dsb
datenschutzbeauftragte
des kantons zürich

Tätigkeitsbericht 2024

Vorwort

Die Datenschutzbeauftragte Dr. Dominika Blonski beim Interview. Foto: dsb

Das zuständige öffentliche Organ hat zu beurteilen, ob die Datenbearbeitungen rechtmässig, zweckmässig und verhältnismässig sind, um seine Aufgabe zu erfüllen.

Die Beauftragte berichtet dem Wahlorgan periodisch über Umfang und Schwerpunkte der Tätigkeiten, über wichtige Feststellungen und Beurteilungen sowie über die Wirkung des Gesetzes. Der Bericht wird veröffentlicht (§ 39 IDG).

Der vorliegende 30. Tätigkeitsbericht deckt den Zeitraum vom 1. Januar 2024 bis und mit 31. Dezember 2024 ab und erscheint ausschliesslich digital. Er wird unter www.datenschutz.ch *(http://www.datenschutz.ch)* publiziert.

Die digitale Transformation in der Verwaltung ist 2024 weiter vorangeschritten, was sich auch auf das Tätigkeitsgebiet der Datenschutzbeauftragten auswirkt. Öffentliche Organe aus den unterschiedlichen Bereichen haben der Datenschutzbeauftragten ihre neu entwickelten digitalen Projekte zur Überprüfung vorgelegt. Dabei sind die Privatsphäre und somit die Grundrechte der Bevölkerung unabhängig von der eingesetzten Technologie zu wahren.

Die Verantwortung für die Bearbeitung von Daten von Bürgerinnen und Bürgern liegt beim jeweils zuständigen öffentlichen Organ. Dieses hat zu beurteilen, ob die Datenbearbeitungen rechtmässig, zweckmässig und verhältnismässig sind, um seine Aufgabe zu erfüllen. Die Datenschutzbeauftragte berät öffentliche Organe und ihre Mitarbeitenden zu Fragen des Datenschutzes und zur Informationssicherheit. Als Aufsichtsbehörde beaufsichtigt sie die öffentlichen Organe im Kanton Zürich.

In ihren Kontrollen aber auch durch die Meldungen von Datenschutzvorfällen stellt die Datenschutzbeauftragte Mängel fest. Gerade angesichts der international zunehmenden Cyberrisiken ist die Umsetzung der datenschutzrechtlichen Vorgaben und der Massnahmen zur Informationssicherheit von hoher Bedeutung. Erfolgt dies nicht, geht das Vertrauen der Bevölkerung verloren – und dieses Vertrauen ist essenziell, damit die öffentlichen Organe ihre Aufgaben erfüllen können.

Dr. Dominika Blonski
Datenschutzbeauftragte des Kantons Zürich

Welche Zukunft für den Datenschutz im Kanton Zürich?

Mit dem Abschluss des Jahres 2024 erreicht die Datenschutzgesetzgebung ihr 30-jähriges Bestehen im Kanton Zürich.

Als das erste Zürcher Datenschutzgesetz am 1. Januar 1995 in Kraft getreten ist, sah die technologische Welt noch anders aus. Das Internet wurde erst gerade schrittweise für die Bevölkerung zugänglich, Computer kamen grossflächig in Büros auf und Textverarbeitungsprogramme wurden auch von privaten Anwenderinnen und Anwendern genutzt. Seither hat sich viel verändert und die Entwicklung schreitet weiter rasant voran. Heute geht kaum jemand ohne Smartphone aus dem Haus, wir kommunizieren über Social Media und lassen Texte durch die Künstliche Intelligenz verfassen. Sitzungen finden in Videocalls statt und Eingaben beim Bauamt, bei der Einbürgerungsbehörde oder bei der Polizei werden online vorgenommen. Die technologische Entwicklung war der Treiber, dass eine Datenschutzgesetzgebung überhaupt erlassen wurde, und sie bleibt weiterhin wegweisend für die Weiterentwicklung der datenschutzrechtlichen Überlegungen. Diese Dynamik war seit dem Inkrafttreten der Datenschutzgesetzgebung vorhanden und wird auch künftig dominieren und uns damit immer wieder vor neue Herausforderungen stellen.

Spitäler finden ihren Weg mit und ohne Cloud
(https://www.datenschutz.ch/tb/2024/spitaeler-mit-und-ohne-cloud?token=KYCETE6oDO1BAHxKmoEBteolLvP4ybNu)

> Wir müssen uns überlegen, welchen Einfluss diese Technologie auf die Gesellschaft insgesamt, auf die Grundrechte der Bevölkerung und damit auch auf das Datenschutzgrundrecht hat.

Bei all der Dynamik: Verändert sich wirklich alles so dynamisch und rasant? Unsere Grundwerte, die sich aus der Bundesverfassung ergeben, sind konstant geblieben und an diesen richten wir uns bis heute aus. Wir sprechen hier von Grundlagen unseres Staates, wie Rechtsstaatlichkeit, Verhältnismässigkeit des staatlichen Handelns und – nicht zuletzt auch im Datenschutzbereich – von Grundrechten, die uns allen als Bevölkerung dieses Landes (und hier ganz spezifisch des Kantons Zürich) zustehen und ein gutes Miteinander ermöglichen.

Hoher Weiterbildungsbedarf zu Datenschutzthemen
(https://www.datenschutz.ch/tb/2024/kontrollen-und-beratungen-erhoeht-weiterbildungsangebote-fast-verdoppelt?token=KYCETE6oDO1BAHxKmoEBteolLvP4ybNu)

Da stellt sich die Frage: Wie möchten wir also mit dieser Entwicklung umgehen – als Gesellschaft, als Gesetzgeber und auch als Aufsichtsbehörde? Mit jeder technologischen Entwicklung – sei das der E-Mail-Versand in den neunziger Jahren oder heute die Künstliche Intelligenz – müssen wir uns aktiv auseinandersetzen. Und uns überlegen, welchen Einfluss diese Technologie auf die Gesellschaft insgesamt, auf die Grundrechte der Bevölkerung und damit auch auf das Datenschutzgrundrecht hat. Wie können wir die Technologie datenschutzkonform nutzen? Welche Personendaten können wir damit bearbeiten? Welche technischen Schutzmassnahmen

setzen wir dafür um? Wir müssen gemeinsam entscheiden, wie wir unsere Zukunft mitgestalten möchten. Denn diese Entwicklungen betreffen uns alle.

Digitale Langzeitarchivierung von Akten der öffentlichen Organe
(https://www.datenschutz.ch/tb/2024/digitale-langzeitarchivierung-oeffentliche-organe?token=KYCETE6oDO1BAHxKmoEBteolLvP4ybNu)

Und spezifisch zum Datenschutz: Ist das Datenschutzrecht noch zeitgemäss? Kaum war das erste Gesetz da, kaum tritt eine Revision in Kraft, führen technologische oder gesellschaftliche Weiterentwicklungen dazu, dass das Gesetz schon bald überholt erscheint. Aber ist dem wirklich so? Das Datenschutzrecht stellt eine Rahmengesetzgebung dar. Das heisst, in den Datenschutzgesetzen sind die Rahmenbedingungen festgehalten, wie Datenbearbeitungen stattfinden können. Diese Vorgaben leiten sich aus der Bundesverfassung ab, die das Grundrecht auf Datenschutz festhält. Spezifische Regelungen zu den jeweiligen Fachbereichen wie Schulen, Gesundheitsbereich oder Polizei finden sich in den Sachgesetzen. Das Datenschutzrecht wurde bewusst technologieneutral formuliert, damit es auch auf neuere Entwicklungen anwendbar ist. Wenn wir also die bestehenden Datenschutzregelungen auf neue Technologien anwenden, haben wir einen soliden Rahmen. Das Datenschutzrecht musste sich auch bisher ständig an die dynamische, rasante Entwicklung anpassen – das gelingt gut. Erkennen wir als Gesellschaft Anpassungsbedarf, weil eine Technologie besondere Auswirkungen zeigt, lässt sich das mit Gesetzesrevisionen umsetzen. Dabei ist es wichtig, dass die Grundwerte der Bundesverfassung beigezogen werden und das staatliche Handeln, das sich auf die rechtlichen Grundlagen stützt, auf die Einhaltung der Grundwerte zu reflektieren. Denn wir schützen mit dem Datenschutz die Menschen in ihren Grundrechten und nicht die Daten.

Einführung neuer digitaler Hilfsmittel in Schulen
(https://www.datenschutz.ch/tb/2024/digitale-hilfsmittel-schulen?token=KYCETE6oDO1BAHxKmoEBteolLvP4ybNu)

Damit kommt die Frage auf: Welche Zukunft für den Datenschutz im Kanton Zürich? Die Auseinandersetzung mit den kantonalen Datenschutzvorgaben im Gesetz über die Information und den Datenschutz (IDG) sowie in der Verordnung über die Information und den Datenschutz (IDV) und der Erlass von neuen Regelungen in diesen noch laufenden Revisionen sind zu begrüssen. So soll eine Beauftragte oder ein Beauftragter für das Öffentlichkeitsprinzip geschaffen werden, offene Behördendaten (OGD) geregelt werden, ein Verzeichnis der verwendeten algorithmischen Entscheidsysteme im Bereich der Künstlichen Intelligenz bestehen und eine Grundlage für Pilotversuche geschaffen werden. Die Vorlage enthält aber auch noch zu diskutierende Regelungen, wie die Ergänzung des publizierten Tätigkeitsberichts der Datenschutzbeauftragten mit Stellungnahmen von öffentlichen Organen oder bedeutende Einschränkungen des Öffentlichkeitsprinzips, indem gewisse Dokumente pauschal vom Zugangsrecht der Bevölkerung ausgeschlossen sein sollen. Auch sollte die Chance genutzt werden, ein Schlichtungsverfahren bei Streitfällen betreffend das Öffentlichkeitsprinzip vorzusehen – das wäre effizient und vertrauenswürdig für die beteiligten Personen.

Im Ergebnis lohnt es sich, Bewährtes beizubehalten und auf die dynamische und rasante Entwicklung anzuwenden, Notwendiges anzupassen, aber auch darauf zu achten, dass keine bürokratischen Hürden geschaffen werden. Wir leben in einer dynamischen Zeit, und das Datenschutzrecht ist ein äusserst dynamisches Gebiet. Für die Zukunft ist es wichtig, dass wir unsere Grundwerte und damit auch unsere Grundrechte nicht vergessen und uns darauf fokussieren. Es braucht die persönliche Freiheit für einen liberalen Rechtsstaat. Nur mit freier Meinungsbildung funktioniert unsere Demokratie. Das sind auch Instrumente gegen Manipulation, denn die Digitalisierung darf nicht zu einem Überwachungsstaat führen. Die Aufgabe der Da-

tenschutzbeauftragten ist es dabei, Checks and Balances sicherzustellen. Die Verantwortung für die grundrechtskonforme Datenbearbeitung liegt bei den öffentlichen Organen, die sich an den öffentlich-rechtlichen Vorgaben ausrichten. Die Datenschutzbeauftragte schaut als Aufsichtsbehörde, dass die gesetzlichen Vorgaben verfassungskonform vollzogen werden, indem sie Kontrollen durchführt und überprüft, ob Grundrechtseingriffe nach rechtsstaatlichen Vorgaben erfolgen. Sie unterstützt die beaufsichtigten Organe auch präventiv dabei, indem sie diese informiert und berät.

Datenschutz in Kirchgemeinden *(https://www.datenschutz.ch/tb/2024/datenschutz-in-kirchgemeinden?token=KYCETE6oDO1BAHxKmoEBteolLvP4ybNu)*

Kontrollen und Beratungen erhöht, Weiterbildungsangebote fast verdoppelt

Die für das Jahr 2024 festgelegten Indikatoren der Datenschutzbeauftragten entwickeln sich weiterhin stabil. Die Weiterbildungsangebote der Datenschutzbeauftragten haben sich beinahe verdoppelt. Angestiegen sind wiederum die Kontrollen, die Beratungen sowie die Besuche auf der Website www.datenschutz.ch *(https://www.datenschutz.ch/)*.

Kontrollen

Ein zentraler Entwicklungsschwerpunkt der Datenschutzbeauftragten ist die Durchführung regelmässiger und nachhaltiger Kontrollen der Datenbearbeitungen bei öffentlichen Organen. Die Datenschutzbeauftragte führte im Jahr 2024 insgesamt 74 Kontrollen durch. Somit wurde einerseits der Indikator von 70 Kontrollen pro Jahr erstmals übertroffen, andererseits konnte die Kontrolltätigkeit gegenüber 2023 (60 Kontrollen) nochmals gesteigert werden. Neben Datenschutzreviews mit Selbstdeklaration bei Gemeinden wurden Schwerpunkte bei Schulen und Kirchen gesetzt. Die Massnahmenumsetzung nach Kontrollen zeigt erneut eine positive Entwicklung und wurde weiter gesteigert. Die prozentuale Umsetzung der Massnahmen durch betroffene öffentliche Organe, die nach Datenschutzreviews zur Behebung von Mängeln festgehalten wurden, liegt bei hohen 93%.

