörde beaufsichtigt die Datenbearbeitung der kantonalen Verwaltung, wie ich schon gesagt habe, der Gemeinden und der übrigen Behörden und öffentlichen Einrichtungen im Kanton, um die Privatsphäre der Einwohnerinnen und Einwohner sicherzustellen. Zudem berät sie die Mitarbeiterinnen und Mitarbeiter der öffentlichen Organe im Kanton sowie Privatpersonen bei Fragen zu Datenbearbeitungen dieser Organe. Aus Sicht der GPK ist es zentral, dass die Datenschutzbehörde dies weiterhin vollständig unabhängig tun kann und die Anliegen des Datenschutzes mit den gesetzlich vorgesehenen Mitteln konsequent einbringt; dies im stetigen Austausch mit den datenbearbeitenden Stellen und nötigenfalls auch gegen deren Widerstand.
Die GPK dank Dominika Blonski und ihrem Team für ihre wichtige Arbeit zugunsten der Bevölkerung des Kantons. Sie beantragt einstimmig, den Tätigkeitsbericht 2023 der Datenschutzbeauftragten zu genehmigen. Besten Dank.

Dominika Blonski, Datenschutzbeauftragte des Kantons Zürich: Ich freue mich, heute wieder bei Ihnen zu sein. Einmal pro Jahr darf ich Ihnen den Tätigkeitsbericht des vergangenen Jahres vorstellen. Sie behandeln diesen heute und ich werde ein paar Worte an Sie richten und insbesondere auch die Vielfalt unserer Tätigkeit aufzeigen.
Unser Tätigkeitsbericht ist wiederum vollständig online erschienen. Er ist nur online zugänglich, kann als PDF bei Bedarf heruntergeladen werden, ist aber im Grundsatz ein Online-Format und hat deshalb auch die Möglichkeit, viele Erklärvideos, audiovisuelle Kommunikation einzubinden. Und die Idee davon ist, dass es möglichst weit verbreitet wird, und das scheint sehr gut zu funktionieren.
Die digitale Transformation beschäftigt uns immer noch und wird uns noch lange beschäftigen. Das führt aus datenschutzrechtlicher Perspektive dazu, dass die Projekte, die in diesem Zusammenhang entstehen, immer komplexer werden und auch die Risiken für den Datenschutz steigen. Was ist da wichtig? Das Vertrauen der Bevölkerung. Die Bevölkerung muss sich darauf verlassen können, dass die öffentlichen Institutionen, die im Rahmen dieser Digitalisierung Daten bearbeiten, das auch wirklich grundrechtskonform tun. Ich hatte eine kurze Rückmeldung eines Referenten an einer unserer Veranstaltungen. Er ist Informatiker und war etwas erstaunt. Als er im Nachgang zu mir gekommen ist, hat er gesagt: «Wieso sprecht ihr über dieses Vertrauen? Das ist doch völlig selbstverständlich. Ich muss mich doch einfach darauf verlassen können, dass der Staat seinen Job gut macht.» Das war für mich ein sehr positives Feedback. Die Bevölkerung wünscht sich das beziehungsweise darf das einfordern, und das ist die Aufgabe der öffentlichen Organe, dass sie das auch sicherstellen. Um das Vertrauen, darum geht es. Wenn dieses einmal verloren ist, nach einem Vorfall beispielsweise, dann ist es sehr schwierig, es wiederaufzubauen.
Was unterstützt dabei? Die Vorabkontrolle, die Beratung, bevor eine Datenbearbeitung stattfindet. Insbesondere, wenn es Risiken gibt bei neuen Technologien, dann kommt das Projekt zu uns. Wir schauen es an, geben Inputs und beurteilen

