Antrag der Geschäftsprüfungskommission*
vom 22. August 2024

KR-Nr. 136/2024

Beschluss des Kantonsrates zum Tätigkeitsbericht der Datenschutzbeauftragten über das Jahr 2023

(vom . . . . . .)

Der Kantonsrat,

nach Einsichtnahme in den Antrag der Geschäftsprüfungskommission vom 22. August 2024,

beschliesst:

I. Der Tätigkeitsbericht der Datenschutzbeauftragten über das Jahr 2023 wird genehmigt.

II. Mitteilung an die Datenschutzbeauftragte des Kantons Zürich.

Zürich, 22. August 2024

Im Namen der Geschäftsprüfungskommission:

Der Präsident:	Der Sekretär:
Jean-Philippe Pinto	Christian Hirschi

* Die Geschäftsprüfungskommission besteht aus folgenden Mitgliedern: Jean-Philippe Pinto, Volketswil (Präsident); Pia Ackermann, Zürich; Sandra Bossert, Wädenswil; Ruth Büchi-Vögeli, Elgg; Edith Häusler, Kilchberg; Corinne Hoss-Blatter, Zollikon; René Isler, Winterthur; Davide Loss, Thalwil; Manuel Sahli, Winterthur; Benno Scherrer, Uster; Yiea Wey Te, Unterengstringen; Sekretär: Christian Hirschi.

Bericht und Antrag

Aufgaben der Datenschutzbeauftragten und Zuständigkeit der Geschäftsprüfungskommission

Die Beauftragte für den Datenschutz (nachfolgend Datenschutzbeauftragte) beaufsichtigt die Datenbearbeitung der kantonalen Verwaltung, der Gemeinden sowie der übrigen Behörden und öffentlichen Einrichtungen im Kanton, um den Schutz der Privatsphäre der Bürgerinnen und Bürger sicherzustellen (§ 34 und 35 Gesetz über die Informationen und den Datenschutz [IDG; LS 170.4]). Wenn es um Datenbearbeitungen von Bundesstellen oder von Privaten geht, ist hingegen der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte zuständig.

Die Datenschutzbeauftragte ist unabhängig. Gewählt wird sie vom Kantonsrat für eine Amtsdauer von vier Jahren. Administrativ ist sie der Geschäftsleitung des Kantonsrates zugeordnet (§ 30 IDG). Seit Mai 2020 wird das Amt der Datenschutzbeauftragten von Dominika Blonski wahrgenommen. Ihr Team besteht aktuell aus 17 Mitarbeitenden mit insgesamt 14,7 Vollzeitstellen in den Bereichen Rechtswissenschaft, Informationssicherheit und Kommunikation.

Die Geschäftsprüfungskommission (GPK) übt die parlamentarische Kontrolle über die Datenschutzbeauftragte aus (§ 104 Abs. 1 Kantonsratsgesetz [LS 171.1] in Verbindung mit § 39 Abs. 1 Kantonsratsreglement [LS 171.11]). Sie prüft den jährlichen Tätigkeitsbericht der Datenschutzbeauftragten und stellt dem Kantonsrat Antrag zu dessen Genehmigung.

Tätigkeiten und Feststellungen der Datenschutzbeauftragten im Berichtsjahr

Die Datenschutzbeauftragte berichtet dem Kantonsrat in ihrem Tätigkeitsbericht jährlich über den Umfang und die Schwerpunkte ihrer Tätigkeiten, über wichtige Feststellungen und Beurteilungen sowie über die Wirkung des kantonalen Datenschutzgesetzes. Der Bericht wird auch öffentlich vorgestellt und publiziert. Zudem stand die Datenschutzbeauftragte der GPK in der Sitzung vom 20. Juni 2024 Rede und Antwort. Neben der Behandlung des Tätigkeitsberichts befragte die GPK die Datenschutzbeauftragte speziell zur Organisation der Datenschutzbehörde und zum Personal, zur Wahrnehmung der Beratungs- und Aufsichtstätigkeiten durch die Datenschutzbehörde, zu den Leistungsindikatoren und Entwicklungsschwerpunkten gemäss Konsolidiertem Entwicklungs- und Finanzplan (KEF) sowie zum Umgang mit Datenschutzvorfällen.