KEF	2022	2023	2024
70	24	60	74

Anzahl Kontrollen

KEF	2022	2023	2024
80%	69%	89%	93%

Prozentuale Massnahmenumsetzung

Beratung und Vorabkontrollen

Ein weiterer Entwicklungsschwerpunkt zielt auf die effiziente und wirksame Unterstützung der Verwaltung, um die Digitalisierungsziele zu erreichen. Sowohl die Beratungstätigkeit der Datenschutzbeauftragten wie auch die durchgeführten Vorabkontrollen betrafen weiterhin vordergründig komplexe Digitalisierungsprojekte. Gegenüber 2023 stiegen die Beratungen im Jahr 2024 erneut an.

KEF	2022	2023	2024
850	569	793	850

Anzahl Beratungen

Aus- und Weiterbildung

Die Aus- und Weiterbildungstätigkeit wurde gegenüber 2023 fast verdoppelt. Vermehrt konnte die Datenschutzbeauftragte Referate auf Gemeindestufe sowie im Kontext von Veranstaltungen zu Digitalisierungsthemen halten. Es besteht weiterhin ein grosser Bedarf, sich Wissen zu datenschutzrechtlichen Themen sowie zu Fragen der Informationssicherheit anzueignen.

KEF	2022	2023	2024
25	29	27	45

Anzahl Aus- und Weiterbildungen

Websitezugriffe

Erneut stiegen die Zugriffe auf die Website www.datenschutz.ch (https://www.datenschutz.ch/) stark an. Die Website beinhaltet eine umfassende Palette an konkreten Hilfestellungen rund um das Thema Datenschutz und Privatsphäre. Die Datenschutzbeauftragte verweist in den Aus- und Weiterbildungsveranstaltungen und in den Beratungen konsequent auf die Online-Informationen. Die zweite Ausgabe des ausschliesslich digital publizierten Tätigkeitsberichtes führte ebenfalls zu zusätzlichen Websitebesuchen.

KEF	2022	2023	2024
45 000	49 585	74 567	88 360

Anzahl Websitezugriffe

Teils erhebliche Mängel durch Kontrollen aufgedeckt

Im Jahr 2024 führte die Datenschutzbeauftragte 74 Kontrollen durch. Kontrolliert wurden Spitex-Organisationen, Schulen, Kirchgemeinden, Alterszentren sowie Ämter oder Direktionen. Zudem wurden Gemeinden zur Kontrolle per Selbstdeklaration eingeladen.

Das Amt für Informatik (AFI) stattet die Mitarbeitenden der kantonalen Verwaltung mit dem neuen Digitalen Arbeitsplatz (DAP) aus. Der DAP basiert unter anderem auf den Microsoft-Produkten Exchange Online und Sharepoint Online. Bei der Nutzung dieser Produkte handelt es sich um eine Auslagerung (Bearbeiten im Auftrag im Sinne des Gesetzes über die Information und den Datenschutz, IDG). Daten werden nicht mehr auf den eigenen Servern oder den Servern eines Hosting-Anbieters, sondern in der Cloud von Microsoft bearbeitet und gespeichert.

Microsoft untersteht als US-amerikanisches Unternehmen dem sogenannten CLOUD Act. Damit können US-Behörden Microsoft verpflichten, Daten ihrer Kundinnen und Kunden herauszugeben, selbst wenn diese Daten nicht in Datenzentren in den USA gespeichert sind. Microsoft darf unter Umständen das öffentliche Organ nicht einmal über die entsprechende Anordnung informieren. Zudem haben das öffentliche Organ respektive die betroffenen Personen keine Verfahrensrechte. Diese Zugriffsmöglichkeit ist aus datenschutzrechtlicher Sicht rechtswidrig. Deshalb dürfen Daten, die unter einem besonderen Amtsgeheimnis oder dem Berufsgeheimnis stehen, nur in der Cloud von Microsoft bearbeitet oder gespeichert werden, wenn technische Massnahmen eine einseitige Möglichkeit zur Kenntnisnahme durch Microsoft ausschliessen. Alternativ können diese Daten bei der Nutzung von M365 im Rahmen einer hybriden Lösung ausserhalb der Microsoft-Cloud bearbeitet und gespeichert werden.

Leitfaden M365 für Gemeinden
(https://www.datenschutz.ch/mitteilungen/2024/neuer-leitfaden-microsoft-365-in-gemeinden)

In einer Stichprobe hat die Datenschutzbeauftragte den Einsatz des DAP überprüft. Beim kontrollierten öffentlichen Organ untersteht ein Grossteil der Daten einem besonderen Amtsgeheimnis. Zudem werden viele besondere Personendaten bearbeitet. Der Fokus lag auf der Verwendung des DAP und der Auslagerung an Microsoft.

Bei der Kontrolle stellte die Datenschutzbeauftragte aus rechtlicher Perspektive insbesondere fest, dass der E-Mail-Server Exchange Online ohne umfassende Verschlüsselung verwendet wird und damit Zugriffe von US-Behörden auf die Inhalte der E-Mails nicht verhindert. Die Absicherung (Härtung) der Geräte und Dienste des DAP ist ungenügend. So werden beispielsweise nur acht statt zwölf Zeichen lange Passwörter verwendet. Schliesslich waren Umfang, Aufbewahrung sowie Löschung von Telemetriedaten nicht geregelt. Verbesserungspotential gibt es zudem unter anderem beim Vulnerability-Management, dem Risikomanagement sowie der Schulung und Sensibilisierung der Mitarbeitenden.

Lücken bei Prozessen und Vorgaben
Die Datenschutzbeauftragte hat das Generalsekretariat einer Direktion mit dem Fokus auf den Prozessen und Vorgaben zum Datenschutz kontrolliert. Die Kontrolle zeigte eine hohe Sensibilisierung bei den verantwortlichen Personen. Es besteht ein systematischer und sinnvoller Ansatz zum Aufbau eines Datenschutzmanagementsystems. Verbesserungspotenzial besteht in der vollständigen Umsetzung der Datenschutzanforderungen in der ganzen Direktion (wie beispielsweise Klärung der

detaillierten Verantwortlichkeiten, Vervollständigung von Prozessen zu Datenschutzvorfällen, Datenschutz-Folgeabschätzungen, Informationszugangs-, Berichtigungs- und Löschgesuchen sowie die vertragliche Regelung der Auslagerung an die Entsorgungsunternehmung).

Unrechtmässige Abfragen beim Schengener Informationssystem
Die Schweiz ist Teil des Schengener Abkommens. Damit haben Schweizer Behörden wie Polizei oder Einwohnerkontrollen Zugriff auf das Schengener Informationssystem (SIS). Darin sind unter anderem Personen gespeichert, welche zur Fahndung ausgeschrieben, vermisst oder mit einer Einreisesperre belegt sind. Die Zugriffe auf das SIS sind stark reglementiert und sind auf das notwendige Minimum zu beschränken. Wie gemäss den europäischen Erlassen gefordert, hat die Datenschutzbeauftragte in einer Zürcher Behörde überprüft, ob dies der Fall ist. Dabei wurde festgestellt, dass Mitarbeitende aus Neugier auch Prominente oder Verwandte abgefragt haben. Das ist nicht zulässig. Die Behörde wird nun die Mitarbeiter stärker schulen.

Verbesserungen bei Polis-Zugriffskontrollen
Im Polizei-Informationssystem Polis speichern die beteiligten Polizeien einen Grossteil ihrer Daten. Dazu gehören Freisprüche, Einstellungen und Nichtanhandnahmen im Strafverfahren, die von den Strafbehörden regelmässig übermittelt und von den beteiligten Polizeien nachzuführen sind. Das Polizeigesetz sieht vor, dass die Datenschutzbeauftragte die Aktualität und die Nachführung der in den Datenbearbeitungssystemen gespeicherten Daten überwacht. Eine entsprechende Kontrolle hat die Datenschutzbeauftragte im Jahr 2024 vorgenommen. Zusätzlich wurde geprüft, ob und wie die Zugriffe auf das Polis kontrolliert werden. Die Kontrolle zeigte eine ausführliche interne Prozessdokumentation für die Nachführung der polizeilichen Datenbearbeitungssysteme sowie eine umfassende Protokollierung der Zugriffe.

Eine Absicherung der mobilen Geräte für Spitex-Mitarbeitende, regelmässige Updates sowie die konsequente Verwendung einer Zwei-Faktor-Authentifizierung sind sehr wichtig. Die Datenschutzbeauftragte stellte fest, dass dies meist nicht der Fall war.

Teils erhebliche Mängel bei Spitex-Organisationen
Im Kanton Zürich gibt es 71 Spitex-Organisationen mit Leistungsaufträgen von Gemeinden. Rund 5'500 Mitarbeitende versorgen so mehrere zehntausend Patientinnen und Patienten während rund 2,5 Millionen Stunden. Die Datenschutzbeauftragte kontrollierte in einer Stichprobe die Informationssicherheit bei 17 Spitex-Organisationen. Sie haben mit ähnlichen Problemen zu kämpfen wie die Alterszentren *(https://www.datenschutz.ch/tb/2023/datenschutzprobleme-in-alters-und-pflegezentren)*, welche die Datenschutzbeauftragte 2023 kontrolliert hat. Der Mensch steht im Zentrum und nicht der Computer. Zudem ist die Fluktuation hoch und die Spitex-Mitarbeitenden sind häufig unterwegs bei den Patientinnen und Patienten.

Die festgestellten Mängel sind grundsätzlich sehr ähnlich wie bei Alterszentren. Im Gegensatz zur stationären Pflege sind Spitex-Mitarbeitende jedoch fast ausschliesslich unterwegs. Darum sind eine Absicherung der mobilen Geräte, regelmässige Updates sowie die konsequente Verwendung einer Zwei-Faktor-Authentifizierung sehr wichtig. Die Datenschutzbeauftragte stellte fest, dass dies meist nicht der Fall war.

Nur wenige Spitex-Organisationen verfügen über ein umfassendes Konzept zur Informationssicherheit und zum Datenschutz. Darum wurden bei den Kontrollen häufig Mängel bei der Schulung und Sensibilisierung, bei der Weisung über die Informationssicherheit und zum Datenschutz sowie den zugehörigen Prozessen wie bei-

spielsweise Verhalten bei Informationssicherheitsvorfällen festgestellt. Die Datenschutzbeauftragte stellt öffentlichen Organen umfangreiche Vorlagen für ein Informationssicherheits- und Datenschutz-Managementsystem *(https://www.datenschutz.ch/datenschutz-in-oeffentlichen-organen/informationssicherheit)* zur Verfügung.

In der Pflegedokumentation einer Spitex sind viele heikle Informationen über die Patientinnen und Patienten gespeichert, wie etwa Arztberichte, Dosierung von Medikamenten oder Sturzprotokolle. Damit sich Spitex-Mitarbeitende gegenseitig vertreten können, haben meist alle Nutzenden Zugriff auf sämtliche Patienteninformationen. Sie dürfen jedoch nur Informationen zu Patientinnen und Patienten lesen, für die sie auch verantwortlich sind. Um unrechtmässige Zugriffe zu erkennen, müssen Lesezugriffe aufgezeichnet und regelmässig kontrolliert werden. Dies war bei fast keiner Spitex der Fall.

Zunahme bei Meldungen von Datenschutzvorfällen

Im Jahr 2024 erhielt die Datenschutzbeauftragte 82 Meldungen zu Datenschutzvorfällen. Das ist eine leichte Zunahme gegenüber dem Vorjahr. Die meisten Vorfälle ereigneten sich in der kantonalen Verwaltung (27 Meldungen) sowie in Spitälern (28), aber zunehmend auch in Gemeinden oder Städten (13). Hauptgrund war der Versand von Personendaten an unberechtigte Personen.

Öffentliche Organe sind ein häufiges Ziel von Cyberangriffen. Eine der Hauptangriffsarten ist das sogenannte Phishing. Meist verschicken die Angreifenden dafür gefälschte E-Mails und versuchen, Mitarbeitende von öffentlichen Organen auf gefälschte Websites zu locken. Dort sollen die Mitarbeitenden Zugangsdaten eingeben. Mit diesen Zugangsdaten verschaffen sich die Angreifenden Zugang zu den IKT-Systemen der öffentlichen Organe. Davon waren im Jahr 2024 diverse Mitarbeitende von öffentlichen Organen betroffen.

Bei einem Angriff missbrauchten Angreifende die Zugangsdaten eines Mitarbeiters einer Gemeinde, um rund 800 Phishing-E-Mails von seinem Konto zu verschicken und E-Mails zu löschen. Bei einem anderen Vorfall haben Angreifende die Zugangsdaten von 80 Personen einer Schule gestohlen. Diese schickten sie anschliessend an 500 interne E-Mail-Adressen – zusammen mit antisemitischen Inhalten.