es, noch bevor es überhaupt durchgeführt wird. Und das ist so ein Instrument, das das Vertrauen natürlich stärken kann beziehungsweise auch wirklich stärkt und ein sehr ein gutes Instrument ist.
Inhaltlich haben wir, was die digitale Transformation betrifft, insbesondere zwei Themen gehabt im letzten Jahr, 2023: Das ist einerseits die Cloud, andererseits die KI *(Künstliche Intelligenz)*, ich möchte zu beidem ganz kurz etwas sagen. Es gab ein Gutachten der Staatskanzlei, das Ende 2023 erstellt wurde und sich mit der Thematik der Cloud, des Cloud-Einsatzes, am konkreten Beispiel von Microsoft-Software beschäftigt, die verfassungsmässige Sicht oder Prüfung dieser Datenbearbeitung darlegt und wichtige Aussagen macht, insbesondere: Es sind Alternativen zu prüfen – wie immer im Rahmen einer Verhältnismässigkeitsprüfung. Öffentliche Organe – es wurde schon kurz angetönt – haben den Verhältnismässigkeitsgrundsatz einzuhalten, das ist ein Teil der grundrechtlichen Vorgaben. Und da gilt es im Rahmen dieser Verhältnismässigkeit Alternativen zu prüfen im Sinne von: Welche Aufgabe muss ich erfüllen? Wie kann ich das genau machen? Welche Mittel habe ich dafür? Und welche Mittel sind die mildesten Mittel? Wo greife ich am wenigsten in die Grundrechte ein?
Bei den Gemeinden braucht es viel Unterstützung in diesem Bereich. Sie sind nicht gross aufgestellt, schon rein vom Know-how oder vom Personal her. Deshalb haben wir immer wieder den Fokus auch auf die Gemeinden und haben einen Leitfaden geschrieben für den Microsoft-Einsatz spezifisch auch bei Gemeinden.
Zur KI kann ich als wichtigste Message sagen: Ja, es werden Daten bearbeitet. Bei der künstlichen Intelligenz ist es jetzt rein aus Datenschutzperspektive eine Datenbearbeitung, natürlich mit allen Grundsätzen und allen Vorgaben, die auch in diesem Rahmen anwendbar sind und zum Zuge kommen. Wichtig ist hier, dass auch eine Auslagerung stattfindet. Also bei der KI wird ein Dienstleister beigezogen, und entsprechend sind insbesondere auch die Vorgaben der Auslagerung, wie auch bei der Cloud beispielsweise, einzuhalten. Das ist also dieser Rahmen, wo wir uns bewegen. Die Transparenz ist bei der KI natürlich ganz wichtig, dass auch Transparenz darüber besteht, dass sie überhaupt eingesetzt wird, und vor allem auch, wie und zu welchem Zweck und so weiter. Auch diese Projekte sind vorabkontrollpflichtige Projekte, die jetzt immer mehr auch zu uns kommen, damit wir das vorab prüfen können.
Die Kontrollen sind eine wichtige Tätigkeit im Rahmen der Aufsicht, ein sehr wirksames Instrument, das wir haben und womit wir auch unterstützen können. Gleichzeitig kontrollieren wir und können auch gleich aufzeigen, wie man etwas verbessern kann. Im letzten Jahr, 2023, haben wir das erste Mal 60 Kontrollen durchgeführt. Das sind viele Kontrollen für unsere Behörden, davor waren es jeweils 20 bis 30 pro Jahr. Und so konnten wir jetzt, nachdem die Corona-Pandemie uns da nicht mehr einen Strich durch die Rechnung gemacht hat, das auch aufholen und jetzt die 60 Kontrollen wirklich durchführen. Ein Schwerpunkt waren die Alters- und Pflegezentren. Da hat sich gezeigt, dass viele Basics, viele einfache Themen nicht gut umgesetzt sind. Beispielsweise fanden wir an Bildschirmen Post-its vor, wo der Benutzername und das Passwort angegeben waren. Man

