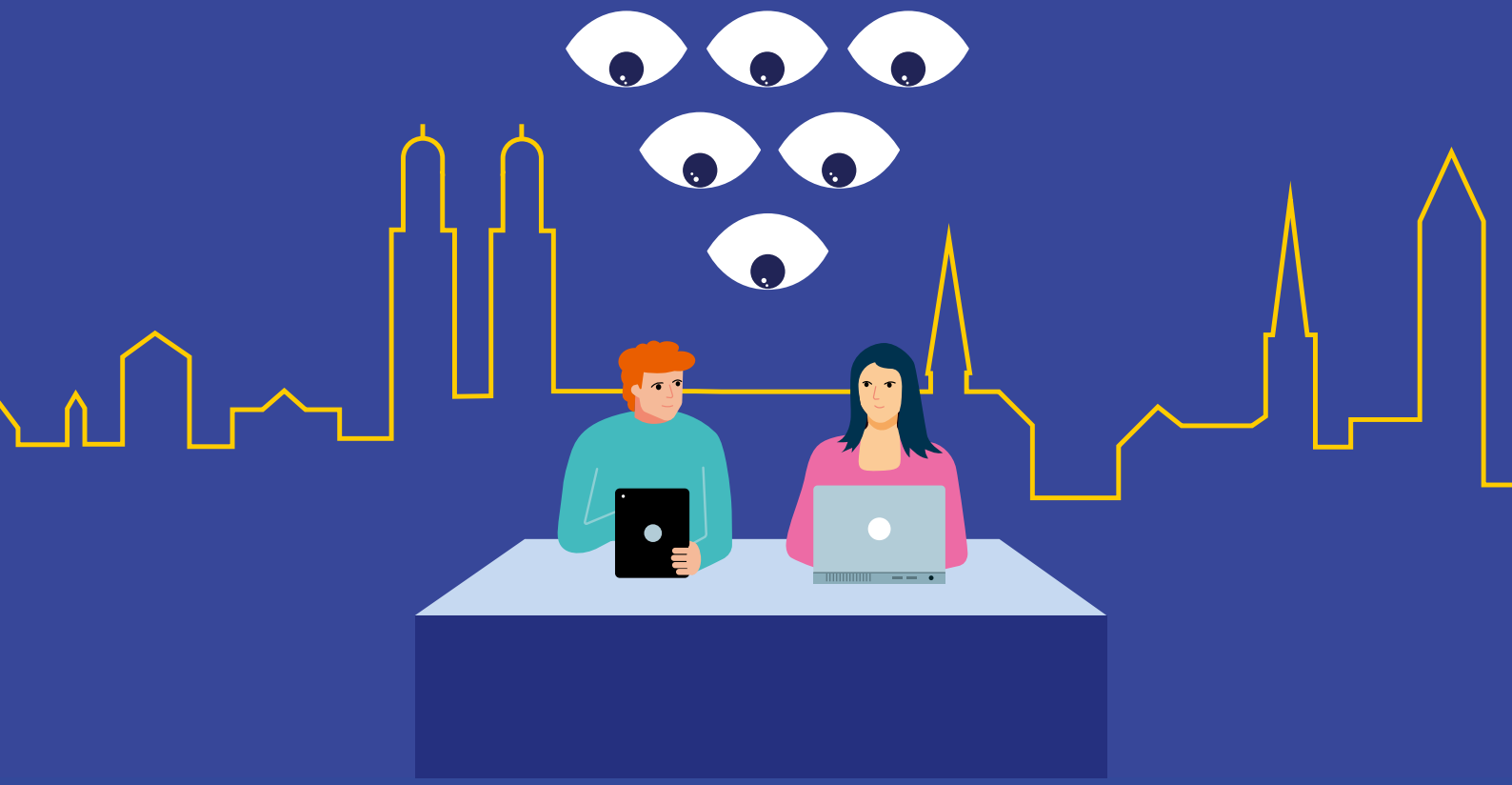
Stadt Zürich
Datenschutzstelle

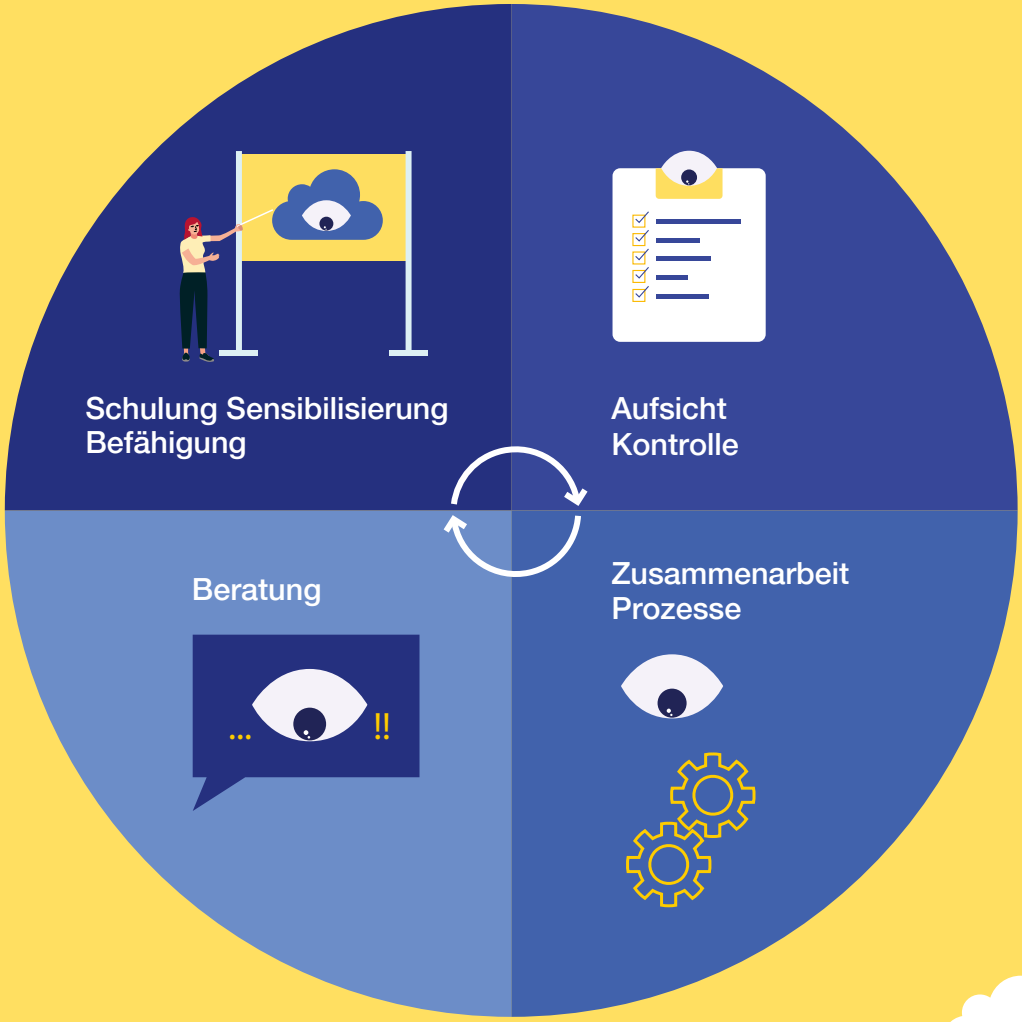
Tätigkeitsbericht der Datenschutz-stelle 2025



Impresssum

Inhalt: Datenschutzstelle der Stadt Zürich
Gestaltung, Illustrationen: Züriblau

Inhalt


Schulung Sensibilisierung
Befähigung
Aufsicht
Kontrolle
Beratung
...
!!
Zusammenarbeit
Prozesse

1 Vorwort

Die Datenschutzbeauftragte erstattet dem Gemeinderat der Stadt Zürich jährlich Bericht über die Tätigkeit der Datenschutzstelle. Die Tätigkeitsberichte geben einen Einblick in aktuelle Datenschutzthemen, in die Feststellungen der Datenschutzstelle sowie in deren Praxisalltag.

Geschätzte Leser*innen

Herzlich willkommen auf der Webseite des Tätigkeitsberichts 2025 der Datenschutzstelle der Stadt Zürich.

Der Schutz personenbezogener Daten und damit der Schutz der Privatsphäre ist in einer zunehmend digitalisierten Welt von zentraler Bedeutung. Die fortschreitende Digitalisierung von Arbeitsbereichen der öffentlichen Verwaltung, neue technologische Entwicklungen sowie sich wandelnde gesellschaftliche Erwartungen stellen den Datenschutz vor immer neue Herausforderungen. Die Tätigkeit der Datenschutzstelle gewinnt vor diesem Hintergrund kontinuierlich an Relevanz.

Der Tätigkeitsbericht 2025 gewährt einen Einblick in die vielfältige und abwechslungsreiche Arbeit der Datenschutzstelle und informiert über wichtige Feststellungen im Bereich des Datenschutzrechts. Der vorliegende Bericht deckt den Zeitraum vom 1. Januar 2025 bis und mit 31. Dezember 2025 ab. Er gliedert sich, wie bereits der letztjährige Tätigkeitsbericht nach den vier Strategieschwerpunkten der Datenschutzstelle (siehe Abbildung) und illustriert beispielhaft die konkrete Arbeit in den jeweiligen Bereichen im Jahr 2025.

Der Bericht soll Transparenz schaffen, Vertrauen fördern und zur weiteren Sensibilisierung für Datenschutzthemen beitragen. Zugleich dient er als Grundlage für den Dialog mit Behörden, der Politik und der Öffentlichkeit.

Ich danke meinem Team sowie all jenen städtischen Mitarbeiter*innen, die während des letzten Jahres zur Weiterentwicklung des Datenschutzes und der Informationssicherheit in der Stadtverwaltung beigetragen haben und wünsche Ihnen – geschätzte Leser*innen – eine spannende Lektüre.

2 Das Jahr 2025

Die Berichterstattung der Datenschutzstelle hat sich zu wichtigen Feststellungen zu äussern. Für das Berichtsjahr 2025 sind die folgenden drei Themen zu erwähnen:

1 Nutzung von M365 in der Stadtverwaltung – es braucht Anpassungen

Die Stadtverwaltung mit rund 36 000 Mitarbeitenden ist auf eine zeitgemässe und effiziente IT-Infrastruktur angewiesen. Dabei sticht insbesondere der in der Stadtverwaltung eingesetzte Dienst von Microsoft 365 (M365) ins Auge. Dieser steht aktuell stark im medialen Fokus. Der Grund dafür: Die Produkte der M365-Lösung werden nur noch in der Cloud angeboten.

Im Praxisalltag der Datenschutzstelle hat sich im Berichtsjahr anhand konkreter Vorhaben gezeigt, dass die Dienstabteilungen der Stadtverwaltung zunehmend in Betracht ziehen, sensible Personendaten aus ihren Fachbereichen und -applikationen in der M365-Cloud zu speichern. Eine solche Auslagerung ist mit dem in der Bundesverfassung verankerten Grundrecht auf Datenschutz bzw. Privatsphäre nur schwer vereinbar. Die Datenschutzbeauftragten der Kantone und des Bundes haben im Namen ihres Fachvereines Privatim ebenfalls auf diese Problematik aufmerksam gemacht.

Gestützt auf den **STRB Nr. 670/2022** hatte die Dienstabteilung Organisation und Informatik (OIZ) im Jahr 2022 die M365-Cloud mit dem Status Basisschutz+ freigegeben. Man war davon ausgegangen, dass in der M365-Cloud grundsätzlich auch besondere (und damit sensible) Personendaten gespeichert und bearbeitet werden dürfen. Diese Annahme ist aus heutiger Sicht aufgrund der technischen und politischen Entwicklung in Frage zu stellen.

Bereits Ende 2024 suchte die Datenschutzstelle den Austausch mit der OIZ, welche für die Gewährleistung der Sicherheit der M365-Cloud gemäss genanntem STRB verantwortlich ist, und setzte sie über ihre Bedenken in Bezug auf die Nutzung der M365-Cloud detailliert in Kenntnis.
Im Zuge dessen nahm die OIZ eine erneute Risikobetrachtung vor, welche sie im Ergebnis dazu bewog, im Frühjahr 2025 ein **Moratorium** auszusprechen. Das Moratorium betrifft **besondere Personendaten**, welche während der Dauer des Moratoriums nicht in einzelne Anwendungen der M365-Cloud ausgelagert werden dürfen.

Um das Schutzniveau der Daten in der M365-Cloud-Umgebung zu erhöhen, soll eine neue Verschlüsselungslösung eingesetzt werden, welche die Daten besser schützt. Vereinfacht gesagt soll mit der Umsetzung dieses Vorhabens der Schlüssel zu den Daten in der M365-Cloud neu durch die OIZ und nicht mehr durch Microsoft selbst verwaltet werden. Damit soll erreicht werden, dass Microsoft keinen Zugang zu den Daten in unverschlüsselter Form hat und damit die Personendaten für Microsoft nicht lesbar sind. Zur Absicherung der Tauglichkeit dieser Lösung hat die Datenschutzstelle im Herbst 2025 ein externes Audit gefordert.