Der vorliegende Tätigkeitsbericht deckt den Zeitraum vom 1. Januar bis 31. Dezember 2023 ab. Bereits seit einigen Jahren wird der Tätigkeitsbericht nicht mehr in gedruckter Form publiziert. Seit letztem Jahr er

scheint der Tätigkeitsbericht zusätzlich auf der Webseite der Datenschutzbeauftragten als Online-Publikation (www.datenschutz.ch/tb/2023). Dadurch können einzelne Themen mit audiovisuellen Inhalten ergänzt und erklärt werden, was zu einer besseren öffentlichen Sensibilisierung für Fragen des Datenschutzes beiträgt.

Kontrolltätigkeit

Eine der Hauptaufgaben der Datenschutzbehörde ist die Durchführung von Kontrollen (Datenschutz-Reviews) bei öffentlichen Organen. Gemäss KEF verfolgt die Datenschutzbehörde den Entwicklungsschwerpunkt, dass regelmässige und nachhaltige Kontrollen der Datenbearbeitungen gewährleistet sind. Sie überprüft dabei, ob die datenschutzrechtlichen und technischen Vorgaben durch die öffentlichen Organe im Kanton Zürich eingehalten werden. Im Berichtsjahr hat die Datenschutzbehörde erstmals 60 solche Kontrollen durchgeführt und damit die Vorgabe des Leistungsindikators gemäss KEF für diese Tätigkeit erfüllt. In den zurückliegenden Jahren lag die Zahl jeweils bei 20 bis 30 Kontrollen. Der nun erfolgte Anstieg hat gemäss der Datenschutzbeauftragten damit zu tun, dass während der Coronapandemie kaum Kontrollen vor Ort durchgeführt werden konnten.

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 durchgeführte Kontrolle bei einer repräsentativen Auswahl der rund 160 Alters- und Pflegezentren, die im Zuständigkeitsbereich der Datenschutzbeauftragten liegen, brachte einige grundlegende Mängel hervor. So erfolgten der Zugriff zu den Daten teilweise über unpersönliche Accounts mit allgemein bekannten Passwörtern, und starke Authentifizierungsmechanismen, die bei der Bearbeitung von besonderen Personendaten Pflicht sind, fehlten.

Zusätzlich hat die Datenschutzbehörde die Datenschutz-Reviews mit Selbstdeklaration bei den Gemeinden vorangetrieben. Bisher konnte in 62 der 160 Gemeinden des Kantons ein solches Datenschutz-Review gestartet werden. 2024 werden diese Reviews bei den weiteren Gemeinden fortgesetzt.

Beratungstätigkeit

Ein weiterer zentraler 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 (Vorabkontrollen) und nimmt Stellung

zu Erlassen. Dabei hat die Zahl von Beratungen und Vorabkontrollen in den vergangenen Jahren kontinuierlich zugenommen. Bei den Vorabkontrollen handelt es sich teilweise um sehr komplexe Projekte. Diese Kontrollen laufen nach einem klar definierten Prozess ab. Zunächst muss das verantwortliche Organ der Datenschutzbehörde bestimmte Informationen zur Verfügung stellen. Dazu gehört eine Rechtsgrundlagenanalyse sowie ein Informations-, Sicherheits- und Datenschutzkonzept. Basierend auf diesen Dokumenten erarbeitet die Datenschutzbehörde eine Stellungnahme. Im Anschluss führt die Datenschutzbehörde gestützt auf ihre Ergebnisse eine Beratung beim verantwortlichen Organ durch.