Die wichtigsten Massnahmen gegen Phishing sind:

1. Regelmässige Schulung und Sensibilisierung aller Mitarbeitenden
2. Einsatz von Multifaktor-Authentifizierung
3. Regelmässige Prüfung der E-Mail-Konten auf Kompromittierung beispielsweise über Websites wie haveibeenpwned.com und intelx.io
4. Nutzung von Filterlisten oder Proxies für den Internetverkehr
5. Erstellung eines Notfallplans für Informationssicherheitsvorfälle
6. Weitere Gegenmassnahmen sind auf der Website der Datenschutzbeauftragten oder des Bundesamtes für Cybersicherheit publiziert

Eine der Hauptangriffsarten ist das sogenannte Phishing. Meist verschicken die Angreifenden dafür gefälschte E-Mails und versuchen, Mitarbeitende von öffentlichen Organen auf gefälschte Websites zu locken.

Angriff auf Dienstleister
Ein Lieferant einer Cloud-Software wurde Ziel eines Ransomware-Angriffs. Ein öffentliches Organ verwendet die Software zur Erfassung des Energieverbrauchs der kantonalen Gebäude. Die Angreifenden haben alle Systeme des Lieferanten verschlüsselt. Die Daten konnten nach dem Vorfall aus einem Backup wiederhergestellt werden. Sämtliche Systeme werden einer vertieften Prüfung unterzogen.

Patientendaten auf Tiktok
In Stationszimmern oder Medikamentenabgaberäumen von Kliniken lagern neben Medikamenten auch viele heikle Personendaten. Darum dürfen Patientinnen und Patienten solche Zimmer nur unter Aufsicht von Fachpersonen betreten. Bei einem Datenschutzvorfall filmte ein Patient mit seinem Smartphone eine Liste mit Patientendaten und veröffentlichte die Aufnahmen anschliessend auf Tiktok. Die Klinik reagierte sofort und veranlasste deren Löschung. Zudem wurden die Mitarbeitenden unter anderem dahingehend sensibilisiert, dass sämtliche Bild- und Tonaufnahmen auf dem gesamten Gelände der Klinik verboten sind.

Hauptursache Fehlversand
Von total 82 Meldungen im Jahr 2024 waren rund zwei Drittel auf Fehler beim Versand von Daten zurückzuführen. Hauptursache waren Flüchtigkeitsfehler oder falsche Stammdaten. So verschickte beispielsweise ein öffentliches Organ eine Verfügung an eine falsche Person. Grund war die Verwechslung des Wohnortes bei gleich lautendem Namen. Eine unberechtigte Person erfuhr dadurch heikle Daten über einen Betroffenen wie beispielsweise über Sozialhilfe oder Prämienverbilligung.

Eine weitere Ursache für Fehlversendungen war die automatische Vervollständigung von E-Mail-Adressen. Mitarbeitende verschiedener öffentlicher Organe kontrollierten die automatisch erstellten Empfängeradressen ungenügend und verschickten Daten an unberechtigte Personen.

Um Fehlversendungen zu vermeiden, können unter anderem folgende Massnahmen ergriffen werden:

1. Liste führen: Damit ein öffentliches Organ weiss, wo und bei welchen Vorgängen wie viele Fehler passieren, sollte es Datenschutzvorfälle zentral aufzeichnen und klassifizieren. Dadurch können Muster erkannt und gezielte Massnahmen umgesetzt werden.
2. Schulungen und Sensibilisierungen: Flüchtigkeitsfehler passieren häufig wegen Zeitdruck oder einer hohen Fluktuation in der Belegschaft. Darum sollten Mitarbeitende regelmässig geschult und für mögliche Fehlerquellen sensibilisiert werden.
3. Anpassung automatische Vervollständigung: In E-Mail-Programmen wie Outlook sollte die automatische Vervollständigung von E-Mail-Adressen angepasst oder ausgeschaltet werden.
4. Double-Opt-in: Bei Anmeldungen für Newsletter oder bei Internetportalen ist das Double-Opt-in mittlerweile Standard. Beim Double-Opt-in werden den Nutzenden ihre Angaben in einem E-Mail zugesandt. Das Konto wird erst eröffnet, wenn der Erhalt des E-Mails bestätigt wird. Die Plattformbetreibenden sind dann sicher, dass die E-Mail-Adresse richtig ist. So können Fehler in den Stammdaten verhindert werden.
5. Plattform: Informationen können auch über eine Plattform ausgetauscht werden, statt sie per E-Mail oder Post zu senden. Ein öffentliches Organ kann beim Eintritt die persönlichen Zugangsdaten bereitstellen.
6. Vier-Augen-Prinzip: Beim Einpacken von Berichten in Couverts kann das Vier-Augen-Prinzip sinnvoll sein.
7. Rundschreiben: Sind sehr viele Stammdaten fehlerhaft, ist das Anschreiben jeder einzelnen Person die einzige Möglichkeit, die Fehler zu korrigieren.

Vorfall wegen fehlerhaftem Update
Bei einem öffentlichen Organ führte ein fehlerhaftes Update einer Smartphone-App zu unberechtigten Zugriffen. Einige Personen konnten die Personendaten anderer Personen einsehen. Das Organ handelte schnell, nahm die App innert 2,5 Stunden offline und entfernte die neue Programmbibliothek, die den Vorfall verursachte. In Zukunft werden Anpassungen an zentralen Verarbeitungsfunktionen besser kontrolliert, getestet und einem strengeren Review-Prozess unterzogen. Zudem soll der Support bei Software-Änderungen verstärkt und besser erreichbar gemacht werden.

Breites Aus- und Weiterbildungsportfolio

Die Datenschutzbeauftragte führte im Jahr 2024 insgesamt 45 Aus- und Weiterbildungen durch. Neben den bereits mehrjährig durchgeführten Weiterbildungsaktivitäten beim CAS Datenschutzberaterin und -berater, dem CAS Sozialhilfe und dem CAS KESR an der ZHAW sowie dem CAS MedLaw an der Universität Zürich, hat die Datenschutzbeauftragte vermehrt auf Gemeindeebene sowie an Veranstaltungen zu Digitalisierungsthemen referiert. Es fanden Grundlagenreferate bei Gemeinden statt, aber auch spezifische Referate, beispielsweise bei Gemeindebibliotheken oder im Bildungsbereich. Zudem wirkte die Datenschutzbeauftragte an der KI-Konferenz der Universität St. Gallen unter dem Titel «Regulierung von künstlicher Intelligenz in der Schweiz» mit und erläuterte an der egov-Stunde von egovpartner den Einsatz von M365 in Gemeinden. Sie wurde ausserdem von Bundesorganen wie der Digitalen Verwaltung Schweiz für Referate zur Cloud-Nutzung bei öffentlichen Organen eingeladen.

Zum Datenschutztag 2024 veranstaltete die Datenschutzbeauftragte ein Festival unter dem Titel «Künstliche Intelligenz – Mitbestimmen statt mitlaufen».

Zum Datenschutztag 2024 veranstaltete die Datenschutzbeauftragte ein Festival unter dem Titel «Künstliche Intelligenz – Mitbestimmen statt mitlaufen», das darauf aufmerksam machen sollte, dass Technologieentwicklung eine gesellschaftliche Diskussion benötigt, bei der auch die Bevölkerung mitbestimmen und die Entwicklung mitgestalten können muss. Das Festival umfasste Filmvorführungen im Kino Frame, Podiumsdiskussionen sowie ausgestellte Installationen.

Fester Bestandteil der Aus- und Weiterbildungstätigkeit der Datenschutzbeauftragten ist – neben dem Symposium on Privacy and Security, das 2024 unter dem Titel «Grenzlose Datennutzung – eingeschränkter Datenschutz?» stattfand – die Zürcher Datenschutztagung, die 2024 zum dritten Mal durchgeführt wurde. Die Datenschutzbeauftragte referierte zum Einmaleins der Grundrechte bei der Überwachung. Zudem erläuterte Prof. Markus Schefer die Rahmenbedingungen der Datenbearbeitung in der Cloud, Simon Carl Hardegger referierte über den Risikofaktor Mensch und Giovanni Garra zum Einsatz von Bodycams. Die Workshops beleuchteten die Themen der Videoüberwachung im öffentlichen Raum, der Überwachung am Arbeitsplatz sowie der Tätigkeit von Sozialdetektiven im Versicherungsbereich. Die Tagung wird jährlich zusammen mit der ZHAW organisiert und richtet sich vor allem an Mitarbeitende der Gemeinden im Kanton Zürich.

Digitale Langzeitarchivierung von Akten der öffentlichen Organe

Das Staatsarchiv des Kantons Zürich, das für die Langzeitarchivierung der Akten der kantonalen öffentlichen Organe verantwortlich ist, arbeitet an einer digitalen Plattform. Diese soll eine elektronische Langzeitarchivierung für Kantonsverwaltung und Gemeinden ermöglichen. Die Datenschutzbeauftragte überprüfte die geplante Plattform DIMAG im Rahmen einer Vorabkontrolle und hielt datenschutzrechtliche Massnahmen fest.

Öffentliche Organe bieten nach Ablauf von bestimmten Fristen die Akten ihrer abgeschlossenen Geschäfte dem zuständigen Archiv an. Für Gemeindeorgane sind die Gemeindearchive zuständig. Das Staatsarchiv ist für die öffentlichen Organe der kantonalen Verwaltung zuständig. Den Entscheid, ob die Akten archivwürdig sind, fällt das jeweils zuständige Archiv. Ist dies der Fall, archiviert das entsprechende Archiv die Akten und stellt sie nach Ablauf von bestimmten Schutzfristen der Öffentlichkeit zur Verfügung. Dadurch wird die Überlieferung der Verwaltungstätigkeit historisch gewährleistet. Die Schutzfristen tragen dabei der Sensitivität der in den Akten enthaltenen Personendaten Rechnung. So beträgt die Schutzfrist für Patientendokumentationen in der Regel 120 Jahre. Werden Akten vom zuständigen Archiv als nicht archivwürdig bewertet, hat das öffentliche Organ sie zu vernichten. Während in der Vergangenheit die Akten mehrheitlich physisch vorlagen und entsprechend in Räumlichkeiten zu archivieren waren, sind im Zuge der Digitalisierung neue Lösungen für digitale Akten zu erarbeiten.

Das Staatsarchiv arbeitet seit mehreren Jahren an einer digitalen Plattform, welche die elektronische Langzeitarchivierung im Kanton und in den Gemeinden nach Ablauf der gesetzlichen Aufbewahrungsfristen ermöglichen soll. Hierfür hat sich das Staatsarchiv mit den Archiven der Kantone Aargau, Appenzell Innerrhoden, Schaffhausen und Solothurn zum Archivverbund DIMAG Schweiz zusammengeschlossen. Gemeinsam suchte der Archivverbund nach einer geeigneten Lösung. Das Staatsarchiv des Kantons Zürich bot sich dabei an, eine innerkantonale Lösung zu erarbeiten, die sowohl den anderen Kantonen als auch den Gemeinden im Kanton Zürich zur Verfügung gestellt werden kann. Dabei arbeitete das Staatsarchiv mit der Abteilung Digital Solutions (DigiSol) der Direktion der Justiz und des Inneren (JI) als Entwickler, Betreiber und Hoster zusammen, und entwickelte für das Staatsarchiv die Archivierungsplattform DIMAG.

Es ist ein Prozess zu definieren, wie betroffene Personen während den Schutzfristen Zugriff zu ihren auf der Plattform gespeicherten Personendaten erhalten können.

Die Datenschutzbeauftragte überprüfte das Vorhaben im Rahmen einer Vorabkontrolle. Sie kam zum Schluss, dass in Bezug auf die Datenbearbeitung durch DigiSol keine Auslagerung vorliegt, wenn Ämter und Verwaltungseinheiten wie das Staatsarchiv, die der JI unterstellt sind, IT-Lösungen von DigiSol verwenden. Sofern jedoch Gemeinden IT-Lösungen von DigiSol beziehen, liegt ein Bearbeiten im Auftrag der Gemeinden vor, da Gemeinden nicht der JI unterstellt sind. Inhaltlich war zu begrüssen, dass die Plattform DIMAG der Archivgesetzgebung Rechnung trägt: Sobald die Akten auf der Plattform erfasst sind, werden nicht mehr die Personendaten in den Akten bearbeitet, sondern nur die vom Staatsarchiv neu angelegten Metadaten. Gemäss dem Archivgesetz darf das Archiv keine inhaltliche Veränderung der Perso-

nendaten in den Akten mehr vornehmen. Dadurch wird gewährleistet, dass der Inhalt der Akten wahrheitsgetreu überliefert werden kann. Die Datenschutzbeauftragte stellte jedoch fest, dass noch nicht festgelegt wurde, wie betroffene Personen während der Schutzfristen Zugriff zu ihren auf der Plattform gespeicherten Personendaten erhalten können. Dafür ist ein Prozess zu definieren. Weiter überprüfte die Datenschutzbeauftragte den Vertrag zwischen dem Staatsarchiv und den Gemeinden des Kantons. Sie wies darauf hin, dass eine Regelung fehlte, ob die Gemeinden als für die Datenbearbeitung verantwortlichen öffentlichen Organe oder das Staatsarchiv als für den Betrieb von DIMAG verantwortliche kantonale Stelle die Verantwortung für die öffentliche Lesbarkeit der archivierten Akten trägt. Als technische Massnahmen sind Zugriffe auf die Plattform zu protokollieren und Datenflüsse zwischen Gemeinden und dem kantonalen Staatsarchiv beziehungsweise DigiSol zu verschlüsseln.