Für die öffentliche Verwaltung ist eine Exitstrategie kein optionales Zusatzthema, sondern ein zentraler Bestandteil einer verantwortungsvollen und verbindlichen Cloud-Governance.

Am Ende des Berichtsjahrs wurde dieses Audit fertiggestellt. Es bestätigte im Ergebnis, dass die geplante Verschlüsselungslösung grundsätzlich geeignet ist, die Datensicherheit in Bezug auf die datenschutzrelevanten Schutzziele, insbesondere Vertraulichkeit und Integrität, zu gewährleisten. Jedoch verbleiben auch mit dem Einsatz der Verschlüsselungslösung (Rest-)Risiken.

Die Datenschutzstelle hat diesbezüglich den Gesamtstadtrat einbezogen und ist bei ihm vorstellig geworden. Sie vertritt die Haltung, dass – aufgrund der Tragweite der Entscheidung sowie der momentan herrschenden politischen Diskussion über die Nutzung der M365-Cloud-Umgebung – diese Restrisikoübernahme durch den Stadtrat zu erfolgen hat. Die Tragweite, Konsequenz und insbesondere der konkrete Einsatz der Verschlüsselungslösung bzw. der M365-Cloud muss vom Stadtrat in einer verbindlichen Cloud-Governance definiert werden.
Aufgrund der hohen Abhängigkeit zum Anbieter Microsoft hat die Datenschutzstelle den Stadtrat zudem aufgefordert, eine verbindliche, valide und operationalisierbare Exitstrategie zu verabschieden. Für die öffentliche Verwaltung ist eine Exitstrategie kein optionales Zusatzthema, sondern ein zentraler Bestandteil einer verantwortungsvollen und verbindlichen **Cloud-Governance**.

2 KI und Datenschutz – Vereinbarkeit und Massnahmen im Berichtsjahr

Der Einsatz von künstlicher Intelligenz (KI) in der Verwaltung der Stadt Zürich bietet Potenzial: Sie kann administrative Prozesse beschleunigen, Fehler reduzieren und Ressourcen effizienter einsetzen – etwa bei der Automatisierung von Anträgen, der Auswertung von Bürger*innen-Feedbacks oder der Vorhersage des Bedarfs im Sozial- oder Umweltbereich.

Gleichzeitig bringen KI-Systeme auch komplexe Fragen mit sich und stellen die öffentliche Verwaltung vor zentrale datenschutzrechtliche Herausforderungen. Zunächst geht es um die Wahrung von **Rechtsstaatlichkeit und Transparenz**. Staatliches Handeln muss nachvollziehbar und überprüfbar bleiben – auch dann, wenn KI-Systeme eingesetzt werden. Bürger*innen müssen verstehen können, auf welcher Grundlage Entscheidungen getroffen werden. Eine abschliessende Beurteilung durch städtische Mitarbeiter*innen, also natürliche Personen, bleibt dabei zentral.

Im Kontext der KI-Nutzung kommt die Frage nach dem Schutz sensibler Verwaltungsdaten hinzu. Behörden bearbeiten häufig besondere Personendaten in den Bereichen Gesundheit, Polizei und Soziales oder weitere Personendaten unter speziellen Geheimhaltungsbestimmungen wie im Steuerbereich. Beim Einsatz von KI-Systemen muss daher sichergestellt werden, dass diese Daten angemessen geschützt und nicht zweckwidrig verwendet werden.

Um den Herausforderungen der KI-Nutzung zu begegnen und datenschutzkonform mit dieser Technologie umzugehen, braucht die Stadt Zürich klare und verbindliche Vorgaben, wie KI-Systeme in der Verwaltung eingesetzt werden dürfen. Solche Richtlinien schaffen Orientierung für die Mitarbeitenden und stellen sicher, dass der Einsatz von KI rechtlich korrekt, verantwortungsvoll und transparent erfolgt.

Wichtig sind verbindliche Regeln, Prozesse und Verantwortlichkeiten

Zudem muss jedes KI-Vorhaben die für die Verwaltung im Bereich Datenschutz und Informationssicherheit festgelegten Prozesse durchlaufen. Dazu gehört insbesondere die Durchführung einer Datenschutz-Folgenabschätzung. In beson-

ders sensiblen Fällen ist zusätzlich eine Vorabkontrolle durch die Datenschutzstelle erforderlich. So wird sichergestellt, dass mögliche Gefahren für die Rechte und Freiheiten betroffener Personen frühzeitig erkannt und minimiert werden.

KI und die Stadtverwaltung im Berichtsjahr

In Zusammenarbeit zwischen der Datenschutzstelle, der OIZ und dem Rechtskonsulenten wurde im Berichtsjahr eine städtische KI-Richtlinie erarbeitet. Die KI-Richtlinie regelt den Umgang mit Werkzeugen der generativen künstlichen Intelligenz (sog. KI-Werkzeuge) von verwaltungsexternen Anbietenden (z.B. ChatGPT).

Die KI-Richtlinie wurde am 20. August 2025 vom Stadtrat verabschiedet **(STRB Nr. 2025-2281)** und ist in der Stadtverwaltung für alle Nutzenden von KI-Werkzeugen verpflichtend.

Trotz der Etablierung der Richtlinie bleibt der Umgang mit KI-Werkzeugen, die durch verwaltungsexterne Anbietende zur Verfügung gestellt werden und über das Internet zugänglich sind, herausfordernd. Ein zentrales Risiko betrifft dabei den Datenschutz. In der Verwaltung werden häufig besondere Personendaten oder weitere Personendaten unter speziellen Geheimhaltungsbestimmungen verarbeitet, etwa zu Gesundheit, Sozialleistungen, Strafverfahren oder Steuern. Zudem ist eine effektive Anonymisierung von Daten oftmals viel schwieriger zu erreichen, als dies allgemein bekannt ist. Werden solche Informationen unbedacht in ein externes KI-System eingegeben, kann nicht kontrolliert werden, wo und wie diese Daten weiterverarbeitet oder gespeichert werden. Dadurch besteht die Gefahr von Datenschutzverletzungen oder einer unzulässigen Datenübermittlung.

Die OIZ hat mitunter aus diesem Grund im Berichtsjahr eine stadteigene KI-Assistenz geschaffen, die **ZüriA**. Sie ist ein KI-Chatbot basierend auf Open Source-Sprachmodellen. Die KI-Infrastruktur ist in die Rechenzentren der Stadt Zürich integriert. Am Ende des Berichtsjahrs hat die Datenschutzstelle die Basisversion von **ZüriA** mittels Vorabkontrolle geprüft. Sie konnte in ihrem Prüfbericht festhalten, dass die Lösung hohen Datenschutzanforderungen genügt.

Die KI-Richtlinie regelt den Umgang mit Werkzeugen der generativen künstlichen Intelligenz (sog. KI-Werkzeuge) von verwaltungsexternen Anbietenden (z.B. ChatGPT).

Ansonsten wurden bei der Datenschutzstelle im Berichtsjahr nur wenige KI-Projekte aktiv zur Vorabkontrolle angemeldet. Die Datenschutzstelle wurde mehrmals aufgrund von Medienberichten und/oder städtischen Intranet-Meldungen auf kritische KI-Vorhaben aufmerksam und musste die Anmeldung solcher Vorhaben nachträglich einfordern.

Dies zeigt, dass Dienstabteilungen und Projektleitende die potenziellen Risiken beim Einsatz mit KI regelmässig unterschätzen. Zudem fehlt zum Teil das Bewusstsein, dass der städtische Informationssicherheits- und Datenschutzprozess (ISDS-Prozess) auch bei KI-Vorhaben verbindlich eingehalten werden muss. Die Datenschutzstelle wird in den kommenden Jahren diesbezüglich ihr Beratungsangebot und ihre Kontrolltätigkeit ausbauen müssen. Mitarbeitende müssen die datenschutzrechtlichen Anforderungen verstehen und wissen, wie sie KI-Werkzeuge korrekt und sicher einsetzen. Zudem werden auch vermehrt Stichproben im Bereich von KI-Vorhaben durchgeführt werden müssen.

Keine Hochrisiko-Systeme in der Verwaltung

Grundsätzlich muss festgehalten werden, dass die Stadtverwaltung auf sogenannte Hochrisiko-KI-Systeme (zu nennen ist hier das Beispiel der Gesichtserkennung im öffentlichen Raum) verzichten sollte, wenn die damit verbundenen rechtlichen oder ethischen Risiken nicht ausreichend beherrschbar sind. Der Schutz der Bevölkerung und die Wahrung rechtsstaatlicher Grundsätze haben Vorrang vor allfälligen Effizienzgewinnen.

3 Datenschutz an Schulen: Ein zentrales Anliegen der Datenschutzstelle

Im Berichtsjahr hat die Datenschutzstelle gezielt daran gearbeitet, das Bewusstsein für Datenschutz im Schulbereich zu stärken, Prozesse zu stabilisieren und rechtliche Rahmenbedingungen praxisnah umzusetzen.

Zu den Massnahmen gehörten unter anderem:

- Ein Schulungsreferat an einer Tagung aller Schulleiter*innen der Stadt Zürich mit dem Thema «Datenschutz an Schulen – Bewusstsein schaffen / Sicherheit stärken», das auf positive Resonanz stiess;
- Die Schulung von Schulinformatiker*innen zu datenschutzkonformen Prozessen;
- Die enge Zusammenarbeit mit dem Rechtsdienst des Schul- und Sportdepartements zur Entwicklung einer einheitlichen Haltung zur Datenweitergabe – insbesondere im Kontext von Schulabsentismus;
- Die Begleitung der Weiterentwicklung der Plattform «Meine Kinder» durch eine Vorabkontrolle;
- Die Planung einer thematischen Kampagne für die kommenden Jahre, um Datenschutz im Schulalltag sichtbarer und nachhaltiger zu verankern.

Datenschutz an öffentlichen Schulen ist besonders komplex: Hier werden täglich grosse Mengen sensibler personenbezogener Daten verarbeitet – nicht nur Stammdaten, sondern auch Leistungs-, Verhaltens-, Förder- und Gesundheitsdaten sowie Fotos. Nach dem Gesetz über die Information und den Datenschutz (IDG) unterliegen diese einem erhöhten Schutzbedarf.
Gleichzeitig wird der Schulalltag zunehmend digital: Lernplattformen, Videokonferenzen und Messenger-Apps sind alltäglich und müssen datenschutzrechtlich geprüft und konform eingesetzt werden.

Datenschutz an öffentlichen Schulen ist besonders komplex

Diese Herausforderungen werden verschärft durch eine dezentralisierte Organisation sowie begrenzte Ressourcen. Schulen verfügen selten über spezialisierte Datenschutzexpertise. Lehrkräfte sind pädagogisch, Verwaltungspersonal kaufmännisch ausgebildet – aber kaum datenschutzrechtlich geschult. Datenschutz bleibt daher oft «Nebensache» und wird nicht systematisch integriert. Das er-