konnte sich also einfach so einloggen. Genau, Sie schmunzeln, aber das ist tatsächlich so, das haben wir so festgestellt. Es gibt auch viele unpersönliche Accounts, die eingesetzt werden, sie sind also nicht einer Person zuzuordnen, die am Computer arbeitet, sondern es ist ein allgemeiner Account. Das ist zu personifizieren. Und es gab auch viele fehlende Back-ups und Updates, die nicht durchgeführt wurden; dies so ein paar Beispiele, die wir da gefunden haben.
Bei den Gemeinden setzen wir auf die Selbstdeklaration. Das ist ein Instrument, ein Kontrollinstrument, bei dem wir den Gemeinden Grundlagen, Unterlagen zur Verfügung stellen, Musterdokumente, sodass die Gemeinden mit der Anwendung oder Umsetzung dieser Dokumente eine Basisinformationssicherheit in ihrer Gemeinde sicherstellen können. Das freut die Gemeinden, das wird rege genutzt. Wir haben aktuell 62 der 160 Gemeinden, die es im Kanton gibt, die das bereits umgesetzt haben. Die Idee, das Ziel ist, das flächendeckend umzusetzen. Beispiele, was dafür in den Dokumenten drin ist, sind Konzepte, Informationen, Sicherheitskonzepte, Back-up-Konzepte und so weiter. Das sind aber auch Rollenberechtigungen beispielsweise, also wirklich die Grundlagen der Informationssicherheit, die da abgedeckt sind.
Bei den Meldungen stellen wir weiterhin fest, dass die häufigsten Vorfälle, die passiert sind, Fehlversände waren, also wenn ein Dokument an eine falsche Person versendet wird. Meist sind da falsche Stammdaten die Grundlage. Das kann man mit verschiedenen Massnahmen verhindern, beispielsweise und an erster Stelle durch Schulung der Mitarbeitenden, damit diese auch wissen, worauf sie achten müssen, und die E-Mail vielleicht noch einmal überprüfen, bevor sie sie verschicken. Man kann beispielsweise auch ein Vier-Augen-Prinzip umsetzen. Oder es gibt auch technische Lösungen, bei denen beispielsweise eine E-Mail vorab bestätigt werden muss und es so dann sicher die richtige E-Mail ist, die beispielsweise zu einer Patientin oder einem Patienten gehört.
Als weiteres Oberthema ein bisschen allgemeiner Natur habe ich «Datenschutz ist nicht verhandelbar» als Thema gewählt, auch im Tätigkeitsbericht. Denn ich stelle immer wieder fest, dass privatrechtliche Argumentationen in den öffentlichen Bereich kommen. Das Privatrecht und das öffentliche Recht unterscheiden sich grundlegend in der Art und Weise, wie gearbeitet wird. Bei den öffentlichen Organen haben wir die Bundesverfassung, die uns mit den Grundrechten und auch der Möglichkeit, diese allenfalls einzuschränken, klare Vorgaben macht. Wir haben diese verfassungsmässigen Prinzipien, die im öffentlichen Bereich gelten, die bei den Privaten nicht in dieser Form gelten. Deshalb diese Unterschiede, und diese Bereiche sind klar auseinanderzuhalten, entsprechend kann nicht so argumentiert werden. Was bedeutet das? Wir haben bei den verfassungsmässigen Prinzipien, die ich bereits erwähnt habe, ein Legalitätsprinzip. Im öffentlichen Bereich dürfen nur Daten bearbeitet werden, wenn dafür eine Grundlage in einem Gesetz oder einer Verordnung besteht. Das ist im privaten Bereich anders. Da darf man grundsätzlich bearbeiten, es sei denn, man verletzt die Persönlichkeit; es ist ein umgekehrtes System. Weiter brauchen wir im öffentlichen Bereich ein öffentliches Interesse, damit die Daten überhaupt bearbeitet werden dürfen, und die bereits erwähnte Verhältnismässigkeit. Es ist eben zu prüfen, mit welchen Mitteln,