Datenschutzaspekte beim Pilotbetrieb justitia.swiss

Ab 2026 werden auch öffentliche Organe des Kantons Zürich für ihre Justizverfahren die Schweizer E-Justizplattform justitia.swiss einsetzen. Dazu wurden kantonale Rechtsgrundlagen angepasst oder geschaffen. Die Datenschutzbeauftragte hat sich bei den entsprechenden Rechtsetzungsarbeiten regelmässig eingebracht. Für den seit Anfang des Jahres 2024 angelaufenen Pilotbetrieb hat sie ausserdem geprüft, ob eine Vorabkontrolle durchzuführen ist. Sie kam zum Schluss, dass die Datenschutzaspekte aufgrund der Zuständigkeitenregelung durch den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) zu prüfen sind.

Mit dem Ziel, die Schweizer Justiz in die digitale Zukunft zu führen, haben die eidgenössischen Gerichte und die kantonalen Straf- und Justizvollzugsbehörden das Pilotprojekt Justitia 4.0 initiiert. Der elektronische Rechtsverkehr soll für Anwältinnen und Anwälte sowie für die in einem Verfahren beteiligten Behörden obligatorisch werden. Damit alle an einem Justizverfahren beteiligten Parteien mit den Gerichten, Staatsanwaltschaften und Justizvollzugsbehörden Daten austauschen können, wurde mit justitia.swiss eine zentrale E-Justizplattform aufgebaut. Sie wird mit Inkrafttreten des Bundesgesetzes über die elektronische Kommunikation in der Justiz (BEKJ) schweizweit eingeführt. Über die cloudbasierte E-Justizplattform werden Verfahrensakten mit Personendaten und weiteren potenziell sensitiven Inhalten ausgetauscht. In justitia.swiss werden zudem weitere Personendaten wie beispielsweise Nutzendendaten bearbeitet.

Im Kanton Zürich wurden dazu Anpassungen im kantonalen Verwaltungsrechtspflegegesetz (VRG) vorgenommen sowie eine Verordnung über elektronische Verfahrenshandlungen (VeVV) erlassen, die 2026 in Kraft treten werden. In beiden Rechtsetzungsprojekten hat die Datenschutzbeauftragte mehrmals Stellung genommen und sich mit dem Projektteam ausgetauscht. Dabei konnten zentrale Aspekte des Datenschutzes und der Informationssicherheit eingebracht werden. Einige Hinweise der Datenschutzbeauftragten wurden im Vernehmlassungsentwurf der VeVV nicht berücksichtigt, flossen aber in den Vernehmlassungsentwurf für das Gesetz über digitale Basisdienste (GEB) ein: Unter anderem brachte die Datenschutzbeauftragte vor, dass für die Bearbeitung von besonderen Personendaten eine Regelung in einem formellen Gesetz notwendig ist und ein materielles Gesetz wie die VeVV dafür nicht ausreicht. Gleiches wurde für die Rechtsgrundlagen betreffend den Webzugang zu elektronischen Behördenleistungen sowie der vom Bund betriebenen Authentifizierungsdienste vorgebracht, wonach entsprechende Rechtsgrundlagen in einem Gesetz im formellen Sinne wie dem GEB vorzusehen sind.

Ab Inkrafttreten des Bundesgesetzes über die elektronische Kommunikation in der Justiz (BEKJ) wird die Plattform im Aufsichtsbereich des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) sein, weshalb die Datenschutzbeauftragte davon absah, eine eigene Vorabkontrolle durchzuführen.

Bis zum Inkrafttreten der Erlasse zum elektronischen Geschäftsverkehr finden in den Kantonen verschiedene Pilotversuche statt, um die Prozesse hinsichtlich der definitiven Einführung der Plattform zu überprüfen und Nutzerinnen und Nutzer an die Plattform zu gewöhnen. Im Kanton Zürich beteiligen sich das Verwaltungsge-

richt, ausgewählte Behörden und freiwillig teilnehmende Parteien an einem Pilotbetrieb, um erste Erfahrungen mit der Plattform zu sammeln. Der Pilotbetrieb wird von der Staatskanzlei koordiniert. Ab Inkrafttreten des BEKJ wird die Plattform im Aufsichtsbereich des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) sein, weshalb die Datenschutzbeauftragte davon absah, eine eigene Vorabkontrolle durchzuführen.

Einführung neuer digitaler Hilfsmittel in Schulen

Möchte eine Schule neue digitale Hilfsmittel wie eine Software oder App einführen, hat sie vor dem Einsatz auch die datenschutzrechtlichen Vorgaben zu prüfen.

Werden mit den geplanten digitalen Hilfsmitteln Personendaten bearbeitet, hat die Schule zunächst eine Datenschutz-Folgenabschätzung (DSFA) vorzunehmen. Wird beispielsweise eine Schulaufgabe mittels einer Software oder App gelöst und können daraus Rückschlüsse auf eine bestimmte Schülerin oder einen bestimmten Schüler gezogen werden (auch durch Login-Daten), handelt es sich dabei um eine Bearbeitung von Personendaten. Mit der DSFA bewertet die Schule die Risiken für die Grundrechte der Schülerinnen und Schüler, die mit der beabsichtigten Einführung des digitalen Hilfsmittels entstehen.

Wird beispielsweise eine Schulaufgabe mittels einer Software oder App gelöst und können daraus Rückschlüsse auf eine bestimmte Schülerin oder einen bestimmten Schüler gezogen werden, handelt es sich dabei um eine Bearbeitung von Personendaten.

Werden mit der DSFA besondere Risiken für die Grundrechte der Schülerinnen und Schüler identifiziert, unterbreitet die Schule das Vorhaben der Datenschutzbeauftragten zur Vorabkontrolle. Besondere Risiken liegen bei einem Vorhaben zur Einführung neuer digitaler Hilfsmittel beispielsweise dann vor, wenn es die Sammlung einer Vielzahl besonderer Personendaten betrifft oder mit dem Einsatz neuer Technologien (z.B. künstliche Intelligenz, KI) verbunden ist. Aufgrund der Art und der Häufigkeit der Nutzung sowie den abgefragten Inhalten kann ein Persönlichkeitsprofil eines Schulkindes entstehen. Bei einer Software für Lernförderung, die sämtliche Aktivitäten der Schülerinnen und Schüler über einen längeren Zeitraum speichert und analysiert, können bei regelmässiger Nutzung Persönlichkeitsprofile und somit besondere Personendaten bearbeitet werden. Aber auch bereits mit der Eingabe von einzelnen Informationen über die Gesundheit oder die Religion in eine Schulverwaltungs-App werden besondere Personendaten bearbeitet.

Der Einsatz von digitalen Hilfsmitteln erfolgt meist unter Beizug eines Dienstleisters. In diesen Fällen liegt ein Bearbeiten im Auftrag vor, womit zudem die Voraussetzungen für das Bearbeiten im Auftrag zu prüfen und umzusetzen sind.

Auswirkungen des neuen Datenschutzrahmens zwischen der Schweiz und der USA auf kantonale Organe

Der Bundesrat kam zum Schluss, dass der neue Datenschutzrahmen zwischen der Schweiz und den USA einen sicheren Austausch von Personendaten zwischen der Schweiz und zertifizierten US-Organisationen biete. Die Datenschutzbeauftragte hat einen Webartikel publiziert, der aufzeigt, welche Auswirkungen dieser Entscheid auf die kantonalen Organe im Kanton Zürich hat.

Der neue Datenschutzrahmen, der sogenannte Swiss-US Data Privacy Framework, trat am 15. September 2024 mit einer entsprechenden Änderung der Datenschutzverordnung des Bundes (DSV) in Kraft. In der Folge wurde die Datenschutzbeauftragte angefragt, ob die Auslagerung in Cloud-Infrastrukturen, die von US-Unternehmen wie Microsoft gehostet werden, nunmehr ohne zusätzliche Massnahmen zulässig sei. In einem Webartikel hat die Datenschutzbeauftragte dargelegt, dass diese Beurteilung für öffentliche Organe relevant ist, wenn sie Personendaten an zertifizierte Organisationen in den USA bekanntgeben. Unabhängig davon ist bei der Auslagerung der Bearbeitung von Personendaten an ein US-Unternehmen die Datenbearbeitung durch Dritte (Auslagerung) zu prüfen. Dies ist zum Beispiel im Rahmen der Nutzung einer Cloud der Fall.

Das Swiss-US Data Privacy Framework ist kein bilateraler Vertrag zwischen der Schweiz und den USA. Es handelt sich um einseitige Regelungen der USA, die zertifizierte US-Unternehmen zur Anwendung einzelner Datenschutzgrundsätze verpflichten.

Bei der Auslagerung der Bearbeitung von Personendaten an ein US-Unternehmen sind unabhängig vom Swiss-US Data Privacy Framework die kantonalen Vorgaben für die Datenbearbeitung durch Dritte zu prüfen.

Neben dem Swiss-US Data Privacy Framework gelten nach wie vor andere ausländische Gesetze wie der CLOUD Act: Der CLOUD Act verpflichtet US-Clouddienstanbieter, den zuständigen US-Behörden Zugang zu den Daten ihrer Kundinnen und Kunden zu geben, auch wenn diese Daten ausserhalb der USA gespeichert sind. Solche Zugriffe auf Personendaten sind mit dem Datenschutzrecht und dem übergeordneten Schweizerischen Recht nicht vereinbar. Dieses Vorgehen verstösst gegen den Ordre Public der Schweiz, weil es eine Umgehung des internationalen Rechtshilfewegs darstellt.

Eine Auslagerung der Bearbeitung von besonderen Personendaten an US-Unternehmen ist deshalb nach wie vor nur möglich, wenn mittels umfassender Verschlüsselung Zugriffe von US-Behörden beziehungsweise die Offenbarung von durch eine besondere Geheimnispflicht geschützten Informationen an Dritte verunmöglicht werden. Diese Bestimmungen gelten unabhängig davon, ob es sich dabei um ein nach Swiss-US Data Privacy Framework zertifiziertes Unternehmen handelt.

Spitäler finden ihren Weg mit und ohne Cloud

Die Datenschutzbeauftragte überprüfte 2024 verschiedene Applikationen, die ihr mehrere Spitäler vorlegten. Im Fokus standen dabei die Wahrung des Berufsgeheimnisses sowie der Schutz von besonderen Personendaten. Cloud-Lösungen von US-amerikanischen Anbietern sind dann zulässig, wenn die sensitiven Daten verschlüsselt sind und der US-Anbieter keine Möglichkeit zur Einsicht in die Daten hat. Einige Spitäler prüfen Applikationslösungen ohne Cloud.

Während des Jahres 2024 legten verschiedene Spitäler der Datenschutzbeauftragten Applikationen zur Vorabkontrolle vor, die vom jeweiligen Anbieter als Cloud-Lösung betrieben werden. Dabei verwendeten die Betreiber als Cloud-Speicherplattform häufig den Dienst Azure von Microsoft, Amazon Web Services (AWS) oder Google Cloud Plattform (GCP). Mit Azure stellt Microsoft den Betreibern von Applikationen Speicherplatz, Rechenleistung und Netzwerkinfrastruktur zur Verfügung. Dies ermöglicht es insbesondere auch kleinen bis mittleren Anbietern, ihre Applikationen für eine grosse Anzahl von Kundinnen und Kunden zur Verfügung zu stellen. Viele dieser Unternehmen haben ihren Sitz in den USA, betreiben aber ihre Cloud-Speicherplattformen auch auf Servern in der Schweiz. Will ein Spital eine Applikation einsetzen, die in einer solchen Cloud gehostet wird, handelt es sich um eine Auslagerung an den jeweiligen Cloudanbieter. Wird beispielsweise die Speicherplattform Azure von Microsoft verwendet, bearbeitet Microsoft Personendaten im Auftrag des Spitals. In diesem Fall bleibt das Spital für die Bearbeitung der Personendaten verantwortlich. Hostet ein Spital Software-Lösungen in der Azure-Cloud, die für die Bearbeitung von Patientendaten eingesetzt werden, besteht die Gefahr, dass vertrauliche Patientendaten, die dem Berufsgeheimnis unterstehen, in die Cloud gelangen und Microsoft so Zugriff auf die Patientendaten erhält. Dies würde eine Verletzung der Schweigepflicht darstellen.

Die Datenschutzbeauftragte überprüfte im Rahmen einer Vorabkontrolle Dragon Medical One, eine in Azure gehostete Spracherkennungsapplikation, die in Spitälern eingesetzt wird, um die Patientendokumentationen zu führen. Dabei sprechen die Mitarbeitenden des Spitals einen Text ein, der in der Cloud von Azure in eine Textdatei umgewandelt wird, die in die Patientendokumentation integriert werden kann.