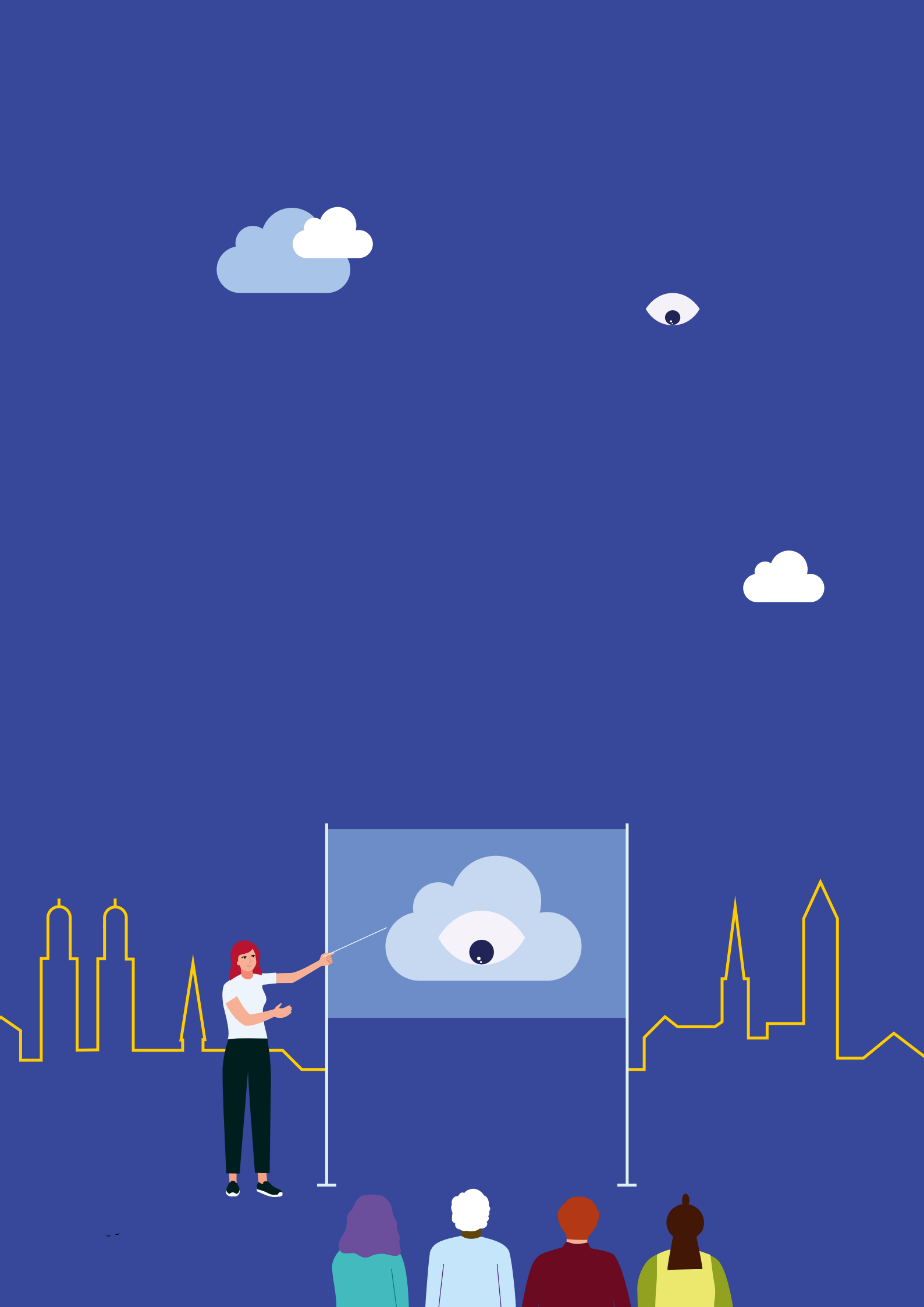
höht einerseits das Risiko unbeabsichtigter Verstösse, andererseits kann es auch dazu führen, dass das Datenschutzrecht in der Praxis teilweise zu streng ausgelegt wird.
Auch die rechtliche Einordnung ist anspruchsvoll: Welche Rechtsgrundlage gilt? Wann ist eine Einwilligung nötig? Wie wird die Urteilsfähigkeit von Kindern beurteilt? Und was bedeutet das für die Rolle der Eltern? Diese Fragen sind komplex und oft nicht eindeutig beantwortbar.

Warum ist gezielter Datenschutz an Schulen so wichtig?

Schüler*innen gehören zu einer besonders schutzbedürftigen Gruppe: Sie können die langfristigen Folgen von Datenbearbeitungen oft noch nicht abschätzen. Ein verantwortungsvoller Umgang mit ihren Informationen schützt sie vor Stigmatisierung, Diskriminierung oder ungewollter Offenlegung von sensiblen Lebens- und Bildungsdaten – und trägt direkt zu ihrem Wohl bei.

Zudem baut transparenter Datenschutz Vertrauen auf: Wenn klar kommuniziert wird, welche Daten zu welchem Zweck erhoben, genutzt und bei einem Schulwechsel weitergegeben werden, fühlen sich Eltern ernstgenommen und Schüler*innen respektiert. Dies fördert die Zusammenarbeit zwischen Schule, Familie und Lernenden und reduziert Konflikte und Beschwerden.

Schliesslich schützt ein konsequenter Datenschutz auch die Schulen selbst. Klare Regeln, verständliche Verfahren und geschultes Personal verhindern Datenschutzpannen und damit verbundene rechtliche Risiken – für Schulleitungen, Lehrkräfte und Verwaltung gleichermassen.



3 Schulung – Sensibilisierung – Befähigung

Einleitung

Das Datenschutzrecht beschlägt mehr oder weniger alle Bereiche der Stadtverwaltung und bringt aufgrund des gesellschaftlichen und technologischen Wandels immer wieder neue Fragestellungen mit sich. Damit es seine Wirkung entfalten kann, muss es in der Stadtverwaltung bekannt sein. Die Wissensvermittlung und Kompetenzförderung im Bereich Datenschutz ist deshalb eine Kernaufgabe der Datenschutzstelle.

Schulungen und Weiterbildungen sind ein essenzieller Faktor, damit Datenschutz in der städtischen Verwaltung umgesetzt wird. Sie vermitteln das nötige Fachwissen und fördern zudem eine Kultur der Verantwortung. Dienstabteilungen und Departemente, die in Datenschutz-Schulungen investieren, reduzieren Risiken und nehmen ihre rechtliche Verantwortung wahr.

Die Datenschutzstelle bietet Schulungen an, die sich spezifisch auf die Bedürfnisse städtischer Verwaltungsstellen ausrichten. Im Jahr 2025 führte sie eine Vielzahl solcher Schulungen durch.

Nebst den Schulungen erarbeitet die Datenschutzstelle Merkblätter und Hilfsmittel. Diese sollen mit der Vermittlung von Wissen oder konkreten Hilfestellungen ebenfalls zur Umsetzung des Datenschutzrechts beitragen und die Adressat*innen befähigen, das Datenschutzrecht umzusetzen und damit die Grundrechte der Betroffenen zu schützen. Neu finden sich alle publizierten Merkblätter, Leitfäden und Hilfestellungen der Datenschutzstelle auf dem 2025 geschaffenen Datenschutz-Portal im städtischen Intranet.

E-Government und Datenschutz

Im September 2025 referierte die Datenschutzstelle zum Thema «Datenschutz schafft Vertrauen» am städtischen E-Government Forum.

Die Datenschutzschulung im Bereich E-Government ist wichtig, weil öffentliche Verwaltungen mit vertraulichen und sensiblen Daten von Bürger*innen korrekt und gesetzeskonform umzugehen haben – etwa mit Steuer-, Gesundheits-, Sozial- oder Polizeidaten. Diese Daten sind hochgradig schützenswert und ihr Missbrauch oder ihre unautorisierte Weitergabe könnte nicht nur rechtliche Konsequenzen haben, sondern auch das Vertrauen der Bevölkerung in digitale öffentliche Dienste schwer beschädigen.

Anlässlich des E-Government Forums wurden die circa 100 Teilnehmenden zu folgenden Aspekten geschult und es wurde ihnen anhand von Theorie und praktischen Beispielen vor Augen geführt, dass:

- Mitarbeiter*innen und Entscheidungsträger*innen die geltenden Gesetze (IDG, IDV) und ihre Anwendung im digitalen Verwaltungsumfeld verstehen müssen,
- Prozesse im E-Government datenschutzkonform gestaltet und umgesetzt werden müssen,
- Risiken wie Datenlecks, unzulässige Datenweitergabe oder fehlerhafte Berechtigungsmanagement-Systeme früh erkannt und vermieden werden müssen,
- für das Vertrauen der Bürger*innen in das E-Government der zweckkonforme und sichere Umgang mit ihren Daten von zentraler Bedeutung ist.

Zudem förderte diese Schulung bei E-Government-Verantwortlichen eine kulturbezogene Verankerung des Datenschutzes als Grundrecht – nicht als Hindernis, sondern als integralen Bestandteil verantwortungsvoller Digitalisierung. Nur wenn alle Beteiligten im E-Government datenschutzbewusst handeln, kann die digitale Transformation der Verwaltung nachhaltig, transparent und bevölkerungsnah gelingen.

Digital Forum der Stadtverwaltung

Die Datenschutzstelle und die Fachstelle Informationssicherheit nutzten das Digital Forum für ein gemeinsames Referat, bei dem eine wesentliche Zielgruppe erreicht werden konnte.

Anlässlich des jährlich stattfindenden Digital Forums der OIZ beleuchteten die Datenschutzstelle und die Fachstelle für Informationssicherheit die wichtigsten und häufigsten Fragestellungen rund um die datenschutzkonforme Umsetzung von Projekten und erklärten, wie der ISDS-Prozess die Projektverantwortlichen dabei unterstützen kann.

Das Digital Forum im Juni 2025 mit seinen über 500 Teilnehmenden bot der Datenschutzstelle eine ideale Gelegenheit, alle städtischen Mitarbeitenden anzusprechen, die sich mit der Digitalisierung auseinandersetzen. Sie alle profitieren von einem vertieften Verständnis des städtischen ISDS-Prozesses.

Den Teilnehmenden wurde in Erinnerung gerufen, dass im Rahmen von Digitalisierungsvorhaben nicht nur die Funktion eines Services, sondern auch der angemessene Schutz von geschäftsrelevanten Informationen und Daten sichergestellt werden muss. Dies geschieht, indem Risiken erkannt und adressiert, Informationssicherheitsmassnahmen umgesetzt und die Einhaltung der Datenschutzvorschriften dokumentiert werden.

Schulung der Geschäftsleitung der Stadtpolizei Zürich

Die Datenschutz-Schulung unterstützt die Mitglieder der Geschäftsleitung der Stadtpolizei dabei, Wissen und Kompetenzen im Bereich Datenschutz aufzubauen, städtische Prozesse besser zu verstehen und ihre Verantwortung im Datenschutz bewusster wahrzunehmen.

Die Datenschutzstelle legt Wert darauf, dass nicht nur die Mitarbeitenden an der Front, die Rechtsdienste und die Projektleitenden, sondern auch Geschäftsleitungsmitglieder im Datenschutz geschult werden.

Die Schulung dieser Verwaltungsebene ist deshalb so wichtig, weil die Geschäftsleitung die strategische Verantwortung für die Einhaltung der gesetzlichen Vorgaben des IDG trägt.

Sie entscheidet über Ressourcen, Prozesse und die «Unternehmenskultur» – und damit auch darüber, ob Datenschutz konstruktiv als integraler Bestandteil der Führungsaufgabe verstanden wird oder als Problem angesehen wird.

Durch eine gezielte Schulung werden Geschäftsleitungsmitglieder erinnert an:

– ihre rechtliche Verantwortung,
– die Risiken von Datenschutzverletzungen (z. B. Reputationsschaden, Verlust von Vertrauen),
– welche Massnahmen notwendig sind, um datenschutzkonforme Prozesse zu implementieren und zu überwachen.

Ohne dieses Verständnis laufen Geschäftsleitungsmitglieder Gefahr, datenschutzrechtliche Pflichten zu vernachlässigen, was zu schwerwiegenden Konsequenzen führen kann. Eine geschulte Geschäftsleitung setzt daher den Ton für eine datenschutzbewusste «Unternehmenskultur» auf allen Ebenen.

Datenschutz im Intranet und im neuen Datenschutz-Portal

Die Datenschutzstelle überarbeitete ihren Auftritt im Intranet, um mehr Informationen für Mitarbeitende der Verwaltung anzubieten.

Nachdem im Dezember 2024 der neue Webauftritt der Stadt Zürich eingeführt worden war, folgte Ende November 2025 das neue städtische Intranet. Die Informationen im Intranet sind nun für alle Mitarbeitenden der Stadtverwaltung leicht auffindbar und können auch auf mobilen Geräten aufgerufen werden.

Das neue Intranet unterstützt die Datenschutzstelle bei der Vermittlung von Grundlagen und der Beratung bei Fragen zum Datenschutz, denn Informationen zum Datenschutz werden neuerdings gleich mehrfach präsentiert. Die Einstiegsseite enthält eine erste Einführung für alle Mitarbeitenden und führt in die Grundsätze und die wichtigsten Themen des Datenschutzes ein. Da alle Mitarbeitenden der Stadtverwaltung täglich mit Daten und Informationen arbeiten, sollen die wichtigsten Begriffe und Grundsätze des Datenschutzes an prominenter Stelle einfach und einprägsam erklärt werden.

Für alle, die mehr wissen möchten oder konkrete Fragen haben, gibt es neu zusätzlich das sogenannte Datenschutz-Portal. Dieses enthält detailliertere Informationen, Wegleitungen sowie Hilfsmittel und beantwortet Fragen rund um das Thema Datenschutz. Die darin enthaltenen, detaillierten Informationen unterstützen auch Spezialist*innen bei der Arbeit. Es wird in Zukunft laufend aktualisiert und ergänzt.

Zusammen mit der Fachstelle Informationssicherheit unterhält die Datenschutzstelle zudem das ISDS-Portal. Dieses enthält Informationen und Hilfestellungen zum ISDS-Prozess, der von sämtlichen Projekten, bei denen Daten bearbeitet werden, durchlaufen werden muss.