Die öffentlichen Organe sind gemäss § 10 IDG zur Durchführung einer solchen Vorabkontrolle verpflichtet, wenn eine beabsichtigte Bearbeitung von Personendaten mit besonderen Risiken für die Grundrechte der betroffenen Personen verbunden ist. Stellt die Datenschutzbehörde eine Verletzung der Datenschutzbestimmungen fest, gibt sie dem zuständigen öffentlichen Organ eine Empfehlung ab, welche Massnahmen zur Behebung und zukünftigen Vermeidung der festgestellten Datenschutzverletzung zu ergreifen sind (§ 36 Abs. 1 IDG). Zudem kann die Datenschutzbeauftragte eine Verfügung aussprechen, wenn sich ein Organ nicht an ihre Empfehlung hält. Darin kann sie verlangen, dass die Datenbearbeitung ganz oder teilweise angepasst, unterbrochen oder abgebrochen wird und die Personendaten ganz oder teilweise gelöscht oder vernichtet werden (§ 36a Abs. 1 IDG). Eine solche Verfügung hat die Datenschutzbeauftragte seit ihrem Amtsantritt noch keine ausgesprochen. Dem Instrument der Verfügung kommt jedoch eine wichtige Vorauswirkung zu. Indem es diese Möglichkeit gibt und dies den öffentlichen Organen bewusst ist, erhalten die Empfehlungen der Datenschutzbeauftragten ein stärkeres Gewicht, da diese notfalls auch rechtlich verbindlich durchgesetzt werden können.

Digitale Transformation

Die Umsetzung der datenschutzrechtlichen Vorgaben und der Massnahmen zur Informationssicherheit sind ein zentrales Thema der fortschreitenden digitalen Transformation des Kantons und der Gesellschaft generell. Die Digitalisierung bietet viele neue Möglichkeiten und Vereinfachungen, sowohl für die Behörden als auch für die Einwohnerinnen und Einwohner. Sie ist aber auch mit Risiken behaftet. Die Datenschutzbeauftragte weist deshalb in ihrem aktuellen Tätigkeitsbericht darauf hin, dass die Bevölkerung gerade in diesem Umfeld der rasanten Entwicklungen auf die grundrechtskonforme Umsetzung des Datenschutzes vertrauen können müsse. Es sei deshalb wichtig, dass die Datenschutzbehörde durch die Behörden früh einbezogen werde. Das Datenschutzrecht sei eine grosse Hilfe, damit die digitale Transformation auch nachhaltig gelinge. Dabei sei der Datenschutz «nicht verhandelbar».

Konkret fordert die Datenschutzbeauftragte, dass die öffentlichen Organe auch bei Cloud-Lösungen sicherstellen müssen, dass der Datenschutz gewährleistet ist, wie wenn sie die Daten selbst bearbeiten würden. So seien gesetzliche Schweigepflichten wie etwa das Arztgeheimnis oder das Steuergeheimnis einzuhalten. Vor allem ist sicherzustellen, dass nicht Dritte in Umgehung von Bestimmungen der internationalen Rechtshilfe auch auf Daten, die in der Schweiz gespeichert sind, zugreifen können. Im Vordergrund dieser Betrachtungen steht der Einsatz von Microsoft-Cloud-Lösungen (M365). Der Regierungsrat hat diesen für die kantonale Verwaltung mit Beschluss Nr. 542/2022 bewilligt. Die Datenschutzbeauftragte war in diesen Prozess involviert und brachte ihre datenschutzrechtlichen Anliegen ein. Zudem legten im Berichtsjahr verschiedene Gemeinden und Stadtverwaltungen der Datenschutzbeauftragten ihre Projekte zur Einführung von M365 zur Vorabkontrolle zu. Vor Jahresfrist hielt die Datenschutzbeauftragte in ihrem Tätigkeitsbericht noch fest, dass zum damaligen Zeitpunkt noch kein öffentliches Organ im Kanton Zürich der Datenschutzbehörde ein Projekt zur Einführung von M365 zur Vorabkontrolle vorgelegt hatte.