Im Rahmen von Vorabkontrollen wurde der Datenschutzbeauftragten die Spracherkennungssoftware Voize unterbreitet. Diese auf künstlicher Intelligenz basierende Software wird in Heimen für die mündliche Datenerfassung eingesetzt. Pflegemitarbeitende können sie beispielsweise verwenden, um Pflegedaten zu Heimbewohnenden über ein betriebliches Smartphone mündlich zu erfassen. Die Sprachdaten werden lokal auf dem Smartphone zu Text umgewandelt, der in die Pflegedokumentation übertragen werden kann. Die Applikation wird von der Voize GmbH entwickelt und betrieben, aber auf den Servern von AWS gehostet. Das KI-Modell, das auf den Servern der AWS gespeichert ist, wertet mit Machine Learning einzelne Einträge der Pflegemitarbeitenden aus, um die Sprachumwandlung mit entsprechenden Aktualisierungen zu verbessern.

Weiter beurteilte die Datenschutzbeauftragte das Vorhaben eines Spitals, eine Applikation einzuführen, die es den Patientinnen und Patienten ermöglicht, per Bluetooth via Mobiltelefon-App eine Videokonferenz mit ihrer behandelnden Ärztin oder ihrem behandelnden Arzt zu vereinbaren. Die Applikation stellt dem Spital Informationen zu bei den Patientinnen und Patienten eingesetzten Medizinprodukten direkt via App zur Verfügung und leitet eine Anfrage zur Videotelefonie an die zuständige Ärztin oder den zuständigen Arzt weiter. So können virtuelle Sprechstunden mit di-

rekt verfügbaren Personendaten abgehalten werden. Die Videotelefonie-Applikation wird dabei in Microsoft Azure gehostet.

Bearbeitet ein Cloud-Anbieter im Auftrag eines Spitals Personendaten, bleibt das Spital für die Bearbeitung der Personendaten verantwortlich.

Bei der Nutzung einer Spracherkennungssoftware oder einer Applikation für Videokonferenzen werden Personendaten in die Cloud des Anbieters übermittelt. Dort werden sie durch die Betreiber der Software bearbeitet. In den konkreten Fällen handelte es sich sowohl um die Stimmdaten des Personals als auch die Personendaten der Patientinnen und Patienten. Bei Patientendaten gilt das Berufsgeheimnis, weshalb Dritte keinen Zugriff auf die Patientendaten in der Cloud haben dürfen. Ansonsten hat das Spital beziehungsweise das Heim keine Kontrolle mehr über die Personendaten. Handelt es sich bei den Betreibern der Spracherkennungssoftware um europäische Unternehmen, die an die DSGVO gebunden sind, dürfen diese Zugriff auf die Patientendaten erhalten, sofern sie vertraglich dem Weisungsrecht des Spitals beziehungsweise des Heims unterstellt werden. Für Unternehmen aus den USA wie Microsoft gilt jedoch, dass sie aufgrund des CLOUD Acts von US-Behörden verpflichtet werden können, Personendaten herauszugeben, auch wenn diese ausserhalb der USA gespeichert sind. Um eine solche Verletzung zu verhindern, ist sicherzustellen, dass US-Unternehmen keinen Zugriff auf diese Patientendaten erhalten.

Zudem prüfte die Datenschutzbeauftragte den geplanten Einsatz einer digitalen Patientinnen- und Patientenbetreuung zur Begleitung von Operationen in einem Spital. Neben individuell zugeschnittenen Physiotherapie-Übungen soll die Applikation auch den Regenerationsprozess nach der Operation dokumentieren (unter anderem mit Angaben aus gängigen Gesundheitsapplikationen wie beispielsweise Google Fit) und die Kommunikation mit Ärztinnen und Ärzten ermöglichen. Die Lösung wird von einem US-Medizinaltechnik-Unternehmen angeboten, die Datenhaltung erfolgt in der Microsoft-Azure-Infrastruktur in Deutschland. Auch hier hat die Datenschutzbeauftragte darauf hingewiesen, dass Dritte keine Einsichtsmöglichkeit in die Patientinnen- und Patientendatendaten haben dürfen. Das Spital muss dies mittels ausreichender Verschlüsselung zuverlässig verhindern.

Datenbearbeitungen müssen nicht zwingend in der Cloud erfolgen. Einige Spitäler haben Varianten geprüft, um Patientendaten mit Microsoft-Office-Applikationen zu bearbeiten, ohne dass hierfür auf die Microsoft Cloud zurückgegriffen werden muss. Sie legten der Datenschutzbeauftragten Datenschutz-Folgenabschätzungen vor, die aufzeigten, dass sie für die Verwendung von Office Produkten wie Word, Excel, PowerPoint und Outlook auf die Cloud von Microsoft verzichtet haben. Stattdessen haben sie Lizenzen dieser Produkte erworben, die den lokalen Betrieb auf eigenen Servern vor Ort (on-premises) ermöglichen. Auch wenn nicht alle M365-Produkte lokal auf eigenen Servern gehostet werden können, ermöglicht dies für gewisse Applikationen die datenschutzkonforme Bearbeitung von Patientendaten mit Applikationen von Microsoft und eröffnet den Weg für den hybriden Betrieb, bei dem die Datenbearbeitung in der Microsoft Cloud nur für administrative Personendaten des Spitals vorgesehen ist und Patientendaten lokal bearbeitet werden.

Datenschutz in Kirchgemeinden

Die Datenschutzbeauftragte hat im Jahr 2024 erstmals Kirchgemeinden kontrolliert. Unsichere mobile Geräte, fehlende Sicherheitsvorgaben und veraltete Systeme bergen erhebliche Risiken für den Datenschutz bei Kirchgemeinden. Im Nachgang zu den durchgeführten Kontrollen hat die Datenschutzbeauftragte mit dem Synodalrat der katholischen Kirche des Kantons Zürich und der evangelisch-reformierten Landeskirche des Kantons Zürich eine unterstützende Zusammenarbeit lanciert, die den Kirchen die Umsetzung der festgehaltenen Massnahmen erleichtern soll.

Die Kirchgemeinden im Kanton Zürich, die gemäss Kantonsverfassung anerkannte öffentlich-rechtliche Körperschaften des Kantons Zürich sind, unterstehen der Aufsicht der Datenschutzbeauftragten des Kantons Zürich. Die Kantonsverfassung des Kantons Zürich anerkennt als Körperschaften des öffentlichen Rechts die evangelisch-reformierte Landeskirche und ihre Kirchgemeinden, die römisch-katholische Körperschaft und ihre Kirchgemeinden sowie die christkatholischen Kirchgemeinden.

Im Jahr 2024 führte die Datenschutzbeauftragte in sieben Kirchgemeinden der römisch-katholischen und evangelisch-reformierten Kirche Kontrollen durch. Dabei zeigten sich ähnliche Herausforderungen. Die Kontrollen ergaben, dass die kantonalen Kirchen dem Datenschutz grosse Bedeutung zumessen und bei den Verantwortlichen ein hohes Bewusstsein für Datenschutzthemen vorliegt. Sie schätzten die Verbesserungsvorschläge der Datenschutzbeauftragten im Rahmen der Kontrolle sowie die Aussensicht auf ihre IT-Infrastruktur. Sie setzen seither die empfohlenen Massnahmen der Datenschutzbeauftragten zielführend um. Unterstützende Beratung und praxisnahe Hilfestellungen auf der Website der Datenschutzbeauftragten begleiten die Kirchgemeinden und erleichtern die Umsetzung in der täglichen Arbeit.

Die kantonalen Kirchen messen dem Datenschutz grosse Bedeutung zu und setzen die empfohlenen Massnahmen der Datenschutzbeauftragten um.

Aufgrund der Arbeit von professionellen IT-Dienstleistern waren technische Sicherheitsmassnahmen wie beispielsweise das Backup der Daten bei allen Kirchgemeinden vorhanden. Verbesserungspotenzial besteht insbesondere bei der sicheren Nutzung mobiler Geräte, dem Schutz geschäftlicher Daten im Homeoffice und bei der Schulung, Sensibilisierung sowie bei detaillierten Vorgaben zur Informationssicherheit wie beispielsweise durch ein Informationssicherheitskonzept.

Nach den ersten Kontrollen hat die Datenschutzbeauftragte eine Zusammenarbeit mit dem Synodalrat der katholischen Kirche des Kantons Zürich und der evangelisch-reformierten Landeskirche des Kantons Zürich gestartet. Dabei wurden die Beteiligten über die Schwachstellen informiert und sie erhielten Vorlagen, um diese zu schliessen. Die Vorlagen der Datenschutzbeauftragten werden durch den Synodalrat und durch die Landeskirche bezüglich der Eigenheiten der Kirchgemeinden angepasst. Danach werden diese den Kirchgemeinden zur weiteren Bearbeitung zur Verfügung gestellt. Die Datenschutzbeauftragte wird den Synodalrat, die Landeskirche und die Kirchgemeinden begleitend beraten und die Ergebnisse im Rahmen der Nachkontrolle überprüfen.

Wann dürfen Ärztinnen und Ärzte Patientendaten an die Polizei bekanntgeben?

Die Datenschutzbeauftragte beriet 2024 diverse Spitäler bei der Frage, ob Ärztinnen und Ärzte Personendaten von Patientinnen und Patienten an die Polizei bekanntgeben dürfen. Dabei zeigte sich, dass häufig unklar ist, wann Angaben über Patientinnen und Patienten an Strafbehörden mitgeteilt werden müssen und wann dies nicht erlaubt ist.

Ärztinnen und Ärzte sowie ihre Hilfspersonen unterliegen dem Berufsgeheimnis. Dieses gilt gegenüber allen Personen mit Ausnahme der Patientin oder des Patienten selbst. Das Berufsgeheimnis ist auch über deren Tod hinaus zu wahren. Für die Durchbrechung der Schweigepflicht braucht es eine explizite gesetzliche Grundlage, die zur Bekanntgabe von Personendaten ermächtigt oder verpflichtet. Alternativ kann im Einzelfall vorgängig die informierte Einwilligung der betroffenen Patientin oder des betroffenen Patienten eingeholt werden oder eine Entbindung von der Gesundheitsdirektion eingeholt werden. Ausserhalb dieser Möglichkeiten macht sich eine Ärztin oder ein Arzt beziehungsweise ihre Hilfsperson strafbar, wenn sie Patientendaten bekanntgibt.

Es gibt wenige gesetzliche Bestimmungen, die den Ärztinnen und Ärzten die Pflicht auferlegen, Strafbehörden zu kontaktieren und Daten über Patientinnen und Patienten bekanntzugeben. Kommt es beispielsweise zu einem Todesfall infolge einer Fehlbehandlung oder ist die Ursache unklar, müssen die Ärztinnen und Ärzte den aussergewöhnlichen Todesfall den Strafverfolgungsbehörden melden. Gleiches gilt für den Tod einer Patientin oder eines Patienten nach einem Unfall oder bei Suizid.

Weiter muss das Spital immer Meldung an die Polizei machen, wenn bei Patientinnen und Patienten ernsthafte Anzeichen von gefährlichen übertragbaren Krankheiten an Menschen und Tieren bestehen. Dies soll verhindern, dass es zu einer Epidemie kommt und Infektionsquellen möglichst früh isoliert werden können.

> Für die Durchbrechung der Schweigepflicht braucht es eine explizite gesetzliche Grundlage, die zur Bekanntgabe von Personendaten ermächtigt oder verpflichtet.

Bestehen Anzeichen auf eine Straftat, die nicht unter einen Todesfall infolge Fehlbehandlung, Unfall oder Selbsttötung fällt, ist die Situation schwieriger zu beurteilen. Liegt beispielsweise eine schwere Körperverletzung vor oder bestehen Hinweise auf Sexualdelikte, kann die Ärztin oder der Arzt eine Meldung an die Polizei und die Opferhilfe machen. Es handelt sich in diesen Fällen jedoch um ein Melderecht und keine Pflicht. Die Ausübung von Rechten ist immer mit einem Ermessensspielraum verbunden: Es liegt in der Verantwortung der Ärztin oder des Arztes, ob eine Meldung erfolgen soll oder nicht. Eine solche Entscheidung ist für Ärztinnen und Ärzte im hektischen Spitalalltag schwierig zu fällen und sie laufen Gefahr, ihre ärztliche Schweigepflicht zu verletzen, wenn die Patientin oder der Patient nicht einwilligt oder einwilligen kann. In diesen Fällen wird oft eine Entbindung vom Berufsgeheimnis bei der Gesundheitsdirektion eingeholt.

Wenn Strafbehörden gegen Patientinnen und Patienten in einem Spital ermitteln, gelten die Regeln der Strafprozessordnung. Für Durchsuchungen muss die Polizei beispielsweise einen entsprechenden Befehl vorweisen können, der die Patientin

oder den Patienten und seine Räumlichkeiten konkret nennt. In dringenden Fällen kann der Befehl mündlich erfolgen, ansonsten gilt das Schriftformerfordernis.

Möglicherweise erhebt ein Spital Strafanzeige gegen eine Patientin oder einen Patienten. Müssen dafür Patientendaten an die Strafbehörden bekanntgegeben werden, ist die Entbindung von der Gesundheitsdirektion einzuholen.

Bekanntgabe von Gesundheitsdaten von Schülerinnen und Schülern bei einem Schulwechsel oder -übertritt

Kommt es zu einem Schulwechsel oder -übertritt von Schülerinnen und Schülern, stellt sich die Frage, welche Informationen die (bisherige) Schule an die neue Schule bekanntgeben darf.