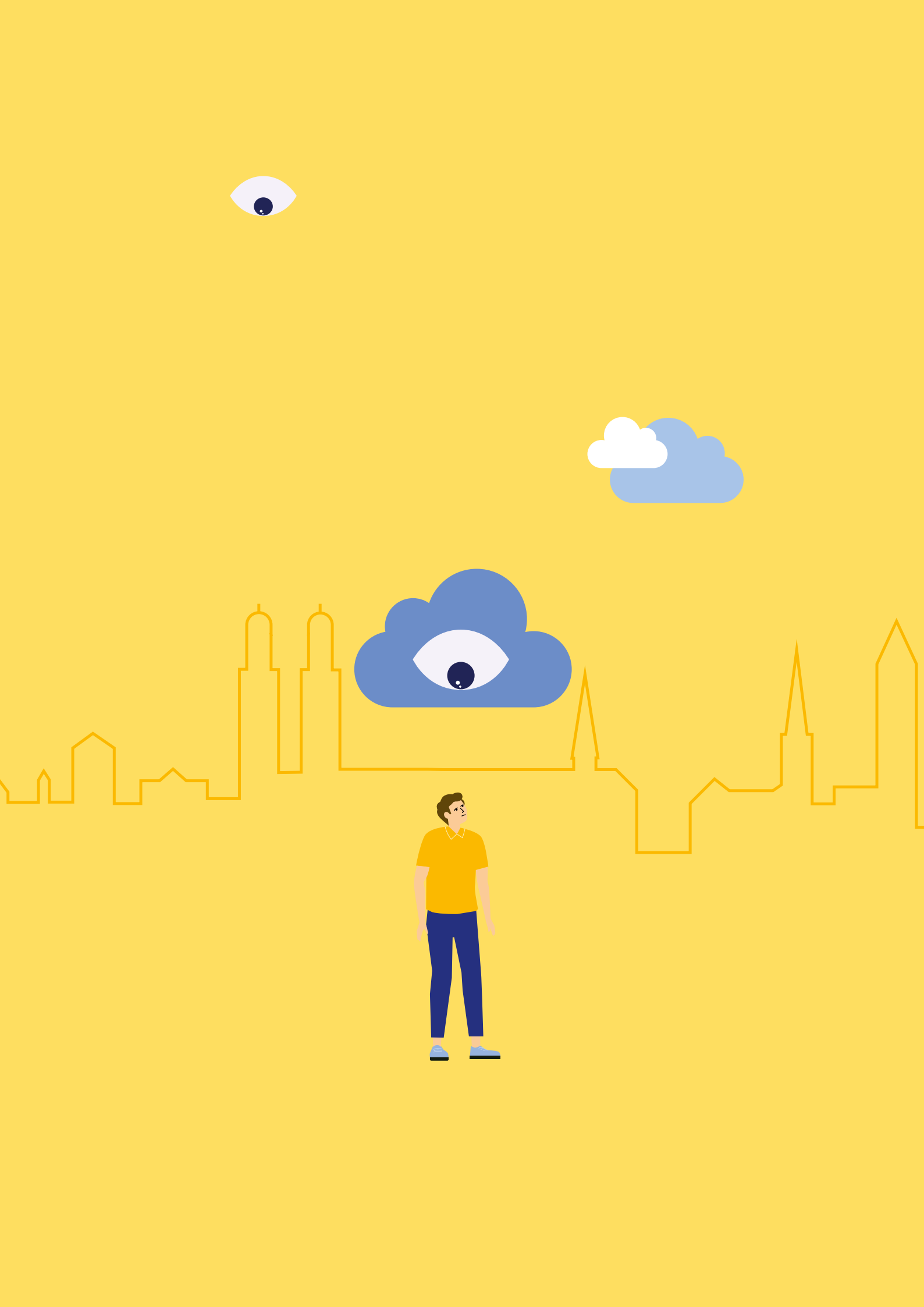
Die neuen Kommunikationsmittel erleichtern das adressatengerechte Vermitteln von Grundlagen und aktuellen Informationen zum Datenschutz und sollen vermehrt genutzt werden.

Zürcher Datenschutztagung

Die Datenschutzstelle bot gemeinsam mit der ZHAW einen Workshop zu Amtshilfe und Datenbekanntgaben an.

Die Datenschutzstelle wirkte bei der Zürcher Datenschutztagung vom 25. September 2025 der Zürcher Hochschule für Angewandte Wissenschaften und der Kantonalen Datenschutzbeauftragten mit. Die Tagung widmete sich dem Thema «Auftragsbearbeitung, Bekanntgabe & Cloud: Das ABC für Datenschutz und Informationssicherheit». Die Tagung bot lehrreiche fachliche Referate und einen inspirierenden Austausch mit Vertreter*innen aus vielen Zürcher Gemeinden sowie auch aus der Zürcher Stadtverwaltung.

Im Rahmen der Tagung gestaltete die Datenschutzstelle einen praxisnahen Workshop zum Thema Amtshilfe und Datenbekanntgaben. Diskutiert wurden unter anderem die Herausgabe von Akten aus Bau-, Schüler*innen- und Steuerdossiers. Die Rückmeldung der Teilnehmenden zum Workshop der Datenschutzstelle waren durchwegs positiv.



4 Aufsicht und Kontrolle

Einleitung

Es gehört zu den gesetzlichen Aufgaben der Datenschutzstelle, dass sie die verantwortlichen öffentlichen Organe bei der Einhaltung der Vorschriften in rechtlicher, technischer und organisatorischer Hinsicht nicht nur berät und unterstützt, sondern auch überwacht. Diese Aufgabe nimmt die Datenschutzstelle insbesondere auf die folgenden Arten wahr:

- mit der Durchführung von Vorabkontrollen bei Projekten, die eine erhöhtes datenschutzrechtliches Risiko aufweisen,
- mittels Kontrollen im Rahmen ihrer Aufsichtstätigkeit, wobei die Datenschutzstelle die Umsetzung der Vorgaben überprüft,
- durch die Prüfung von rechtssetzenden Erlassen mit Datenschutzbezug,
- durch die Entgegennahme und Prüfung meldepflichtiger Datenschutzvorfälle.

Für die Umsetzung der Vorabkontrollen, den Umgang mit meldepflichtigen Vorfällen und die Begleitung von Gesetzgebungsarbeiten bestehen etablierte Prozesse. Die Datenschutzstelle hat im Berichtsjahr 2025 neben den Vorabkontrollen diverse weitere Kontrollen durchgeführt. Ziel der Kontrollen ist neben konkreten Erkenntnissen zum Handlungsbedarf immer auch eine Sensibilisierung für effektiven Datenschutz.

Neue Parkuhren für die Stadt

Die neu beschafften Parkuhren der Stadt Zürich verlangen die Eingabe des Kontrollschildes und basieren teilweise auf einem Cloud-System. Die Datenschutzstelle hat das Vorhaben geprüft.

Was haben Parkuhren mit Datenschutz zu tun? Mit der Beschaffung und Inbetriebnahme der neuen Parkuhren der Stadt Zürich stellte sich genau diese Frage. Während die bisherigen Parkuhren grundsätzlich keine Eingaben verlangten, welche personenbezogene Rückschlüsse erlaubten, ist dies bei den neuen Parkuhren anders: Diese erfordern für den Parkvorgang die Eingabe der Kontrollschildnummer. Bei dieser Angabe handelt es sich um ein sogenanntes Personendatum, weshalb das Datenschutzrecht zur Anwendung gelangt. Denn jede Kontrollschildnummer kann einer*m bestimmten Fahrzeughalter*in zugewiesen werden. Mittels Halter*innenabfragen kann grundsätzlich eruiert werden, wer hinter einem bestimmten Kontrollschild steckt und an welcher Wohnadresse die Person registriert ist.

Die neuen Parkuhren basieren auf einem Cloud-System eines externen Auftragsdatenbearbeiters. Dies bedingt, dass über einen beschränkten Zeitraum das Kontrollschild, Angaben zum Parkvorgang sowie Angaben zu Finanztransaktionen bearbeitet werden. Die eigentliche Ablage und Bewirtschaftung der Daten erfolgt auf einer – ebenfalls neu geschaffenen – städtischen Parkdatenplattform, welche bei der Stadt selbst betrieben wird. Für die eigentliche Kontrolltätigkeit der Parkfelder sowie für das Inkasso müssen die zuständigen Abteilungen der Stadtpolizei Zugang zu den Daten in dieser Parkdatenplattform haben. Die Datenschutzstelle hat das Vorhaben im Rahmen einer Vorabkontrolle geprüft. Im Fokus standen die vertragliche Regelung mit dem Auftragsdatenbearbeiter, die Rechtsgrundlagen für die Parkplatzkontrolle, die Zugriffsregelungen sowie generell die Informationssicherheit.

Vorbereitung auf die Digitalisierung der Verwaltungsverfahren

Neue kantonale Rechtsgrundlagen ermöglichen, dass Verwaltungsverfahren zukünftig auch elektronisch durchgeführt werden können. Dies führt zu einem Ausbau von «Mein Konto», welchen die Datenschutzstelle begleitet.

Der Kanton Zürich hat neue Rechtsgrundlagen erlassen, welche per 1. Januar 2027 in Kraft treten und ermöglichen, dass Verwaltungsverfahren zukünftig auch elektronisch durchgeführt werden können. Für die Umsetzung durch den Kanton und die Gemeinden gelten umfassende Vorgaben. So müssen für die elektronischen Verfahrenshandlungen sichere Kanäle verwendet werden, die eine geschützte Übertragung ermöglichen. Zudem müssen die nutzenden Personen eindeutig identifiziert werden können und Eingaben und Anordnungen korrekt quittiert werden.

Die Stadt Zürich verfügt mit «Mein Konto», bereits über einen E-Government-Kanal, über den verschiedene Behördenkontakte sicher abgewickelt werden können. «Mein Konto» wird beispielsweise für die Steuerverwaltung, die Bewerbung für städtische Liegenschaften, die schulische Betreuung oder den Bezug des Sport Abos genutzt.

Der Stadtrat hat entschieden, «Mein Konto» auch zum massgeblichen Kanal für die Verwaltungsverfahren auszubauen. Da «Mein Konto» dadurch zukünftig viel breiter genutzt werden wird und zahlreiche neue Anforderungen erfüllen muss, führt die Datenschutzstelle eine Vorabkontrolle durch. Gleichzeitig finden zusätzliche kommunale Gesetzgebungsarbeiten statt, um die nötigen Grundlagen für die Datenbearbeitungen auf dem E-Government-Kanal «Mein Konto» zu schaffen. Die Datenschutzstelle begleitete diese umfangreichen Projektarbeiten im Berichtsjahr und wird sie im kommenden Jahr fortsetzen.

Neue Vorhaben der Videoüberwachung

Die Datenschutzstelle prüfte im Berichtsjahr erste Vorhaben der Videoüberwachung gemäss revidierter Datenschutzverordnung.

Ende 2024 trat die revidierte städtische Datenschutzversordnung (DSV) in Kraft und legte strengere Vorgaben für die Videoüberwachung durch die Verwaltung fest. Demnach müssen alle neuen Videoüberwachungen sowie Erweiterungen bestehender Systeme eine Vorabkontrolle durch die Datenschutzstelle durchlaufen.

Der Einsatz von Videoüberwachung ist nur zulässig, wenn die folgenden Voraussetzungen kumulativ erfüllt sind:

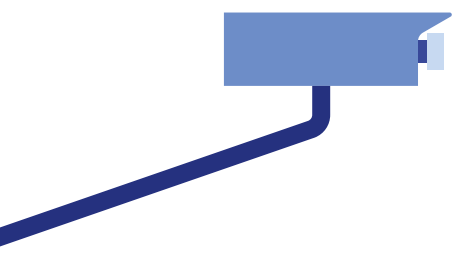
- Die Überwachung ist zur Erfüllung der öffentlichen Aufgaben erforderlich und geeignet;
- Es besteht eine erhebliche Gefahr für Leib und Leben oder für Sachen mit grosser Schadensfolge;
- Keine überwiegenden schutzwürdigen Interessen stehen der Überwachung entgegen.

Die Verhinderung oder Ahndung geringfügiger strafbarer Handlungen stellt ausdrücklich keinen hinreichenden Grund für den Einsatz von Videoüberwachung dar.

Im Berichtsjahr hat die Datenschutzstelle erste Vorhaben gemäss den neuen Vorgaben geprüft. Dabei kam sie beispielsweise für die Velostation im Stadttunnel zum Schluss, dass die strengen gesetzlichen Voraussetzungen nicht erfüllt sind. Der Diebstahl von Velos fällt in den Bagatellbereich. Zudem war nicht ersichtlich, dass im stark frequentierten Tunnel am Hauptbahnhof eine erhebliche Gefahr für Leib und Leben bestehen könnte, die sich von anderen öffentlichen unterirdischen Standorten unterscheidet und der mit Videoüberwachung begegnet werden könnte.