Aus datenschutzrechtlicher Sicht ist jede Bearbeitung von Personendaten ein Eingriff in die Grundrechte. Bevor Cloud-Dienste eingesetzt werden können, muss ein öffentliches Organ deshalb nicht nur abklären, ob diese Bearbeitung der Personendaten einer gesetzlichen Aufgabe dient, sondern auch, ob der Eingriff in die Grundrechte verhältnismässig ist. Die GPK liess sich von der Datenschutzbeauftragten über diese Thematik ausführlich informieren. Zudem hörte eine Vertretung von GPK und Finanzkommission im Rahmen einer Subkommission auch das Amt für Informatik in der Sache an. Es ist offensichtlich, dass es zwischen der Datenschutzbeauftragten und dem Regierungsrat in diesen Fragen teilweise unterschiedliche Auffassungen gibt. Während der Regierungsrat mit seinem Beschluss einen risikoorientierten Ansatz verfolgt, darf der Staat aus Sicht der Datenschutzbeauftragten das Grundrecht auf Datenschutz nicht durch Einwilligungen und Risiko- und Compliance-Überlegungen einzuschränken versuchen. Auch beim Einsatz von Anwendungen mit künstlicher Intelligenz handelt es sich aus datenschutzrechtlicher Sicht immer um eine Auslagerung von Daten, da diese zumindest teilweise auf Cloud-basierte Tools zurückgreifen.

Umgang mit Datenschutzvorfällen

Gestützt auf § 12a IDG besteht für das verantwortliche öffentliche Organ bei Datenschutzvorfällen eine Meldepflicht an die Datenschutzbeauftragte. Ein Datenschutzvorfall liegt vor, wenn personenbezogene Daten unwiederbringlich vernichtet werden oder verloren gehen, unbeabsichtigt oder unrechtmässig verändert oder offenbart werden oder Un

befugten zugänglich werden. Im Berichtsjahr gab es gemäss Datenschutzbeauftragte 72 Meldungen zu solchen Datenschutzvorfällen. In 39 Fällen wurden Personendaten per E-Mail oder Brief an unberechtigte Personen verschickt. Oft stammten die Meldungen von Spitälern. Für die Meldung eines Datenschutzvorfalles steht auf der Webseite der Datenschutzbeauftragten ein Formular zur Verfügung. Zudem gibt es ein Merkblatt und weitere nützliche Informationen.

Wie die Datenschutzbeauftragte gegenüber der GPK ausführte, ist die Meldepflicht dennoch nicht überall bekannt. Wenn die Datenschutzbeauftragte auf anderem Weg Kenntnis eines Datenschutzvorfalles erhält (zum Beispiel über die Medien oder direkt von Betroffenen), fragt sie beim zuständigen Organ nach, weist auf die Meldepflicht hin und fordert diese vom Organ nachträglich ein. Basierend auf der Meldung beurteilt die Datenschutzbehörde den Sachverhalt und prüft, ob Sofortmassnahmen ergriffen werden müssen. In einem weiteren Schritt wird das zuständige Organ beraten. Dabei geht es vor allem darum, dafür zu sorgen, dass ähnliche Vorfälle künftig vermieden werden können. Die von der Datenschutzbehörde vorgeschlagenen Massnahmen werden zusammen mit einer Umsetzungsfrist in einer Stellungnahme festgehalten. Nach Ablauf der Frist erfolgt eine Nachkontrolle, ob die Massnahmen umgesetzt wurden.

Würdigung durch die GPK und Antrag

Die kantonale Datenschutzbehörde beaufsichtigt die Datenbearbeitungen der kantonalen Verwaltung, 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 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 dankt Dominika Blonski und ihrem Team für ihre wichtige Arbeit zugunsten der Bevölkerung des Kantons. Sie beantragt einstimmig, den Tätigkeitsbericht 2023 der Datenschutzbeauftragten zu genehmigen.