Bei einem Schulwechsel oder -übertritt gibt die bisherige Schule der neuen Schule die für die Aufnahme notwendigen Personendaten und besonderen Personendaten von Schülerinnen und Schülern bekannt. Für diese Bekanntgabe im Rahmen des Schulwechsels oder -übertritts besteht eine Rechtsgrundlage.

Die Bekanntgabe hat unter Einhaltung des Grundsatzes der Verhältnismässigkeit zu erfolgen. Verhältnismässig ist eine Datenbekanntgabe an die neue Schule, wenn sie geeignet und erforderlich ist für die Aufgabenerfüllung der neuen Schule und ein vernünftiges Verhältnis zwischen dem verfolgten Zweck und der Datenbearbeitung besteht. Dies ist beispielsweise für die Aufnahme der Schülerinnen und Schüler in die neue Schule der Fall.

Neben Personendaten wie Vorname, Name, Adresse, Geschlecht, Heimatort, Muttersprache und Geburtsdatum sowie auch Angaben über die Inhaber der elterlichen Sorge darf die bisherige Schule der neuen Schule auch besondere Personendaten wie Informationen über die Gesundheit (ärztliche Schülerkarte oder Zahnkontrollheft) bekannt geben, da diese Informationen für die schulischen Belange geeignet und notwendig sind.

In diesen Fällen ist das Berufsgeheimnis von Schulpsychologinnen und Schulpsychologen zu beachten.

Eine Besonderheit ergibt sich bei der Bekanntgabe von schulpsychologischen Informationen. In diesen Fällen ist das Berufsgeheimnis von Schulpsychologinnen und Schulpsychologen zu beachten. Oft kommt es vor, dass bei einem Schulwechsel oder -übertritt die Weitergabe von schulpsychologischen Berichten verlangt wird. Der schulpsychologische Dienst erstellt den Bericht grundsätzlich nach einer schulpsychologischen Abklärung. Wurde diese Abklärung aufgrund eines gemeinsamen Auftrages der Schule mit den Eltern eines Kindes vorgenommen, müssen die Eltern vorgängig über die Bekanntgabe der schulpsychologischen Informationen informiert werden. Nach deren Einwilligung in die Weitergabe kann ein schulpsychologischer Bericht allen Auftraggebenden und dem neu zuständigen Dienst zugestellt werden. Damit willigen die Eltern als gesetzliche Vertreter des betroffenen Kindes auch in die Offenbarung des dem Berufsgeheimnis unterstehenden Berichts ein.

Wenn keine Einwilligung der Eltern vorliegt, können spezifische Angaben aus den Berichten (wie weiterzuführende Massnahmen) gestützt auf die oben erwähnte Rechtsgrundlage der neuen Schule bekannt gegeben werden. Dies ist jedoch nur möglich, wenn die neue Schule die Angaben für ihre Aufgabenerfüllung benötigt.

Falls die schulpsychologische Abklärung hingegen nur im Auftrag der Schulpflege erfolgte, kann der schulpsychologische Dienst seinen gesamten Bericht im Rahmen der Amtshilfe der neuen Schule bekanntgeben. Zusätzlich müsste eine Entbindung vom Berufsgeheimnis durch die zuständige Behörde erteilt werden.

Welche Unterlagen bei einem Schulwechsel oder -übertritt zwischen den Schulen ausgetauscht werden dürfen, ist im Einzelfall durch die betreffenden Schulen zu entscheiden. Dabei ist zu beachten, dass vor der Datenbekanntgabe eine Interessenabwägung zwischen den Interessen des Kindes und der zu erfüllenden Aufgabe der Schule vorzunehmen ist.

Weitergabe von Patientendaten an die Seelsorge gesetzlich vorgesehen

Eine Gesundheitsinstitution kontaktierte die Datenschutzbeauftragte bezüglich der Handhabung der seelsorgerischen Betreuung im Klinikalltag.

Konkret stand ihre Meldung von neuen und potenziell zu betreuenden Patientinnen und Patienten an die Spitalseelsorge zur Diskussion. Da damit Angaben zur jeweiligen Konfession gemacht werden und zudem sichtbar wird, dass ein medizinisches Behandlungsverhältnis besteht, handelt es sich um eine Bekanntgabe von besonderen Personendaten.

Die gesetzliche Bestimmung zur Seelsorge in Zürcher Spitälern stellt eine hinreichende Grundlage für die Bekanntgabe von Angaben zu neuen Patientinnen und Patienten an die jeweilige Seelsorge dar.

Die gesetzliche Bestimmung zur Seelsorge in Zürcher Spitälern stellt eine hinreichende Grundlage für die Bekanntgabe von Angaben zu neuen Patientinnen und Patienten an die jeweilige Seelsorge dar. Im Sinne des Verhältnismässigkeitsprinzips ist jedoch darauf zu achten, dass nur diejenigen Angaben bekanntgegeben werden, die für die Besuchsplanung notwendig sind. Davon unangetastet bleibt die Entscheidungsfreiheit der Patientinnen und Patienten, seelsorgerische Unterstützungsangebote anzunehmen oder abzulehnen.

Neues Musterreglement für Videoüberwachung im öffentlichen Raum

Öffentliche Organe des Kantons Zürich setzen Videoüberwachung beispielsweise bei öffentlichen Anlagen oder an Schulen zum Schutz von Personen, Gebäuden und Sachwerten ein.

Eine Videoüberwachung ist datenschutzkonform, wenn sie dazu dient, den Betrieb der öffentlichen Anlage ohne Störung aufrecht zu erhalten und die Sicherheit nicht mit anderen, weniger in die Persönlichkeitsrechte eingreifenden Mitteln gewährleistet werden kann. Die Überwachung ist räumlich und zeitlich auf das absolut Notwendige zu beschränken. Die Aufbewahrungsfrist der Aufnahmen sollte möglichst kurz sein. Es ist zudem auf die Videoüberwachung hinzuweisen.

Zur Unterstützung der öffentlichen Organe hat die Datenschutzbeauftragte ein Musterreglement für die Videoüberwachung erarbeitet, das auf der Website der Datenschutzbeauftragten heruntergeladen und zur eigenen Verwendung angepasst werden kann.

Das öffentliche Organ erlässt und publiziert ein Reglement, das die Modalitäten, insbesondere auch diejenigen der Auswertung, transparent regelt. Zur Unterstützung der öffentlichen Organe hat die Datenschutzbeauftragte ein Musterreglement für die Videoüberwachung erarbeitet, das auf der Website der Datenschutzbeauftragten heruntergeladen und zur eigenen Verwendung angepasst werden kann.

Links zu den Hilfsdokumenten:

- Anleitung Musterreglement Videoüberwachung
- Musterreglement Videoüberwachung
- Leitfaden Videoüberwachung durch öffentliche Organe (ohne Strafverfolgungsbehörden)

Sperrmöglichkeit für Grundbuchdaten im Internet

Seit Ende 2024 können Grundeigentümerinnen und Grundeigentümer ihre Eigentümerdaten für den GIS-Browser sperren lassen. Die Datenschutzbeauftragte regte an, die Möglichkeit einer Sperre der Grundeigentümerdaten zu schaffen.

Im Jahr 2023 wurde im Kanton Zürich die Möglichkeit geschaffen, Grundeigentümerdaten über das kantonale geografische Informationssystem (GIS-Browser) im Internet abzurufen. Die Datenschutzbeauftragte hielt als Antwort auf mehrere Anfragen von Privatpersonen fest, dass für diese Veröffentlichung von Grundbuchdaten eine genügende Rechtsgrundlage in der kantonalen Grundbuchverordnung besteht und das geltende Recht in diesem Bereich keine Möglichkeit einer Datensperre vorsieht (vgl. dazu Tätigkeitsbericht 2023). Sie regte zudem beim zuständigen Notariatsinspektorat an, die Möglichkeit einer Sperre der elektronischen Datenbekanntgabe aus dem Grundbuch im kantonalen Grundbuchrecht zu schaffen, wie dies in verschiedenen anderen Kantonen bereits der Fall ist.

Seit Ende 2024 können Grundeigentümerinnen und Grundeigentümer die Sperrung der Eigentümerdaten im GIS-Browser verlangen.

Seit dem 1. Dezember 2024 können Grundeigentümerinnen und Grundeigentümer die Sperrung der Eigentumsdaten im GIS-Browser verlangen. Dafür wurde in der kantonalen Grundbuchverordnung eine rechtliche Grundlage geschaffen. Über die Website der Notariate Zürich *(https://www.notariate-zh.ch/deu/grundbuch/elektronische-eigentumsabfrage/sperrung-entsperrung/)* kann die Sperrung mittels Formular *(https://www.notariate-zh.ch/deu/grundbuch/elektronische-eigentumsabfrage/sperrung-entsperrung/)* verlangt werden. Eine allfällige Entsperrung erfolgt über den gleichen Kanal.

Die neue Sperrmöglichkeit besteht nur für die Eigentumsabfrage über den kantonalen GIS-Browser. Eine Sperrung der über das Grundbuchamt erhältlichen Grundbuchdaten ist nicht möglich, da es sich beim Grundbuch um ein öffentliches Register handelt.

Smart Prisons Zürich wird umgesetzt

Im Jahr 2024 hat das Amt für Justizvollzug und Wiedereingliederung (JuWe) das Projekt Smart Prisons Zürich (SMAZH) der Datenschutzbeauftragten zur Vorabkontrolle vorgelegt. Mit dem Projekt sollen inhaftierten Personen in den Institutionen des JuWe IT-Geräte zur Verfügung gestellt werden.

Mit SMAZH sollen Wiedereingliederung, Normalisierung und Gewährleistung des Betriebs des Justizvollzugs in den Hafträumen gefördert werden. Die modulare Lösung ermöglicht es inhaftierten Personen, über diese IT-Geräte verschiedene Dienste in Anspruch zu nehmen. Dazu gehören etwa elektronische Formulare, Finanzmanagement, Infoboard, Kalender, Nachrichtenkomponenten sowie Telefon- und Videokommunikation.

Durch Prozesse ist sicherzustellen, dass den betroffenen Personen ihre Rechte gewährt werden.

Die Datenschutzbeauftragte hat das System in rechtlicher und organisatorisch-technischer Hinsicht überprüft und ein sehr durchdachtes und weitgehend datenschutzkonformes System vorgefunden. Sie hat einige rechtliche Hinweise gegeben und wenige Massnahmen im technisch-organisatorischen Bereich vorgeschlagen. Insbesondere hat sie darauf hingewiesen, dass die im Rahmen des Projekts vorgesehenen Bearbeitungen von Personendaten in Ergänzung der im Straf- und Justizvollzugsgesetz (StJVG) und der zugehörigen Verordnung verankerten Rechtsgrundlagen in der Verordnung oder einem Reglement ausführlich zu regeln sind. Ebenso hat sie festgehalten, dass durch Prozesse und Kontrollen sichergestellt werden muss, dass keine über die vorgesehenen Zwecke hinausgehende Bearbeitung von Personendaten erfolgt und nur die für diese Zwecke notwendigen Bearbeitungen durchgeführt werden.

Durch Prozesse ist sicherzustellen, dass den betroffenen Personen ihre Rechte gewährt werden. Falls Entwicklungsprozesse, Wartung und Support den Zugriff der Leistungserbringerin auf besondere Personendaten erfordern, sind diese durch spezielle Massnahmen zu schützen.

Generative künstliche Intelligenz für öffentliche Organe

Möchten öffentliche Organe künstliche Intelligenz (KI) für die Erfüllung ihrer Aufgaben nutzen, sind dafür verschiedene datenschutzrechtliche Abklärungen zu treffen. Der Datenschutzbeauftragten wurden 2024 erste Projekte zur künstlichen Intelligenz vorgelegt. Öffentliche Organe erstellten erste Konzepte zu Large Language Models (LLM), die beispielsweise medizinische Berichte mit wenigen Eingabetexten erstellen sollen.

Die Datenschutzbeauftragte hat erstmals den Einsatz generativer KI im Rahmen einer Vorabkontrolle beurteilt. Eine Gemeinde wollte ihren Mitarbeitenden eine Plattform mit Zugang zu einem eigenen LLM zur Verfügung stellen, die sie im beruflichen Alltag unterstützen soll. Das LLM wird durch einen Dritten im Auftrag der Gemeinde betrieben. Dabei soll das LLM laufend optimiert werden, so dass es für die Bedürfnisse der Gemeinde massgeschneidert wird.

Möchte ein öffentliches Organ wie zum Beispiel eine Gemeindeverwaltung eine KI für die Erfüllung ihrer Aufgaben einsetzen, hat sie sich in einem ersten Schritt zu fragen, für welche Aufgaben sie die KI einsetzen möchte: Sollen Briefe an Einwohnerinnen und Einwohner standardisiert vorformuliert werden? Soll die KI eine vollständige Steuerveranlagungsverfügung erstellen können? Geht es darum, Bau- oder Sozialhilfegesuche in das LLM einzugeben, damit dieses dann vorformulierte Entscheide für den Mitarbeitenden der Gemeinde erstellt?