Zu einem anderen Schluss gelangte die Datenschutzstelle für die Parkhäuser, die infolge einer gemeinderätlichen Motion per 1. Januar 2026 in die Stadtverwaltung integriert worden sind. Die Parkhäuser waren bereits vor der Übernahme mit Videoüberwachung ausgestattet, die zwecks Aufrechterhaltung der Betriebssicherheit übernommen werden sollte. Im Rahmen der Vorabkontrolle erachtete die Datenschutzstelle die Beurteilung der zuständigen Dienstabteilung, wonach die Voraussetzungen erfüllt waren, als nachvollziehbar. Parkhäuser bergen insbesondere in Bezug auf Brände und Explosionen ein hohes Gefahrenpotenzial. Betriebliche Gründe würden hingegen nicht genügen, um den Einsatz von Videoüberwachung zu rechtfertigen.

Die Datenschutzstelle hat die Anwendung der neuen gesetzlichen Vorgaben im Berichtsjahr umgesetzt. Weitere Anfragen seitens der Stadtverwaltung sind pendent. Die Datenschutzstelle wird ihre Praxis festigen können, um eine einheitliche und rechtskonforme Umsetzung zu gewährleisten. Die bisherigen Fälle zeigen, dass die neuen gesetzlichen Vorgaben einschneidende Folgen haben dürften. Die Datenschutzstelle geht davon aus, dass zahlreiche Videoüberwachungen, die heute gestützt auf geltende Reglemente in Betrieb sind, nach Ablauf der Übergangsfrist im Herbst 2032 eingestellt werden müssen. In diese Richtung deutet auch der lesenswerte Entscheid des Verwaltungsgerichts des Kantons Zürich vom 4. September 2025 (AN.2024.00003), der die Videoüberwachung in Innen- und Aussenbereichen von Gebäuden der kantonalen Verwaltung gestützt auf ausführliche und illustrative Erwägungen als eine schwerwiegende Beschränkung der Privatsphäre qualifiziert.



Modernisierung des Fallführungssystems der SEB

Das seit Jahren in Betrieb stehende Fallführungssystem der Sozialen Einrichtungen und Betriebe wurde im Berichtsjahr angepasst und deshalb überprüft.

Informationsbearbeitungssysteme haben einen beschränkten Lebenszyklus. Bei Ablösungen und erheblichen Systemänderungen müssen neben der Informationssicherheit auch Aspekte des Datenschutzes geprüft werden. Die Datenschutzstelle legt Wert darauf, dass Anpassungen an den Systemen nicht nur technisch, sondern auch rechtlich geprüft werden.

Vor über zehn Jahren haben die Sozialen Einrichtungen und Betriebe (SEB) ein Fallführungssystem eingeführt. Dieses wurde damals von der Datenschutzstelle geprüft. Im Berichtsjahr hat dieses System im Rahmen einer «Modernisierung» verschiedene Änderungen erfahren. An den bestehenden Datenbearbeitungen hat sich allerdings nichts geändert. Aufgrund der langen Zeitspanne seit der letzten Prüfung hat die Datenschutzstelle gleichwohl eine erneute Prüfung vorgenommen. Dabei hat sich gezeigt, dass – aufgrund der rechtlichen Entwicklung im Datenschutzrecht und den damit zusammenhängenden städtischen Umsetzungsprozessen – das bestehende Datenschutzkonzept nicht mehr dem aktuellen Standard entsprach und in wesentlichen Bereichen zu aktualisieren war.

Losgelöst vom konkreten Beispiel der SEB erachtet die Datenschutzstelle ein solches aufsichtsrechtliches Vorgehen generell als angezeigt, wenn bei sogenannten «Modernisierungen» von älteren Systemen sensible Personendatenbearbeitungen betroffen sind. Dabei gilt es nicht nur, die technischen Fragen rund um die Informationssicherheit im Auge zu behalten, sondern den Fokus auch auf ein aktuelles Datenschutzkonzept zu legen, welches die Datenbearbeitungen und deren Rahmenbedingungen dokumentiert.

Integriertes Lagebild von Schweizer Blaulichtorganisationen

Im Berichtsjahr prüfte die Datenschutzstelle die Nutzung eines neuen Lageinformationssystems. Es konnte festgestellt werden, dass auf Stadtebene nur in wenigen Ausnahmefällen sensible Personendaten bearbeitet werden.

Blaulichtorganisationen wie Polizei- und Rettungsdienste sind zur zeitnahen Einschätzung und Bewältigung von Ereignissen in bestimmten Sonderlagen auf grundlegende Informationen angewiesen.

Dabei kann ein rascher Informationsaustausch über die Gemeinde- und Kantonsgrenze hinaus notwendig sein. Mehrere Blaulichtorganisationen aus der Deutschschweiz haben unter der Gesamtverantwortung der Konferenz der Kantonalen Polizeikommandantinnen und -kommandanten der Schweiz, Bereich Polizeitechnik und -Informatik (PTI) ein System aufgebaut, welches die geobasierte Darstellung aktueller Lagesituationen erlaubt. Dieses wird auf Stadtebene auch von der Stadtpolizei Zürich sowie von Schutz & Rettung genutzt. Das System wird auf der Infrastruktur und im Rechenzentrum der Kantonspolizei Zürich betrieben, weshalb die Durchführung einer Vorabkontrolle primär in der Zuständigkeit der kantonalen Datenschutzbeauftragten lag. Basierend auf dem diesbezüglichen Prüfungsergebnis hat die Datenschutzstelle die konkrete Nutzung durch die Stadtpolizei Zürich einer zusätzlichen Vorabkontrolle unterzogen.

Die Datenschutzstelle hat sich im Rahmen dieser Kontrolle die konkreten Anwendungsfälle der Stadtpolizei vor Ort vorführen lassen. Dabei konnte sich die Datenschutzstelle vergewissern, dass auf Stadtebene nur in wenigen Anwendungsfällen sensible Personendaten bearbeitet werden. Dies ist beispielsweise dann der Fall, wenn es um unmittelbare Gefährdungen für Leib und Leben geht. Die Stadtpolizei hat im Datenschutzkonzept dargelegt, gestützt auf welche gesetzlichen Grundlagen aus dem Polizeirecht solche Datenbearbeitungen zulässig sind.

Kein Anlass für eine weitere Kontrolle gab die Dienstabteilung Schutz & Rettung. Mit ihrer Nutzung des Systems sind keine sensiblen Personendatenbearbeitungen verbunden.

«Open Source Intelligence» – alles öffentlich?

Die polizeiliche Arbeit mit der sogenannten OSINT birgt datenschutzrechtliche Herausforderungen.

Unter «Open Source Intelligence» (OSINT) versteht man die Beschaffung von allgemein zugänglichen Informationen und ihre ermittlungstechnische Aufarbeitung. Das Internet dient den Strafverfolgungsbehörden als wichtige Informationsquelle. Insbesondere wird OSINT häufig zu Fahndungszwecken verwendet. Aus datenschutzrechtlicher Sicht handelt es sich aufgrund des Kontexts um die Bearbeitung besonderer Personendaten. Deshalb beschäftigte sich auch die Datenschutzstelle im Berichtsjahr mit dem Thema.

Die Verwendung von OSINT ist in der Schweiz umstritten. Dies gilt vor allem darum, weil bis dato keine spezifische gesetzliche Regelung vorliegt und eine klare Abgrenzung zwischen einfacher Recherche und klarem Grundrechtseingriff fehlt. Die Strafprozessordnung enthält zwar im Kontext der allgemeinen Ermittlungsbefugnisse Normen, die von den Strafverfolgungsbehörden als rechtfertigende Rechtsgrundlage für den Einsatz von OSINT herangezogen werden. Diese sind jedoch sehr allgemeiner Natur. Allerdings ist bald mit einer zumindest teilweisen Klärung zu rechnen: Der Kanton Zürich sieht eine Anpassung des Polizeigesetzes vor, welche unter anderem die Informationsbeschaffung im virtuellen Raum umfassen soll.

Aus datenschutzrechtlicher Perspektive ist klar: OSINT-Recherchen berühren das verfassungsrechtliche Grundrecht auf Privatsphäre. Auch wenn Personendaten öffentlich zugänglich sind, bedeutet das nicht automatisch, dass der Staat sie systematisch sammeln und analysieren darf. Dieser muss sich auf eine ausreichende gesetzliche Grundlage abstützen können. Auch eine mutmassliche Einwilligung von Betroffenen kann eine solche gesetzliche Grundlage nicht ersetzen. Zudem ist oftmals schwer zu eruieren, wer welche Informationen im Internet tatsächlich selbst und freiwillig publiziert hat.

Für die datenschutzrechtliche Beurteilung erscheint eine differenzierte Betrachtung nötig, da verschiedene Recherchemethoden unterschiedlich stark in die Privatsphäre eingreifen. So ist eine Suche in den vollständig öffentlichen Suchmaschinen wie beispielsweise Google anders zu bewerten als die Nutzung eines sozialen Netzwerkes, das die Überwindung spezieller Zugangshürden (wie beispielsweise das Anlegen eines eigenen Kontos) erfordert.

Für die Datenschutzstelle ist nachvollziehbar, dass die Polizei für ihre Arbeit das Internet als Informationsquelle nutzen können muss. Jedoch setzen das Strafprozess- und das Datenschutzrecht Grenzen. Eine rechtskonforme Nutzung setzt eine sorgfältige Prüfung voraus. Der Erlass spezifischer gesetzlicher Grundlagen in Bezug auf OSINT würde Klarheit schaffen und wäre daher wünschenswert.

Soziale Rezepte im Stadtspital

Das Stadtspital betritt auf Anstoss des Gemeinderates mit einem vierjährigen Pilotprojekt gesundheitspolitisches Neuland.

Das medizinische Fachpersonal in fünf Ambulatorien des Stadtspitals kann neu sogenannte «Soziale Rezepte» ausstellen. Dabei werden Patient*innen an eine soziale Koordinationsstelle vermittelt, die begleitet, berät und nicht-medizinische Massnahmen zugänglich macht. Das Projekt geht zurück auf die Motion zweier Gemeinderäte. Vorreiter für das Vorhaben ist Grossbritannien, wo die Verschreibung «Sozialer Rezepte» schon seit vielen Jahren Eingang ins Gesundheitswesen gefunden haben. Bei Patient*innen in schwierigen und therapieintensiven Situationen verspricht sich die Fachwelt durch Integration der sozialen Aspekte eine raschere Genesung und in der Konsequenz eine wesentliche Senkung der Gesundheitskosten. Im Rahmen eines vierjährigen Projektes setzt das Stadtspital in Kooperation mit dem Sozialdepartement die Idee «Sozialer Rezepte» um. Die Datenschutzstelle war in das Projekt frühzeitig involviert.

Da bei diesem Vorhaben sensible Personendaten zwischen dem Stadtspital und den involvierten Fachpersonen des Sozialdepartementes ausgetauscht und dokumentiert werden, war die datenschutzrechtliche Prüfung der Rahmenvoraussetzungen Ausgangspunkt dieses Vorhabens. Einerseits war die Freiwilligkeit der Teilnahme und damit verbunden das Patient*innengeheimnis zu beachten, andererseits standen auch Aspekte der Behandlungsdokumentation und der Informationssicherheit im Fokus. Die Datenschutzstelle hat die Projektverantwortlichen von Anfang an datenschutzrechtlich beraten und das Pilotprojekt im Rahmen der Vorabkontrolle geprüft.

Digitalisierung des Vikariat-Prozesses

Das Schul- und Sportdepartement sah im bestehenden Personalprozess für Absenzen von Lehr- und Therapiepersonen und den damit verbundenen Vikariatsmeldungen dringenden Handlungsbedarf und beabsichtigte, diesen zu digitalisieren.

Die Personendatenbearbeitungen der Stadtverwaltung müssen dem Grundsatz der Verhältnismässigkeit standhalten. Als Teil dieses Grundsatzes gilt die Regel der Datensparsamkeit. Für einen Prozess sollen immer nur so viele Personendaten verwendet werden wie unbedingt nötig. Ausgangspunkt ist hierbei der Zweck eines Vorhabens. Im Zusammenhang mit den Vikariatsmeldungen lag das Hauptziel in der effizienteren Ausgestaltung des damals physischen Prozesses. Neu sollten die Schulen eine Vikariatsmeldung digital erfassen und die Suche nach geeigneten Vikar*innen aufgrund der gewünschten Kriterien (Ausfalldauer, Klassenstufe, Fachbereich usw.) direkt über das Tool abwickeln.

Die Datenschutzstelle kam im Rahmen der Vorabkontrolle zum Schluss, dass der Grundsatz der Datensparsamkeit nicht vollumfänglich eingehalten war. Zur Diskussion stand dabei insbesondere die Verwendung von besonderen Personendaten, wie beispielsweise Arztzeugnissen, welche mit der Erreichung des beabsichtigten Ziels nicht direkt einhergingen.