mit welchen möglichst milden Mitteln ich eine Datenbearbeitung durchführen und damit den Grundrechtseingriff möglichst klein ausfallen lassen kann. In dem Sinne gibt es im öffentlichen Bereich, bei öffentlichen Organen keinen Raum für Einwilligungen. Da kann man nicht etwas abmachen mit der Bevölkerung, sondern das muss im Gesetz festgehalten sein. Und auch Risikoabwälzungen auf Bürgerinnen und Bürger sind nicht zulässig, sondern eine Datenbearbeitung muss so ausgestaltet werden, dass das öffentliche Organ das Risiko vollständig selber trägt und dies auch entsprechend tragbar ist. Ein Spital zum Beispiel kann eine Behandlung nicht davon abhängig machen, dass die Patientinnen und Patienten einwilligen, dass ihre Daten in einer nicht grundrechtskonformen Cloud gespeichert werden, sondern das Spital muss die Behandlung durchführen können, ohne auf diese Einwilligung angewiesen zu sein. Denn es hat eine Grundversorgung zu gewährleisten und die Patientinnen und Patienten können nicht aus diesem Grund abgewiesen werden.
Das Datenschutzrecht im Kanton Zürich gibt es bald 30 Jahre, wir werden das im Januar 2025 entsprechend feiern. Damals ist das erste Datenschutzgesetz im Kanton Zürich in Kraft getreten. Letztes Jahr ist eine Revision des Datenschutzgesetzes des Bundes in Kraft getreten. Das hat uns gezeigt, dass es auch bei den öffentlichen Organen ein bisschen zur Verwirrung geführt hat im Sinne von: Welches Gesetz ist für uns eigentlich anwendbar? Das Datenschutzgesetz des Bundes regelt die Datenbearbeitungen durch den Bund und jene durch private Personen in der ganzen Schweiz. Und in jedem Kanton gibt es ein eigenes kantonales Datenschutzgesetz, das die Datenbearbeitungen durch die öffentlichen Institutionen in diesem Kanton regelt. Und das ist unser Anwendungsbereich hier im Kanton Zürich mit dem IDG *(Gesetz über die Information und den Datenschutz)*. Das ist hier anwendbar und nicht das Datenschutzrecht des Bundes.
Mein Fazit, mein Aufruf wie immer: Die Grundrechte sind zu gewährleisten, insbesondere – also nicht insbesondere, sondern genau – im öffentlichen Bereich. Das ist die Aufgabe, das machen die öffentlichen Organe so, und die Bevölkerung muss sich, wie ich eingangs erwähnt habe, darauf verlassen können. Sie muss Vertrauen in diese Datenbearbeitungen haben können und wissen, dass das korrekt abläuft. Und das ist das, wofür ich mich mit meinem Team einsetze. Ich danke Ihnen für Ihre Aufmerksamkeit.

Markus Schaaf (EVP, Zell): Nachdem wir uns nun über die Dummheit der Pflegeheime amüsieren durften, möchte ich doch als Leiter eines Pflegeheims etwas klarstellen: Es gibt zwei Ebenen von Systemen. Der Zugang zur Betriebssystemebene kann durchaus mit einem einheitlichen Passwort geregelt werden. Da geht es einfach darum, dass man sich an einem Terminalserver oder an einem PC überhaupt anmelden kann. Wenn man das individualisieren möchte, ist es sehr kompliziert, weil dann jeder sein eigenes E-Mail hat. Und wenn jemand dann Mails für eine Abteilung versenden muss, wird es sehr schwierig. Zudem haben wir sehr viele Wechsel. Deshalb macht es durchaus Sinn, abteilungsweise zum Beispiel einen Account zu haben.

Es gibt dann die Fachapplikation, und in der Fachapplikation hat selbstverständlich jede Person ihren eigenen Account, auch entsprechend der Kompetenzstufe, die sie hat. Es ist alles geregelt, das ist alles dokumentenecht. Es war mir einfach ein Anliegen, klarzustellen, dass es nicht ganz so schlimm ist, wie es da geschildert wurde. Es sind nicht die letzten Deppen, die in einem Pflegeheim am Computer sitzen.