In einem nächsten Schritt hat das öffentliche Organ abzuklären, ob für diese Aufgabenerfüllung genügende Rechtsgrundlagen bestehen. Werden besondere Personendaten wie Gesundheitsdaten oder Personendaten von Sozialhilfempfangenden eingegeben, muss dafür eine Grundlage in einem Gesetz im formellen Sinn vorliegen.

Die Verantwortung für die Bearbeitung von Personendaten mit einer KI liegt beim öffentlichen Organ. Die Gemeinde muss daher beispielsweise bei der Nutzung eines LLM protokollieren können, welche Mitarbeitende für welche Aufgabe das LLM verwenden. Nur so kann die Gemeinde Rechenschaft ablegen, dass das LLM gemäss den Rechtsgrundlagen verwendet wird. Ferner ist die Verantwortung innerhalb der Organisation eines öffentlichen Organs festzulegen. Es ist mit internen Reglementen und Weisungen zu regeln, ob die jeweiligen Mitarbeitenden die vom LLM erstellten Antworten kontrollieren und nach welchen Regeln eine Überprüfung vorzunehmen ist.

Projekte zur Nutzung von KI unterbeitet das öffentliche Organ der Datenschutzbeauftragten zur Vorabkontrolle. Dafür reicht es ihr alle Dokumentationen ein.

Schliesslich hat das öffentliche Organ aufzuzeigen, was mit den Eingabetexten, also den Prompts, passiert, wenn Mitarbeitende diese an das LLM übermitteln: Werden sie für das Training der KI verwendet? Werden sie gelöscht? Wer hat beim Dritten Einsicht in die Personendaten, die das öffentliche Organ an das LLM übermittelt? Über welche Trainingsdaten verfügt das LLM? Diese Fragen klären die öffentlichen Organe mit entsprechenden Dokumentationen ab.

Projekte zur Nutzung von KI unterbeitet das öffentliche Organ der Datenschutzbeauftragten zur Vorabkontrolle. Dafür reicht es ihr alle Dokumentationen ein. Die Datenschutzbeauftragte prüft das Projekt und hält in einer Stellungnahme Hinweise und Massnahmen zur datenschutzkonformen Umsetzung des Projekts fest. Bei der Gemeinde überprüfte die Datenschutzbeauftragte, ob die Dritten, die das LLM betrieben, Zugriff auf die von der Gemeinde eingegebenen Personendaten haben. Sie stellte dabei fest, dass die Personendaten zwar auf den Servern eines Unterauftragnehmers fliessen und anschliessend gelöscht werden sollen, der Löschprozess jedoch nicht genügend dokumentiert war. Entsprechend hielt sie fest, dass die Gemeinde zusammen mit den Dritten ein detailliertes Löschkonzept zu verfassen und genau aufzuzeigen hat, ob und wie lange die Dritten auf die Personendaten der Gemeinde zugreifen könnten. Zudem stellte sie bei der Überprüfung fest, dass es sich beim LLM um eine Open-Source-Lösung handelte, die lokal in Rechenzentren der Schweiz betrieben wurde.

Mit selbstgemachter KI zum Ziel

Die Arbeitslosenkasse des Kantons Zürich ist die Ansprechpartnerin für Einwohnerinnen und Einwohner bezüglich Angelegenheiten zu Arbeitslosen-, Insolvenz-, Kurzarbeits- und Schlechtwetterentschädigung. Sie klärt die Ansprüche auf Entschädigung ab, bietet Beratungen zur Arbeitslosenversicherung an und richtet die Entschädigungszahlungen an die Einwohnerinnen und Einwohner aus.

Diese Entschädigungszahlungen sind komplex, weshalb es in der Praxis zu Verzögerungen kommen kann. Dies ist für die Betroffenen unbefriedigend, da sie oftmals rasch auf die Entschädigungszahlungen angewiesen sind. Die Verzögerung entsteht durch die aufwendige Berechnung des versicherten Verdienstes einer betroffenen Person. Sie stützt sich nicht nur auf die Angaben der entsprechenden Person, sondern auch auf Referenzwerte aus verschiedenen Plattformen und Informationssystemen des Kantons und des Bundes, beispielsweise dem SECO Datamart, einer Datenbank, die vom Staatssekratariat für Wirtschaft (SECO) betrieben wird und Beschäftigungsstatistiken, Branchenanalysen und wirtschaftliche Indikatoren umfasst.

Die Datenschutzbeauftragte begrüsste, dass sich diese KI-Lösung ausschliesslich lokal auf den Rechnern der Mitarbeitenden des Amts für Arbeit beziehungsweise der Arbeitslosenkasse befindet.

Um diesen Prozess zu vereinfachen, hat das Amt für Arbeit einen KI-Algorithmus entwickelt, der eine Berechnung des versicherten Verdienstes anhand der genannten Plattformen und Informationssysteme rasch vornehmen kann. Der durch die KI berechnete Betrag kann im Anschluss von den Mitarbeitenden der Arbeitslosenkasse als Referenzwert betrachtet werden, damit sie keine mehrmaligen Kontrollen durchführen müssen. Die Datenschutzbeauftragte beurteilte dieses Vorhaben und begrüsste, dass sich diese KI-Lösung ausschliesslich lokal auf den Rechnern der Mitarbeitenden des Amts für Arbeit beziehungsweise der Arbeitslosenkasse befindet. Die zuständigen öffentlichen Organe haben damit eine vollständige Kontrolle über die Datenbearbeitungen mit dem Algorithmus und können Rechenschaft über diese Datenbearbeitungen abliefern. Zudem stellt ein entsprechendes Rollen- und Berechtigungskonzept sicher, dass nur jene Mitarbeitende Zugriff auf die KI haben, die dies für die Erfüllung ihrer Aufgaben, also die Berechnung des versicherten Verdienstes, benötigen. Diese zielgerichtete Verwendung künstlicher Intelligenz bringt praktischen Nutzen und bietet weniger Risiken als die Verwendung einer unspezifischen generativen KI von einem Drittanbieter, die nicht spezifisch für diesen Anwendungsfall entwickelt wurde.

Teilrevision Polizeigesetz: Entwurf liegt vor

Die Sicherheitsdirektion erarbeitet seit 2021 eine Teilrevision des kantonalen Polizeigesetzes. Die Revisionsbestrebungen betreffen im Wesentlichen den Einsatz von technischen Überwachungsgeräten zur Feststellung des Standortes von Personen oder Sachen (GPS-Ortungsgeräte), die Videoüberwachung des Strassenverkehrs und die automatisierte Fahrzeugfahndung, den Einsatz von Software zur Informationsbeschaffung im virtuellen Raum und den überkantonalen polizeilichen Datenaustausch. Die Datenschutzbeauftragte berät die Sicherheitsdirektion seit Aufnahme der Revisionsarbeiten punktuell zu datenschutzrechtlichen Fragen und nimmt zu den erarbeiteten Revisionsentwürfen Stellung. 2023 hat sich die Datenschutzbeauftragte im Rahmen der Vernehmlassung zum Entwurf geäussert.

Im Nachgang zum Vernehmlassungsverfahren hat die Datenschutzbeauftragte 2024 die Sicherheitsdirektion weiter beraten, um die im Vernehmlassungsverfahren bemängelten Bestimmungen des Revisionsentwurfes zu überarbeiten. Die wesentlichen Kritikpunkte der Datenschutzbeauftragten betrafen nach wie vor die Unbestimmtheit zentraler Bestimmungen des Entwurfes sowie vereinzelt die Unverhältnismässigkeit gewisser vorgesehener Bearbeitungen von Personendaten. Sie bemängelte, dass die vorgesehene Bestimmung über die automatisierte Verkehrsfahndung in verschiedenen Punkten von der bundesgerichtlichen Rechtsprechung abweicht und forderte eine Einschränkung der Bestimmung. Sie hielt ausserdem fest, dass die Bestimmung zum polizeilichen Datenaustausch in der vorgesehenen Form dem verfassungsrechtlichen Gebot der hinreichenden Bestimmtheit nicht genüge.

Die Hinweise der Datenschutzbeauftragten wurden im Zuge dieser Arbeiten teilweise, aber nicht vollständig berücksichtigt. Der Regierungsrat überwies den Revisionsentwurf mit Antrag vom 28. August 2024 an den Kantonsrat.

Aktuelle Entwicklung

Als Reaktion auf den Bundesgerichtsentscheid 1C_63/2023 vom 17. Oktober 2024, der die Rahmenbedingungen bei schweren polizeilichen Eingriffen in die informationelle Selbstbestimmung weiter präzisierte, wurde der Revisionsentwurf durch die Sicherheitsdirektion ein weiteres Mal weitgehend überarbeitet. Die vorgesehene Bestimmung zur automatisierten Fahrzeugfahndung wurde vollständig gestrichen. Bei der Informationsbeschaffung im virtuellen Raum wurden die Voraussetzungen zur Beschaffung von nicht öffentlich zugänglichen Informationen präzisiert. Die Verwendung von Analysesystemen wurde in einer separaten Bestimmung geregelt. Die Bestimmung zur überkantonalen polizeilichen Zusammenarbeit wurde insbesondere bezüglich der vorgesehenen Abrufverfahren und gemeinsamer Informationssysteme detailliert und eingeschränkt. Der Regierungsrat hat den neuen Revisionsentwurf am 5. März 2025 erneut an den Kantonsrat überwiesen.

Die wesentlichen Kritikpunkte der Datenschutzbeauftragten betrafen nach wie vor die Unbestimmtheit zentraler Bestimmungen des Entwurfes sowie vereinzelt die Unverhältnismässigkeit gewisser vorgesehener Personendatenbearbeitungen.

Wegweisender Bundesgerichtsentscheid für neues Polizeigesetz

Mit Urteil vom 17. Oktober 2024 entschied das Bundesgericht über die Zulässigkeit verschiedener Änderungen des Gesetzes über die Luzerner Polizei und präzisierte dabei seine Rechtsprechung in verschiedenen Bereichen polizeilicher Eingriffe in das Grundrecht auf informationelle Selbstbestimmung. Die vom Bundesgericht überprüften Bestimmungen des Luzerner Polizeigesetzes betrafen die automatische Fahrzeugfahndung und Verkehrsüberwachung (AFV), den Betrieb von Analysesystemen im Bereich der seriellen Kriminalität, den gemeinsamen Betrieb von Einsatzleitzentralen, den polizeilichen Informationssystem-Verbund des Bundes und der Kantone und Systeme zur Darstellung von Lagebildern.

Zur automatischen Fahrzeugfahndung und Verkehrsüberwachung (AFV), die nach dem Willen des Gesetzgebers im Kanton Luzern vor allem zur Strafverfolgung eingesetzt werden sollte, hielt das Bundesgericht fest, dass dem Kanton im Bereich des Strafprozessrechts (mit Ausnahmen) keine Rechtsetzungskompetenz zukomme. Die AFV zu Strafverfolgungszwecken bedürfe einer Grundlage in der Eidgenössischen Strafprozessordnung. Weil sich die vorgesehene AFV und die mit ihr vorgesehene, weitreichende Datenerfassung, -auswertung und -aufbewahrung für den verbleibenden Anwendungsbereich der Fahndung nach Personen oder Sachen als nicht verhältnismässig erwies, wurde die Bestimmung vollständig aufgehoben.

Zum Betrieb von Analysesystemen hielt das Bundesgericht fest, dass die vorgesehene Bestimmung aufgrund mangelnder Bestimmtheit nicht als gesetzliche Grundlage für schwerwiegende Grundrechtseingriffe genüge, wie sie beim Einsatz von «intelligenten» Analysesystemen zur automatisierten Analyse von grossen Datenbeständen vorlägen. Damit sei unter der Bestimmung lediglich der Einsatz von «einfachen» Analysesystemen möglich, bei denen die Analyse nicht aufgrund von Algorithmen, sondern durch menschliche Analystinnen und Analysten erfolgt und die Daten manuell eingegeben werden.

Die Bestimmung, die im Luzerner Polizeigesetz als Grundlage des polizeilichen Informationssystem-Verbund des Bundes und der Kantone hätte dienen sollen, hob das Bundesgericht auf, weil sie in der vorgesehenen Form ein überwiegendes öffentliches Interesse vermissen lasse, gegen das Verhältnismässigkeitsprinzip verstosse und dem Bestimmtheitsgebot nicht genüge. Beiläufig bemerkte das Bundesgericht dabei auch, dass es nicht ohne Weiteres ersichtlich sei, wie ein polizeilicher Informationssystem-Verbund des Bundes und der Kantone auf der Grundlage einer Vielzahl von unter Umständen divergierenden kantonalrechtlichen Regelungen zielführend und praktikabel umgesetzt werden kann.

Das Urteil ist für die Teilrevision des Polizeigesetzes im Kanton Zürich insofern von Interesse, als es mehrere Regelungsbereiche betrifft, die auch im Kanton Zürich Teil des Revisionsvorhabens sind.

Die Sicherheitsdirektion hat nach Ergehen dieses Entscheids des Bundesgerichts den Revisionsentwurf des Polizeigesetzes des Kantons Zürich überarbeitet. Am 5. März 2025 wurde dem Kantonsrat ein neuer Revisionsentwurf beantragt.