Das Schul- und Sportdepartement setzte diesen Kritikpunkt um und passte den geplanten Prozess diesbezüglich an, indem die bearbeiteten Daten reduziert wurden. Das Anliegen der Datenschutzstelle, dass gerade bei besonderen Personendaten die Zweck-Mittel-Relation stimmen muss, wurde beachtet und umgesetzt. Es handelt sich um ein gutes Beispiel dafür, wie Digitalisierung und Datenschutz nicht im Widerspruch zueinanderstehen, sondern sich gegenseitig stärken können – wenn sie mit Sorgfalt umgesetzt werden.

Publikumsapotheke im Stadtspital

Auf Anlass einer Anfrage der Rechnungsprüfungskommission des Gemeinderates setzte sich die Datenschutzstelle mit der Frage auseinander, ob eine private Apotheke im Stadtspital Zugriff auf Patient*innendaten haben darf.

In der Eingangshalle des Stadtspitals Triemli gibt es neu eine privat betriebene Publikumsapotheke. Dieser wurde zur Erleichterung der Abläufe ein Direktzugriff auf die Patientendokumentation des Stadtspitals ermöglicht. Nach eingehenden Abklärungen durch die Datenschutzstelle wurde die direkte Zugriffsmöglichkeit wieder eingestellt.

Patient*innen sind bei einem Spitalaustritt regelmässig auf rezeptpflichtige Medikamente angewiesen. Diese müssen sie in der Regel ausserhalb des Stadtspitals selbst besorgen. Als Dienstleistung für die Patient*innen wurde in der Eingangshalle des Stadtspitals eine private Publikumsapotheke eröffnet. Dieser wurde ein direkter Zugriff auf Teilbereiche der Patient*innendokumentation gewährt. Damit sollten die notwendigen Zusatzabklärungen bei rezeptpflichtigen Medikamenten erleichtert werden.

Die Rechtsprüfungskommission des Gemeinderates ersuchte von der Datenschutzstelle eine Prüfung dieser direkten Zugriffsmöglichkeit der Publikumsapotheke. Die Daten der Patient*innen unterstehen besonderen Schweigepflichten. Ein Zugriff auf diese Daten durch Dritte ist nur zulässig, wenn entsprechende gesetzliche Grundlagen dies erlauben oder die ausdrückliche Einwilligung der betroffenen Patient*innen vorliegt. Die Datenschutzstelle konnte im Rahmen der Abklärungen feststellen, dass im konkreten Prozess die Einwilligung für den Zugriff auf die Patientendokumentation einzelfallweise abgeholt wurde. Aufgrund der geringen Anzahl effektiv getätigter Zugriffe durch die Publikumsapotheke kam die Datenschutzstelle allerdings zur Beurteilung, dass keine Notwendigkeit für eine direkte Zugriffsmöglichkeit besteht. Das Stadtspital leitete in der Folge den Rückbau der Zugriffsmöglichkeit der Publikumsapotheke in die Wege.

Datenschutzvorfälle und menschliches Fehlverhalten

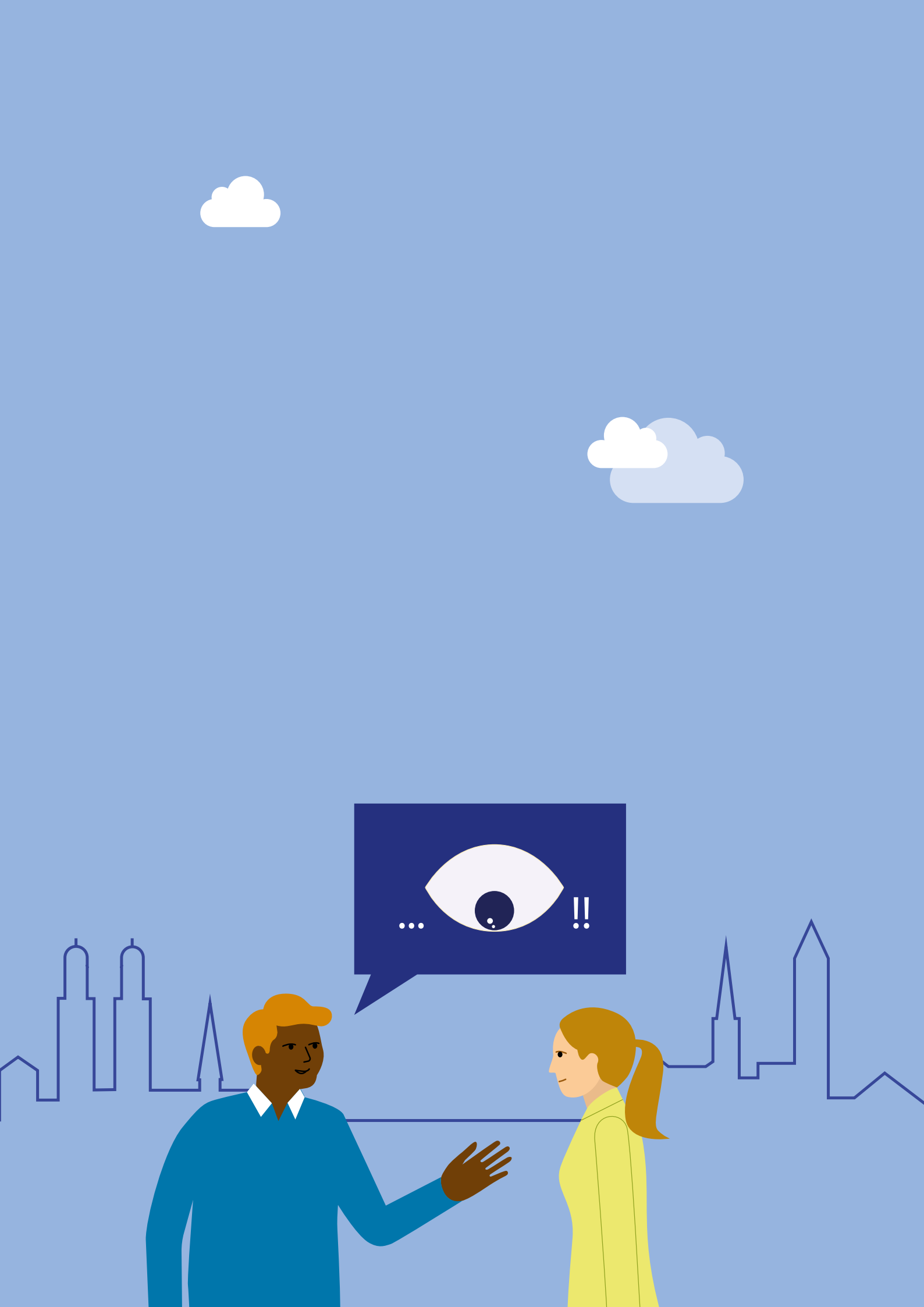
Datenschutzvorfälle entstehen in der Stadtverwaltung häufig aufgrund unachtsamen Verhaltens von Mitarbeitenden.

Wenn Personendaten der Stadtverwaltung unbefugt bearbeitet werden oder verloren gehen, spricht das Gesetz von einem Datenschutzvorfall. Ab einer gewissen Intensität stellt ein solcher Vorfall eine Gefährdung für die Grundrechte der betroffenen Person dar und muss der Datenschutzstelle unverzüglich gemeldet werden.

Die Datenschutzstelle begleitete im Berichtsjahr mehrere Datenschutzvorfälle, welche auf menschliches Fehlverhalten zurückzuführen waren. So unterliefen beispielsweise Mitarbeitenden Fehler beim Post oder E-Mail-Versand, indem sie vertrauliche Dokumente mit besonderen Personendaten unbeteiligten Dritten zustellten.

Bei solchen Vorfällen arbeitet die Datenschutzstelle zusammen mit der verantwortlichen Dienstabteilung geeignete Massnahmen aus, um einerseits die Situation zu bewältigen und andererseits gleichgelagerte Vorfälle in Zukunft zu verhindern. Als Massnahmen kommen primär die Sensibilisierung der Mitarbeitenden sowie die Einführung eines Vier-Augen-Prinzips in Frage. Bei häufigen Fehlern müssen weitere Massnahmen, wie beispielsweise auch die Auslagerung des Postversands an eine dafür spezialisierte Stelle in Betracht gezogen werden.

Die Datenschutzvorfälle zeigen einmal mehr, wie wichtig die Mitwirkung und eine datenschutzbewusste Haltung der städtischen Mitarbeitenden sind, um den Datenschutz zu gewährleisten.



5 Beratung von Stadtverwaltung und Privaten

Einleitung

Die Datenschutzstelle wird regelmässig von Rechtsdiensten, Mitarbeitenden oder Führungskräften der Stadtverwaltung gebeten, Informationsbearbeitungen aus datenschutzrechtlicher Optik zu beurteilen. Dabei geht es beispielsweise darum, ob Personendaten mit anderen Verwaltungsstellen ausgetauscht oder Informationen veröffentlicht werden dürfen, zu bestimmten Vorkommnissen Auskunft erteilt werden darf oder wie bei Forschungsprojekten mit Personendaten umzugehen ist.

Auch Privatpersonen wenden sich regelmässig an die Datenschutzstelle. Ihre Anfragen und Reklamationen führen regelmässig zu umfangreichen Abklärungen: Bevor die Datenschutzstelle eine datenschutzrechtliche Beurteilung abgeben kann, müssen Sachverhalt und Rechtslage unter Mitwirkung der betroffenen städtischen Verwaltungsstellen genau geklärt werden. Solche «Anstösse von aussen» können systematische Defizite bei Datenbearbeitungen in der Stadtverwaltung aufzeigen und zu Prozessoptimierungen führen.

Im Berichtsjahr 2025 waren die Themen der Beratungstätigkeit sehr facettenreich, wie die nachfolgenden Beispiele aus dem Arbeitsalltag der Datenschutzstelle zeigen.

Revision der Publikationsverordnung

Bei der neuen Publikationsverordnung des Gemeinderates stand die Anonymisierungspflicht der amtlichen Mitteilungen nach Ablauf der Publikationsfrist im Vordergrund.

Aufgrund einer gemeinderätlichen Motion hatte sich die Stadtkanzlei im Berichtsjahr mit der Publikation von amtlichen Mitteilungen auseinanderzusetzen. Hierzu erarbeitete sie eine entsprechende Vorlage zur Teilrevision der bestehenden Publikationsverordnung sowie der zugehörigen Ausführungsbestimmungen. Da in amtlichen Publikationen auch Personendaten enthalten sein können, war die Vorlage auch aus Sicht des Datenschutzes zu prüfen.

Im Rahmen der Vorprüfung erwirkte die Datenschutzstelle in Bezug auf die Publikation amtlicher Mitteilungen mit Personendaten im Internet weitergehende technische und organisatorische Abklärungen. Solche Publikationen dürfen zum Schutz der Privatsphäre zeitlich nicht unbeschränkt im Internet verfügbar sein. Dennoch haben die Bürger*innen in Bezug auf staatliches Handeln ein verfassungsmässiges Recht auf Information. Um diesen beiden Interessen genügend Rechnung zu tragen, können amtliche Mitteilungen zeitlich unbeschränkt im Internet zur Verfügung gestellt, müssen jedoch nach Ablauf einer bestimmen Publikationsfrist anonymisiert werden. Die neue Publikationsverordnung sieht hierfür eine generelle Frist von drei Monaten vor. Gestützt auf die Vorabklärungen der Stadtkanzlei konnte sich die Datenschutzstelle vergewissern, dass nach Ablauf dieser Frist auf den offiziellen Publikationskanälen der Stadt nur noch die anonymisierten Mitteilungen zur Verfügung stehen.

Trotzdem besteht aus Sicht Datenschutz bei allen Internetpublikationen eine gewisse Ohnmacht: Was einmal im Netz ist, bleibt auch dort. Es kann nicht verhindert werden, dass die ursprünglichen, mit Personendaten versehenen amtlichen Mitteilungen als Kopien allenfalls doch in einem Internetarchiv recherchierbar sind. Deshalb muss gerade der Inhalt der ursprünglichen Publikation stets sorgfältig geprüft werden.

Früherkennungssystem bei Ertrinkungsfällen

Die Datenschutzstelle beriet das Sportamt zu einem Früherkennungssystem bei Ertrinkungsfällen. Gemeinsam konnte im sensiblen Umfeld von Badeanstalten ein maximal datenschutzfreundliches Ergebnis erreicht werden.

Im Frühjahr 2025 kam das Sportamt auf die Datenschutzstelle zu und gab an, dass sie einen Pilotversuch in einem städtischen Hallenbad machen wollten. Über ein Früherkennungssystems (sog. Unterwasserdetektion) sollten das Badepersonal im Notfall rechtzeitig alarmiert und Ertrinkungsfälle verhindert werden.

Das System arbeitet mit Unterwassersensoren, welche die möglichen Ertrinkungsnotfälle registrieren. Augenscheinlich mussten in diesem Projekt zuerst Aspekte des Datenschutzes geprüft werden.