Nicola Yuste (SP, Zürich): Ich möchte zu Beginn im Namen der SP die Arbeit der Datenschutzbeauftragten und ihres 19-köpfigen Teams würdigen. Der Aufgabenkatalog ist umfassend, die Arbeit bestimmt nicht leicht, aber umso wichtiger. Sie schützen unser Menschenrecht auf Privatsphäre, das auch in der Bundesverfassung verankert ist. Und was dies in der Praxis bedeutet, können wir sehr anschaulich im Tätigkeitsbericht nachverfolgen.
Ich möchte im Sinne der Zeit in meinem Votum vor allem auf einen Bereich etwas näher eingehen, den auch die Datenschützerin in ihrem Bericht prominent platziert hat. Wenn man sich den Tätigkeitsbericht online auf der Website ansieht, so erscheint direkt nach dem Vorwort ein Erklärvideo zur besonderen Rolle von staatlichen Institutionen im Umgang mit persönlichen Daten. Und hier ist vor allem eben der Unterschied zu den privaten Firmen interessant, und ich habe viel bei der Lektüre gelernt. Wir sind uns vom Umgang mit privaten Firmen ja gewohnt, dass wir um eine Einwilligung gebeten werden, damit diese unsere privaten Daten, unsere persönlichen Daten bearbeiten dürfen. Es ist meine freie Entscheidung, diese Leistungen in Anspruch zu nehmen oder eben auch nicht, wenn ich zum Beispiel mit der Bearbeitung der Daten nicht einverstanden bin. Diese Freiheit gibt es im Umgang mit staatlichen Akteuren nicht und deshalb gibt es in der Verfassung verankerte Rahmenbedingungen, wie der Staat mit persönlichen Daten umgehen darf. Ich kann ja beispielsweise nicht einfach entscheiden, dass das Zivilstandsamt meine Daten nicht bearbeiten darf, und auf ein anderes Amt ausweichen. So bestimmt das Legalitätsprinzip, dass Personendaten nur dann bearbeitet werden dürfen, wenn dies in einer rechtlichen Grundlage vorgesehen ist. Die Datenbearbeitung muss im öffentlichen Interesse liegen und verhältnismässig sein. Der Staat kann es nicht von meiner Einwilligung abhängig machen, ob meine Daten bearbeitet werden oder nicht. Wir haben es gehört, Beispiele dafür sind Ämter, eben auch Spitäler mit Grundversorgungsauftrag, aber beispielsweise auch Schulen. Diese öffentlichen Institutionen müssen also – und davon darf ich ausgehen – grundrechtsmässig mit den Daten umgehen und meine Grundrechte schützen, auch – und eben insbesondere auch – im Umgang mit Clouds. Grundsätzlich gilt für jede Gemeindebehörde und Institution: Wenn die Bearbeitung von Personendaten in die Cloud ausgelagert wird, bleibt die staatliche Stelle für die Datenbearbeitung und den Datenschutz verantwortlich; eine riesige Aufgabe, wie wir uns vorstellen können.
Wir haben die Problematik von Cloud-Lösungen für öffentliche Institutionen ja bereits letztes Jahr angesprochen, aber das Thema verdient auch dieses Jahr unsere Aufmerksamkeit. Die derzeit am stärksten verbreitete Cloud-Lösung, die auch der Kanton Zürich nutzt, ist Microsoft 365. Egovpartner, ein Netzwerk von