Revision des Straf- und Justizvollzugsgesetzes

2024 hat die Direktion der Justiz und des Innern eine Teilrevision des Straf- und Justizvollzugsgesetzes in die Vernehmlassung geschickt. Datenschutzrechtlich rele-

vante Bestimmungen umfassen die audiovisuelle Überwachung und die Überwachung von Kontakten beim Einsatz von IKT-Geräten im Strafvollzug, eine allgemeine Bestimmung zur Datenbearbeitung und Datenbekanntgabe durch die Straf- und Justizvollzugsbehörden sowie eine umfassende Regelung zum Electronic Monitoring.

Die Datenschutzbeauftragte begrüsst den Erlass von formell-gesetzlichen Rechtsgrundlagen für die audiovisuelle Überwachung mit technischen Geräten in Vollzugseinrichtungen und die Überwachung von Kontakten beim Einsatz von IKT-Geräten. Zwar sind die vorgesehenen Bestimmungen generell gehalten, erscheinen aber unter der Berücksichtigung des Sonderstatusverhältnisses, in dem sich die in Vollzugseinrichtungen eingewiesenen Personen befinden, als verfassungskonform. Die Datenschutzbeauftragte hat darauf hingewiesen, dass diese generellen Gesetzesbestimmungen der Detaillierung in einer Verordnung oder einem Reglement bedürfen.

Sowohl bei der vorgeschlagenen Generalklausel zu Datenbearbeitungen als auch der Bestimmung zum Datenaustausch sieht die Datenschutzbeauftragte Verbesserungsbedarf. Diese Bestimmungen erscheinen aufgrund der bundesgerichtlichen Rechtsprechung wegen ihrer Unbestimmtheit als ungeeignet, eigenständige formell-gesetzliche Rechtsgrundlagen zu bilden.

Bezüglich der Regelung des Electronic Monitoring hat die Datenschutzbeauftragte in der Vernehmlassung daran erinnert, dass die bundesrechtlichen Rechtsgrundlagen zum Electronic Monitoring bestimmen, zu welchen Zwecken Personendaten bearbeitet werden dürfen. Da die mit dem Revisionsvorhaben vorgesehene Regelung eine weitgehende Erweiterung dieser Zwecke vorsieht, hat sie zur Überprüfung geraten, ob und wo die bundesrechtlichen Regelungen abschliessender Natur sind und weitergehendes kantonales Recht zulässig ist.

Die Datenschutzbeauftragte begrüsst den Erlass von formell-gesetzlichen Rechtsgrundlagen für die audiovisuelle Überwachung mit technischen Geräten in Vollzugseinrichtungen und die Überwachung von Kontakten beim Einsatz von IKT-Geräten.

Interkantonale Vereinbarung zum elektronischen Datenaustausch im Justizvollzug

Im November 2024 hat die Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren die Vernehmlassung zur interkantonalen Vereinbarung zum elektronischen Datenaustausch im Justizvollzug eröffnet. Mit dieser Vereinbarung sollen die Rechtsgrundlagen für den elektronischen Datenaustausch zwischen den Justizvollzugsbehörden der verschiedenen Kantone geschaffen werden.

Es ist vorgesehen, ein elektronisches Aktenablagesystem zu schaffen, das den interkantonalen Austausch von elektronischen Justizvollzugsakten ermöglicht. Zudem soll eine zentrale Datenbank entstehen, in der aktuelle Personendaten im Justizvollzug sowie Informationen zu freien Plätzen in den über die gesamte Schweiz verteilten Vollzugseinrichtungen gesammelt werden.

Die Datenschutzbeauftragte hat in Zusammenarbeit mit privatim, der Konferenz der schweizerischen Datenschutzbeauftragten, an der Vernehmlassung teilgenommen. Neben Hinweisen zu den Verträgen hat sie auf vereinzelten Korrekturbedarf vor dem Hintergrund des Verhältnismässigkeitsgrundsatzes und der von der Rechtsprechung herausgearbeiteten Anforderungen an die Regelungsdichte hingewiesen.

Entwurf Gesetz über elektronische Basisdienste: Nachbesserungsbedarf bei den neuen Regelungen

Im Tätigkeitsbericht 2023 hat die Datenschutzbeauftragte über das Rechtsetzungsprojekt DigiBasis berichtet. Es regelt die elektronische Identifikation, den elektronischen Webzugang des Kantons (Zürikonto) sowie den Digitalen Arbeitsplatz (DAP) der Mitarbeitenden von öffentlichen Organen im Kanton Zürich. Der Vorentwurf enthielt klare Regelungen, welche die Datenschutzbeauftragte begrüsste. Der inzwischen an den Kantonsrat überwiesene Entwurf des Gesetzes über elektronische Basisdienste (GEB) enthält noch ungenügende datenschutzrechtliche Regelungen.

Der Gesetzesvorentwurf von DigiBasis legte Rahmenbedingungen fest, die für eine grundrechts- und datenschutzkonforme Datenbearbeitung zu beachten sind, wenn Anwendungen des Digitalen Arbeitsplatzes (DAP) an Anbietende von cloudbasierten Dienstleistungen ausgelagert werden. So sah § 17 als eine der Voraussetzungen vor, besondere Personendaten oder der Geheimhaltung unterliegende Informationen nur in der Cloud zu bearbeiten, wenn mittels umfassender Verschlüsselung gewährleistet ist, dass der Cloud-Anbieter keinen Zugriff auf die Daten nehmen kann. Zudem legte die Bestimmung fest, dass solche Anwendungen nur in der Schweiz oder der Europäischen Union (EU) betrieben werden dürfen. Diese Vorgaben wurden gestützt auf ein von der Staatskanzlei in Auftrag gegebenes Gutachten (Markus Schefer/Philip Glass, Gutachten zum grundrechtskonformen Einsatz von M365 durch die Gemeinden im Kanton Zürich, 2023) formuliert. Das Gutachten hält fest, dass für eine Auslagerung mit einem so hohen Kontrollverlust, was auf US-amerikanische Unternehmen als Dienstleister zutrifft, ein ausreichender rechtlicher Rahmen für die Auslagerung zu schaffen ist. Mit § 17 des Vorentwurfs des GEB sollte die notwendige Rechtssicherheit für die öffentlichen Organe geschaffen und für die entsprechende Transparenz gegenüber den betroffenen Personen gesorgt werden. Mit der Regelung wäre sichergestellt, dass das öffentliche Organ die geeigneten und erforderlichen Massnahmen der Datensicherheit umsetzt. Die Datenschutzbeauftragte begrüsste die Regelung.

Nach der Durchführung der Vernehmlassung zum Vorentwurf ist der Regierungsrat aufgrund der Vernehmlassungsergebnisse von der ursprünglichen Formulierung abgewichen und hat die Regelung durch eine unbestimmte Formulierung ersetzt. Diese sieht vor, dass die Wahrscheinlichkeit eines Zugriffs ausländischer Staaten anhand der getroffenen Massnahmen abzuschätzen ist. Bei der Beurteilung der Rechtmässigkeit einer Bearbeitung im Auftrag sieht das Gesetz über die Information und den Datenschutz (IDG) keine Wahrscheinlichkeitsabwägung vor. Insbesondere bei besonderen Personendaten, bei denen die besondere Gefahr von Persönlichkeitsverletzungen besteht, sowie bei Informationen, die einer besonderen Geheimnispflicht unterstehen, muss jeder faktisch mögliche, unberechtigte Zugriff ausgeschlossen werden können. Nur eine umfassende Verschlüsselung kann solche Zugriffe verunmöglichen.

Der Vorentwurf des Gesetzes über elektronische Basisdienste (GEB) enthielt klare Regelungen, welche die Datenschutzbeauftragte begrüsste. Die Vorlage an den Kantonsrat nimmt diese nur teilweise auf.

Es ist zu bedauern, dass die klare und verfassungsmässige Regelung ersetzt wurde. Die aktuelle Fassung des Gesetzesentwurfs des Regierungsrats geht damit hinter

die bis anhin geltenden Vorgaben des in den neunziger Jahren verabschiedeten Gesetzes über die Auslagerung von Informatikdienstleistungen zurück, das die damalige Risikolage berücksichtigte. Die vorgeschlagenen Bestimmungen genügen den erhöhten Anforderungen an die Ausgestaltung von Rechtsgrundlagen für die Bearbeitung besonderer Personendaten nicht, wie auch das erwähnte Gutachten festhält. Unabhängig der Regelung des GEB gelten die Vorgaben des IDG. Beim Digitalen Arbeitsplatz sind insbesondere die Vorgaben an die Datenbearbeitung durch Dritte (Auslagerung) einzuhalten.

Anpassungen im Kindes- und Erwachsenenschutzrecht

Die Datenschutzbeauftragte hat im Rahmen der Vernehmlassung zu Anpassungen im Kindes- und Erwachsenenschutzrecht Stellung genommen.

Mit der geplanten Revision des Kindes- und Erwachsenenschutzrechts sollen neu Berufsbeiständinnen und Berufsbeistände nach Beendigung der Massnahme die Akten der verbeiständeten Personen, analog der für die Akten der Kindes- und Erwachsenenschutzbehörde (KESB) geltenden Frist, während 50 Jahren aufbewahren. Diese Aufbewahrungsfrist soll neu auch für nach Abschluss des Mandates der zuständigen KESB übergegebene Akten von privaten Mandatsträgerinnen und Mandatsträgern gelten.

Für Unterlagen von untergeordneter Bedeutung, insbesondere Buchungs- und Rechnungsbelege, Bankauszüge, Versicherungsunterlagen, Steuerunterlagen und Abrechnungen der Sozialversicherungen, wird eine verkürzte Aufbewahrungsfrist von 15 Jahren vorgesehen.

Die Datenschutzbeauftragte begrüsste die geplante, analog für die Akten der KESB geltende, Aufbewahrungsfrist von 50 Jahren für Akten der Berufsbeiständinnen und Berufsbeistände. Auch die verkürzte Frist für Unterlagen von untergeordneter Bedeutung hält sie für sachlich gerechtfertigt.

Die Datenschutzbeauftragte begrüsste die geplante, analog für die Akten der KESB geltende, Aufbewahrungsfrist von 50 Jahren für Akten der Berufsbeiständinnen und Berufsbeistände.

Mit der geplanten Revision soll zudem gesetzlich festgelegt werden, dass sich die Akteneinsicht nach abgeschlossenem Verfahren der KESB nach dem Gesetz über die Information und den Datenschutz (IDG) richtet und nicht nach der Informations- und Akteneinsichtsverordnung der obersten kantonalen Gerichte. Damit sollen Entscheide der KESB, mit denen sie den Zugang zur Information verweigert, einschränkt oder aufschiebt, auf dem verwaltungsrechtlichen Rechtsmittelweg angefochten werden können. Dieser führt über den Bezirksrat an das kantonale Verwaltungsgericht. Die Datenschutzbeauftragte wies darauf hin, dass dies bereits im IDG geregelt und die Anpassung somit nicht notwendig sei.

Schliesslich soll mit der geplanten Revision neu für Informationszugangsgesuche in Akten der verbeiständeten Personen des Erwachsenenschutzes nach abgeschlossenen Verfahren, analog des Kindesschutzes, auch die KESB zuständig sein. Die Berufsbeistandschaften sollen an sie gerichtete Gesuche zusammen mit den entsprechenden Akten der zuständigen KESB übermitteln. Die Datenschutzbeauftragte begrüsste diese Anpassung.

Anwendbarkeit privatrechtlicher Datenschutzbestimmungen für öffentliche Organe

Für öffentliche Organe im wirtschaftlichen Wettbewerb wird das Bundesgesetz über den Datenschutz (DSG) sinngemäss angewendet. Die Datenschutzbeauftragte des Kantons Zürich übt jedoch die Aufsicht aus. Daraus ergeben sich für die betroffenen öffentlichen Organe die folgenden Pflichten gegenüber der Datenschutzbeauftragten: Öffentliche Organe im wirtschaftlichen Wettbewerb müssen der Datenschutzbeauftragten beispielsweise die Person der oder des Datenschutzberatenden nennen. Weiter sind der Datenschutzbeauftragten vorgängig die Datenschutzklauseln mitzuteilen, wenn das entsprechende öffentliche Organ Personendaten an Empfängerinnen oder Empfänger in Staaten ohne angemessenes Datenschutzniveau bekannt gibt und sich dabei auf die Ausnahmeregelung gemäss Art. 16 Abs. 2 DSG stützt. Ausserdem ist eine geplante Bearbeitung der Datenschutzbeauftragten zur Vorabkonsultation vorzulegen, wenn die Datenschutz-Folgenabschätzung (DSFA) ergibt, dass die Bearbeitung trotz den vorgesehenen Massnahmen ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person zur Folge hat. Schliesslich besteht eine Meldepflicht an die Datenschutzbeauftragte bei Verletzungen der Datensicherheit, sofern sie voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führen.

Die Datenschutzbeauftragte des Kantons Zürich übt die Aufsicht für Organe im wirtschaftlichen Wettbewerb aus.