Das Sportamt hat die Datenschutzstelle frühzeitig in dieses Vorhaben einbezogen. Die Datenschutzstelle konnte gemeinsam mit dem Sportamt erreichen, dass die Funktionsweise und Ausgestaltung des Systems so konzipiert werden, dass durch das Unterwasserdetektionssystem zwar visuelle Informationen, aber keine Personendaten bearbeitet werden und damit weder das kantonale Datenschutzrecht noch die Bestimmungen zur Videoüberwachung der städtischen Datenschutzverordnung zur Anwendung kommen.

Mit anderen Worten: Beim fraglichen Unterwasserdetektionssystem sind keine Personen erkennbar und können auch nicht nachträglich erkennbar gemacht werden. Aus datenschutzrechtlicher Sicht ist dies im sensiblen Kontext von Badeanlagen sehr zu begrüssen. Das Projekt ist somit ein gutes Beispiel dafür, wie neue Technologien durch datenschutzfreundliche Voreinstellungen eingesetzt werden können, ohne dass dabei in Bezug auf die Wirksamkeit des Systems Abstriche gemacht werden müssen.

Strafregisterauszüge während laufender Anstellung

Strafregisterauszüge von Stellenbewerber*innen können eingeholt werden – während laufender Anstellung fehlen auf städtischer Ebene Regeln.

Das städtische Personalrecht sieht vor, dass Anstellungsinstanzen von Stellenbewerber*innen die Einreichung eines Strafregisterauszuges verlangen können. Auch diese Leumundsprüfungen werfen schwierige Fragen auf, wie die Datenschutzstelle im letztjährigen Tätigkeitsbericht 2024 ausführte. Für laufende Anstellungsverhältnisse gilt dies umso mehr, da eine vergleichbare gesetzliche Grundlage fehlt. Die Datenschutzstelle wurde im Berichtsjahr angefragt, ob auch bei aktiven Mitarbeitenden unter Umständen Leumundsprüfungen durchgeführt werden können, oder ob dies – mangels gesetzlicher Grundlage – ausgeschlossen ist. Die Frage stellt sich insbesondere bei Tätigkeiten mit besonders vulnerablen Personen sowie jahrelangen Anstellungsverhältnissen, wie sie in der Stadtverwaltung nicht selten vorkommen.

Im Bundesrecht besteht eine ausreichende formell-gesetzliche Grundlage, die es auch auf städtischer Ebene ermöglicht, während der Anstellung für gewisse Gruppen von Mitarbeitenden sogenannte Sonderprivatauszüge einzuholen. Dies betrifft alle Mitarbeitenden, die regelmässig Kontakt mit Minderjährigen oder anderen besonders schutzbedürftigen Personen haben oder eine Tätigkeit im Gesundheitsbereich mit direktem Kontakt zu Patient*innen ausüben.

Unabhängig davon können Behörden auch Anstellungsvoraussetzungen für Tätigkeiten festlegen. Aus der Spezialgesetzgebung ergibt sich punktuell bereits heute eine Pflicht zur Einholung von Strafregisterauszügen, so beispielsweise für Polizist*innen, Mitarbeitende in Kindertagesstätten sowie für Schulleitende und Lehrpersonen.

Die Datenschutzstelle geht davon aus, dass die Frage nach Leumundsprüfungen während der Anstellung – für alle Bereiche, in denen heute eine Grundlage fehlt – in den kommenden Jahren aktuell bleiben wird und eine Regelung im städtischen Personalrecht zweckmässig wäre.

Wie weit geht der Schutz der Berufsgeheimnisse?

Eine Gesundheitsinstitution, welche im öffentlichen Auftrag Leistungen im Bereich der Suchtmedizin erbringt, gelangte mit einer Anfrage von allgemeinem Interesse an die Datenschutzstelle.

Im Zusammenhang mit einem potenziell strafrechtlich relevanten Vorfall zwischen einer*m Patientin*en einer im öffentlichen Auftrag der Stadt Zürich tätigen Institution im Bereich Suchtmedizin und einer*m Sicherheitsmitarbeiter*in ergab sich die Frage, wie eine Meldung an die Polizei datenschutzkonform zu handhaben ist.

Konkret wollte die Leitung der betreffenden Gesundheitsinstitution wissen, ob sie der Polizei den Namen der*s mutmasslichen Täterin*s bekannt geben dürfe, obwohl diese Person in ihrer Institution Patient*in sei. Mit anderen Worten: Kann es sein, dass das ärztliche Berufsgeheimnis eine Anzeige verhindert?

Die ärztliche Schweigepflicht kann grundsätzlich nur durchbrochen werden, wenn eine gesetzliche Bestimmung auf Bundes- oder Kantonsebene eine ermächtigende Rechtsgrundlage im Sinne einer Meldepflicht oder zumindest eines Melderechts vorsieht. Ist keine solche Bestimmung vorhanden muss die Einwilligung der betroffenen Person eingeholt werden oder bei der Gesundheitsdirektion die Entbindung vom Berufsgeheimnis beantragt werden. Auch Hilfspersonen unterstehen dem ärztlichen Berufsgeheimnis. Diese Voraussetzungen sind auch im Rahmen der Strafverfolgung zu beachten.

Gestützt auf eine im Gesundheitsgesetz verankerte gesetzliche Bestimmung dürfen Personen, die einen Beruf im Gesundheitswesen ausüben, sowie deren Hilfspersonen Wahrnehmungen der Polizei melden, welche unter anderem auf ein Verbrechen oder Vergehen gegen Leib und Leben schliessen lassen. Die Gesundheitsinstitution konnte sich im konkreten Fall auf diese Bestimmung abstützen und den Vorfall zur Anzeige bringen.

Die Datenschutzstelle begrüsste es im vorliegenden Fall, dass sich die zuständigen Personen der Gesundheitsinstitution im Vorfeld die richtigen Überlegungen machten und um die Einhaltung des Datenschutzrechts bemüht waren.

Einsicht in die eigenen Bewerbungsunterlagen

Der korrekte Umgang mit personenbezogenen Unterlagen aus Bewerbungsverfahren ist aus unterschiedlichen Gründen relevant. Auch der Zugang zu eigenen Personendaten spielt eine Rolle.

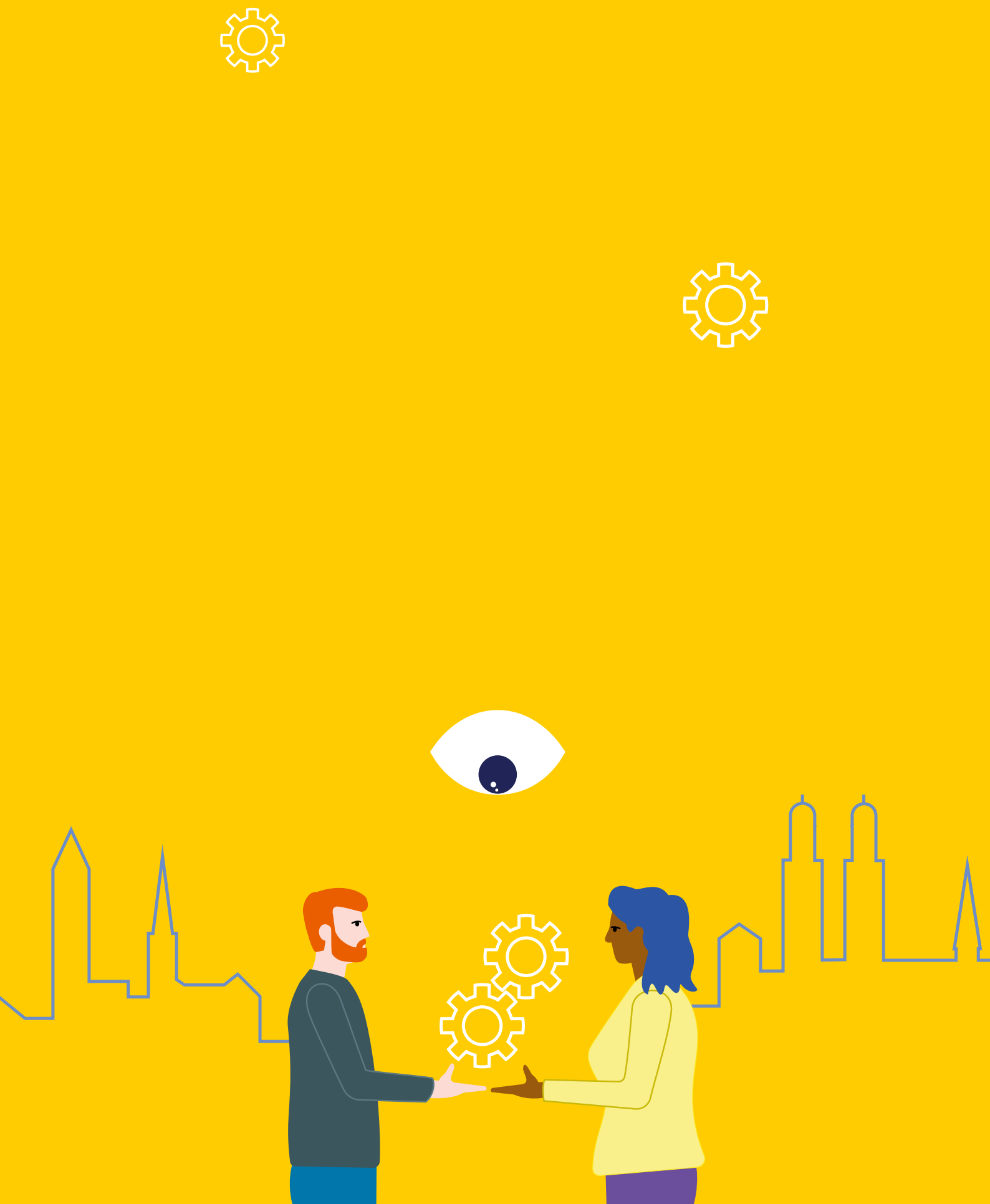
Die Stadtverwaltung Zürich schreibt als Arbeitgeberin fast täglich neue Stellen aus. Für gewisse Stellen werden neben dem ordentlichen Bewerbungsverfahren zusätzliche Testverfahren durchgeführt. Nicht für alle Interessent*innen endet dieser Prozess in einer Anstellung. Im Jahr 2025 gelangten einige Privatpersonen an die Datenschutzstelle. Sie stellten die Frage, inwiefern sie nach einer Absage Einsicht in die für die Rekrutierung erstellten Dossiers und insbesondere in die Testergebnisse verlangen können.

Bei solchen Testverfahren können dem gesetzlichen Anspruch auf Einsicht ins eigene Bewerbungsdossier die Interessen der Verwaltung an der Geheimhaltung der Funktionsweise solcher Assessments bzw. deren Fragen und Ergebnisse entgegenstehen. Die Datenschutzstelle empfiehlt, dass bei solchen Konstellationen die Interessenabwägung im Einzelfall konkret vorgenommen wird und möglichst bereits vorgängig gegenüber den Interessent*innen verständlich kommuniziert wird.

Für die betroffenen Personen soll es generell im Bewerbungsverfahren möglich sein, die Entscheide nachvollziehen zu können. Dazu gehört nicht nur die Möglichkeit, Einsicht in das Dossier zu nehmen, sondern von der Anstellungsinstanz auch eine verständliche Auskunft darüber zu erhalten, weshalb eine Bewerbung nicht erfolgreich war – etwa aufgrund spezifischer Kriterien oder Testergebnisse. Gleichzeitig müssen alle Unterlagen nach Abschluss des Verfahrens zurückgegeben oder nach einer bestimmten Frist ordnungsgemäss gelöscht und vernichtet werden, sofern keine rechtliche Aufbewahrungsfrist besteht.

Relevant ist die Frage dabei keineswegs nur bei negativen Entscheiden: Auch bei einer Anstellung ist die korrekte Ablage der Unterlagen im Personaldossier für eine spätere Einsicht entscheidend.

Transparenz im Bewerbungsprozess schafft einerseits das notwendige Vertrauen der Bewerber*innen in die Verwaltung als Anstellungsinstanz, andererseits stärkt sie die Respektierung des Datenschutzrechts durch die Personalverwaltung als Ganzes.

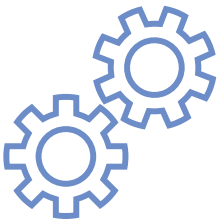


6 Zusammenarbeit und Prozesse

Einleitung

Die Datenschutzstelle ist, wie die öffentliche Verwaltung generell, gesetzlich zu einer wirksamen und wirtschaftlichen Verwaltungsführung verpflichtet. Es ist deshalb wichtig, dass sie verwaltungsinterne Prozesse, städtische Kontrollmechanismen, Synergien und Gremien nutzt, damit sie ihrem Anliegen – der Einhaltung des Datenschutzrechts – maximale Wirkung verleihen kann.