Gemeinden, Städten und dem Kanton, unterstützt die Gemeinden und anderen Institutionen mit verschiedenen Hilfsinstrumenten bei der Einführung von Microsoft 365. Eines der Hilfsmittel, das egovpartner den Gemeinden zur Verfügung stellt, ist ein rechtliches Gutachten zum grundrechtskonformen Einsatz von Microsoft 365 durch Gemeinden im Kanton Zürich. Ein wichtiger Grund, warum der grundrechtskonforme Einsatz von Microsoft 365 so kompliziert ist, ist der US-Cloud-Act, Sie hören ihn jetzt auch nicht zum ersten Mal. Er garantiert US-Behörden Zugang zu allen Personendaten in Clouds von Microsoft und anderen amerikanischen Firmen, auch wenn – und das ist eben wichtig – die Daten nicht in den USA auf einem Server der USA gespeichert sind. Die SP hat bereits im Jahr 2022 auf diese Gefahr hingewiesen, als die Bewilligung von Microsoft 365 für sämtliche der IKT-Strategie unterstehenden Einheiten der kantonalen Verwaltung sowie die Kantonspolizei mittels RRB *(Regierungsratsbeschluss)* bekannt wurde. Das juristische Gutachten, das egovpartner publiziert hat – also ich hatte keinen Zugriff, deswegen beziehe ich mich auf den Bericht der Datenschützerin – und das die Auslagerung von Personendaten in M365-Clouds untersucht hat, kommt eben nun zum Schluss, dass diese Auslagerung einen schwerwiegenden Eingriff in die Grundrechte darstellt. Und ich zitiere aus dem Bericht der Datenschützerin: «Die Daten sämtlicher Personen im Zuständigkeitsbereich des öffentlichen Organs werden durch den Einsatz dieser Cloud-Lösung auf Vorrat zugänglich für US-Behörden.» Damit verliere das öffentliche Organ die Kontrolle über die Daten und könne den Anspruch auf Schutz der Betroffenen vor Missbrauch ihrer persönlichen Daten, wie er in der Bundesverfassung, Artikel 13, Absatz 2, festgeschrieben ist, nicht mehr sicherstellen. Weil die Auslagerung von besonderen Personendaten oder Daten, die der gesetzlichen Geheimnispflicht unterstehen, eine besondere Grundrechtsgefährdung darstellen, dürfen sie nur verschlüsselt in der Cloud abgelegt werden. Das Gutachten stellt ausserdem fest, und das ist ein ganz wichtiger Punkt, dass kein ausreichender rechtlicher Rahmen besteht, der für eine Auslagerung in die Cloud eines US-Unternehmens ausreichen würde. Dies deckt sich auch mit den Einschätzungen der Datenschutzbeauftragten, wie sie schreibt.

Was heisst das nun für den Kanton Zürich und seine öffentlichen Institutionen, Spitäler, Schulen und Gemeinden? Wie können sie – und können sie überhaupt – mit der komplexen datenschutzrechtlichen Lage umgehen? Und die noch viel wichtigere Frage: Wie kam es im Kanton Zürich eigentlich zur Entscheidung für die amerikanische Cloud-Lösung? Wurden Alternativen geprüft? Eben, wir haben es gehört, das ist im Sinne der Verhältnismässigkeit. Als öffentliches Organ sind wir in der Pflicht, Alternativen zu prüfen. Was waren die Gründe, dass man sich gegen eine Schweizer Cloud-Lösung, wo die Daten auf einem Schweizer Server gespeichert sind, entschieden hat?

Wir haben genau diese Frage auch in der Anfrage 354/2022 der Regierung gestellt. Die Antwort war ernüchternd. Und hier zitiere ich aus der Antwort: «RRB-Nummer 354/2022 bezieht sich auf die Zulassung des Einsatzes der Cloud-Lösung M365 von Microsoft. Die Nutzung einzelner M365-Services, zum Beispiel

MS-Teams, bedingt die Nutzung der Microsoft-Cloud. Die Erstellung einer eigenen Cloud oder eines Dienstes mit Server in der Schweiz fällt daher offensichtlich ausser Betracht.» Okay, das heisst, die Regierung erklärt uns: Ja, wir wollten MS-Teams nutzen, deshalb müssen wir auch die Cloud nutzen. Das war mir auch klar. Offensichtlich war das aber nicht unsere Frage, sondern wir wollten fragen: Habt ihr auch andere Cloud-Lösungen mit anderen Services geprüft? Diese Frage blieb unbeantwortet.
Es bleiben viele Fragen offen und ich begrüsse sehr, dass die GPK am Thema dranbleibt. Wir begrüssen es auch, dass die Datenschutzbeauftragte Gemeinden und andere öffentliche Organe im Rahmen ihrer Beratungstätigkeit unterstützt in diesem schwierigen Thema. Und logischerweise genehmigen wir den Bericht. Vielen Dank.

Abstimmung
Der Kantonsrat beschliesst mit 166 : 0 Stimmen (bei 0 Enthaltungen), den Tätigkeitsbericht der Datenschutzbeauftragten über das Jahr 2023 zu genehmigen.

Das Geschäft ist erledigt.