Verbindliche und wirkungsvolle Prozesse dienen der Umsetzung des Datenschutzes und helfen dabei, das «Datenschutzsystem» in der Stadtverwaltung nachhaltig weiterzuentwickeln. Wichtige Beispiele sind der Prüfprozess bei sämtlichen neuen IT-Vorhaben sowie der Prozess zur Stellungnahme der Datenschutzstelle im Gesetzgebungsverfahren. Die Datenschutzstelle entwickelt diese und neue Prozesse regelmässig weiter und etabliert auch Kontrollmechanismen, um das Datenschutzniveau der Stadtverwaltung zu stärken. Dabei arbeitet sie mit anderen Aufsichtsbehörden, der Fachstelle Informationssicherheit und weiteren Stakeholdern zusammen, vertieft so ihr Fachwissen und gleicht ihre Haltung ab. Im Berichtsjahr hat die Datenschutzstelle neue Prozesse etabliert und die Zusammenarbeit mit diversen Gremien und Stellen weiter intensiviert.



Interne und externe Zusammenarbeit

Die Datenschutzstelle arbeitet eng mit der Stadtverwaltung und externen Fachstellen zusammen.

Nachfolgend werden die wichtigsten Kooperationen der Datenschutzstelle umschrieben.

IDG-Fachgruppe

In der IDG-Fachgruppe treffen sich unter der Leitung der Datenschutzstelle und des Rechtskonsulenten die Datenschutzberater*innen der Departemente und der Stadtkanzlei, die Öffentlichkeitsgrundsatzbeauftragten der Departemente sowie weitere an der Thematik interessierte Jurist*innen **drei Mal jährlich** zu Themensitzungen.

Die Ziele dieser Treffen sind der Erfahrungsaustausch, die Diskussion von Herausforderungen aus der Praxis und möglichen Lösungen, aber auch die Vernetzung unter den Teilnehmenden. Weiter interformieren die Leitenden der Fachgruppe regelmässig über Entwicklungen aus Gesetzgebung, Rechtsprechung und Lehre.

Im Jahr 2025 wurden in der IDG-Fachgruppe unter anderem folgende Themen diskutiert: das KI-Reglement der Stadtverwaltung und seine Auslegung, die datenschutzrechtliche Einordung des Moratoriums in Bezug auf die Nutzung von M365 und die Sichtbarkeit bei den Outlook-Kalendern sowie die damit verbundene Datenschutzproblematik. Zudem wurde seitens der Datenschutzstelle eine Umfrage bei den Datenschutzberater*innen zum Zugang zu den eigenen Personendaten gemäss § 20 Abs. 2 IDG durchgeführt. Ziel dieser Umfrage war nicht nur die Bestandesaufnahme, sondern die Evaluation von Massnahmen, welche die Rechte der Betroffenen bezüglich Zugangs zu den eigenen Personendaten stärken. Diese Massnahmen befinden sich in Umsetzung.

Zusammenarbeit mit der Fachstelle Informationssicherheit

Diese Fachstelle der städtischen Dienstabteilung Organisation und Informatik (OIZ) prüft alle Informatikvorhaben auf die Einhaltung der Vorschriften zur Informationssicherheit. Die Prüfung erfolgt im Rahmen des städtischen ISDS-Prozesses und in enger Koordination mit der Datenschutzstelle. Die Datenschutzstelle tauscht sich sowohl projektbezogen als auch darüber hinaus regelmässig mit der Fachstelle Informationssicherheit aus. Themen sind unter anderem die Datensicherheit in der Stadtverwaltung, meldepflichtige Datenschutzvorfälle aber auch strategische Themen und Weichenstellungen.

Im Berichtsjahr wurden gemeinsame Schulungen im Bereich Datenschutz und Datensicherheit angeboten. Diese Formate sollen in den nächsten Jahren weiter ausgebaut werden.

Zusammenarbeit mit anderen Datenschutzstellen der Kantone und Gemeinden/Privatim

Die Datenschutzstelle arbeitete im Jahr 2025 bei mehreren Geschäften mit Datenschutzstellen anderer Gemeinden oder Kantone zusammen, holte Einschätzungen zu anonymisierten Sachverhalten ein oder gab diese selbst ab. Insbesondere mit der Datenschutzstelle des Kantons Zürich pflegt sie einen regelmässigen fachlichen Austausch.

Die Datenschutzstelle der Stadt Zürich ist zudem aktives Mitglied von Privatim, der Konferenz der schweizerischen Datenschutzbeauftragten (www.privatim.ch). Die Datenschutzbehörden aller 26 Kantone, diejenigen von acht Gemeinden sowie der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) gehören Privatim an. Durch einen gemeinsamen Austausch vertiefen die Mitglieder von Privatim ihr Fachwissen sowie ihre Haltung und können ihre Auslegung mit anderen Aufsichtsbehörden abgleichen.

Die Datenschutzstelle der Stadt Zürich war im Jahr 2025 in **folgenden Arbeitsgruppen von Privatim** vertreten:

AG X (Gesundheit): In dieser Arbeitsgruppe diskutieren Jurist*innen aktuelle Themen aus dem Gesundheitsbereich. Im Berichtsjahr hat die Datenschutzstelle der Stadt Zürich an einem internen Merkblatt mitgewirkt, welches verschiedenen aufsichtsrechtlichen Fragen im Spitalbereich nachgeht. Je nach Organisation eines Spitals und abhängig von den öffentlichen Leistungsaufträgen können unterschiedliche aufsichtsrechtliche Zuständigkeiten und damit zusammenhängende schwierige Abgrenzungsfragen entstehen. Dasselbe zeigt sich bei medizinischen Registern oder etwa in der Medizinforschung.

AG Digitale Verwaltung: In der AG Digitale Verwaltung besprechen Jurist*innen und Informatiker*innen primär kantonsübergreifende Digitalisierungsprojekte, aber auch Gesetzgebungsvorhaben. Die AG trifft sich alle drei Monate und ermöglicht den Teilnehmenden einen regelmässigen, unkomplizierten Erfahrungsaustausch. Das von der Unterarbeitsgruppe KI erarbeitete Merkblatt zu online KI-Applikationen wurde 2025 in der AG diskutiert und finalisiert. Es richtet sich an Entscheidungsträger*innen in kantonalen Verwaltungen, erläutert die wichtigsten Datenschutzvorgaben und soll die Entscheidung erleichtern, ob und welche KI eingesetzt wird. Die AG Digitale Verwaltung erleichtert den Wissenstransfer zwischen den Mitarbeitenden der städtischen und kantonalen Datenschutzstellen.

AG Sicherheit: Nach einer längeren Pause hat die Arbeitsgruppe Sicherheit im November 2025 zu einer Sitzung eingeladen. Ab 2026 soll wieder regelmässig über rechtliche Fragen im Bereich der Sicherheit diskutiert und bei Vorhaben von überregionaler Bedeutung zusammengearbeitet werden. Die Datenschutzstelle der Stadt Zürich ist ein dieser Arbeitsgruppe vertreten und begrüsst den fachlichen Austausch in diesem wichtigen Bereich.

Forschungsvorhaben mit städtischen Daten

Die Stadtverwaltung wird häufig um die Bekanntgabe von Daten für Forschungsprojekte ersucht. Dabei müssen Vorgaben eingehalten werden, für deren Umsetzung die Datenschutzstelle neue Hilfsmittel bereitstellt.

Die Bundesverfassung gewährleistet die Freiheit der wissenschaftlichen Lehre und Forschung. Gestützt auf diese allgemeine Grundlage können Forschungsstellen zu Forschungszwecken Daten von öffentlichen Organen verlangen.

Das kantonale Datenschutzrecht enthält verschiedene Bestimmungen über die Datenbekanntgabe zu nicht personenbezogenen Zwecken und definiert die notwendigen Prozesse. Eine Datenbekanntgabe ist grundsätzlich möglich, sofern dies nicht durch eine rechtliche Bestimmung ausgeschlossen ist. Die empfangende Forschungsstelle muss nachweisen, dass die Personendaten anonymisiert werden, aus den Auswertungen keine Rückschlüsse auf betroffene Personen möglich sind und die ursprünglichen Personendaten nach der Auswertung vernichtet werden. Das öffentliche Organ muss einen schriftlichen Entscheid über die Bewilligung des Gesuchs erlassen oder eine entsprechende Vereinbarung schliessen.

Die Datenschutzstelle stellte in der Vergangenheit wiederholt fest, dass diese Vorgaben in der Stadtverwaltung noch zu wenig bekannt sind und in der Praxis erhebliche Unsicherheiten bezüglich der konkreten Umsetzung bestehen. Sie hat deshalb im Berichtsjahr für die Datenbekanntgaben von Personendaten zu Forschungszwecken ein Merkblatt, ein Gesuchsformular sowie einen Musterentscheid ausgearbeitet.

Neues Kontrollkonzept der Datenschutzstelle

Das neu erarbeitete Kontrollkonzept der Datenschutzstelle verschärft massgeblich die konkrete Aufsichtstätigkeit und sieht insbesondere bei Projekten vermehrte Stichkontrollen vor.

Neben der Beratung der öffentlichen Organe der Stadt Zürich hat die Datenschutzstelle gemäss den gesetzlichen Vorgaben auch aufsichtsrechtliche Aufgaben zu erfüllen, unter anderem in Form von Kontrollen. In zwei Bereichen hat die Datenschutzstelle bisher die Durchführung systematischer Kontrollen etabliert: im Rahmen der gesetzlich vorgesehenen Vorabkontrollen sowie der Kontrollen infolge meldepflichtiger Datenschutzvorfälle. Diese Kontrollen hat die Datenschutzstelle mit verbindlichen Prozessabläufen und Vorlagen operationalisiert. Neben diesen systematischen Kontrollen wird die Datenschutzstelle immer wieder auf Anstoss bzw. Hinweis der Bevölkerung oder der Verwaltung aufsichtsrechtlich aktiv.

Im Berichtsjahr hat die Datenschutzstelle ein Kontrollkonzept erarbeitet, welches vermehrte Stichkontrollen ins Auge fasst. Damit soll einerseits die Datenschutzqualität insbesondere bei Projekten weiter erhöht werden und andererseits soll durch die zusätzlichen Kontrollen ein klares Signal an die Verantwortlichen gesendet werden, dass das Thema Datenschutz ernst zu nehmen sei. Das geltende Datenschutzrecht gibt der Datenschutzstelle den nötigen gesetzlichen Spielraum zur Umsetzung dieser Kontrollen.

Gesetzgebungsprojekte

Die Datenschutzstelle prüft Erlassentwürfe, welche Belange des Datenschutzes betreffen.

Werden rechtliche Grundlagen der Stadtverwaltung neu geschaffen oder angepasst, welche Belange des Datenschutzes betreffen, prüft die Datenschutzstelle diese Erlassentwürfe. Sie ist regelmässig bereits in die entsprechenden Gesetzgebungsprojekte involviert.

Den gesetzlichen Grundlagen kommt aus Sicht des Grundrechts- und Persönlichkeitsschutzes grosse Bedeutung zu. Das Gesetzmässigkeitsprinzip schreibt vor, dass sich staatliches Handeln auf eine normstufengerechte und hinreichend bestimmte gesetzliche Grundlage stützen muss. Auch aus Gründen der Rechtssicherheit sowie der Transparenz und Information gegenüber den von staatlichen Datenbearbeitungen betroffenen Personen sind entsprechende Regelungen wichtig. Betroffene Personen sind dabei nicht nur Bürger*innen, sondern auch die Mitarbeitenden der Verwaltung.

Im Jahr 2025 begleitete die Datenschutzstelle unter anderem folgende Gesetzgebungsprojekte, welche zumindest teilweise noch nicht abgeschlossen sind:

- Revision IDV (kantonale Verordnung über die Information und den Datenschutz, LS 170.41)
- Revisionen Personalrecht und Ausführungsbestimmungen (u.a. Einsicht ins Personaldossier)
- Städtisches Reglement Datenaustausch (RDA)
- Städtische KI-Richtlinie
- Teilrevision Publikationsverordnung
- Verordnung Politikfinanzierung
- Verordnung über die Testung sexuell übertragbarer Infektionen
- Verordnung über die Bewilligung von Ausgaben für die Arbeitsintegration

7 Datenschutzstelle – Vorstellung und Aufgaben

Wer sind wir?

Die Datenschutzstelle der Stadt Zürich besteht aus der Datenschutzbeauftragten, vier juristischen Mitarbeitenden und einer Sekretariatsmitarbeiterin.

Im Berichtsjahr 2025 setzte sich die Datenschutzstelle personell wie folgt zusammen:

- Patrizia Schwarz, Dr. iur.; Datenschutzbeauftragte (80%)
- Jürg von Flüe, lic. iur.; Stv. Datenschutzbeauftragter (70%)
- Nina van Haaften, MLaw; Juristische Mitarbeiterin (60%)
- Meret Tobler, RA; MLaw; Juristische Mitarbeiterin (80%)
- Marion Weber, lic. iur.; dipl. inform. UZH; Mitarbeiterin Recht und Informatik (80%)
- Christine Dickey; Sekretariat

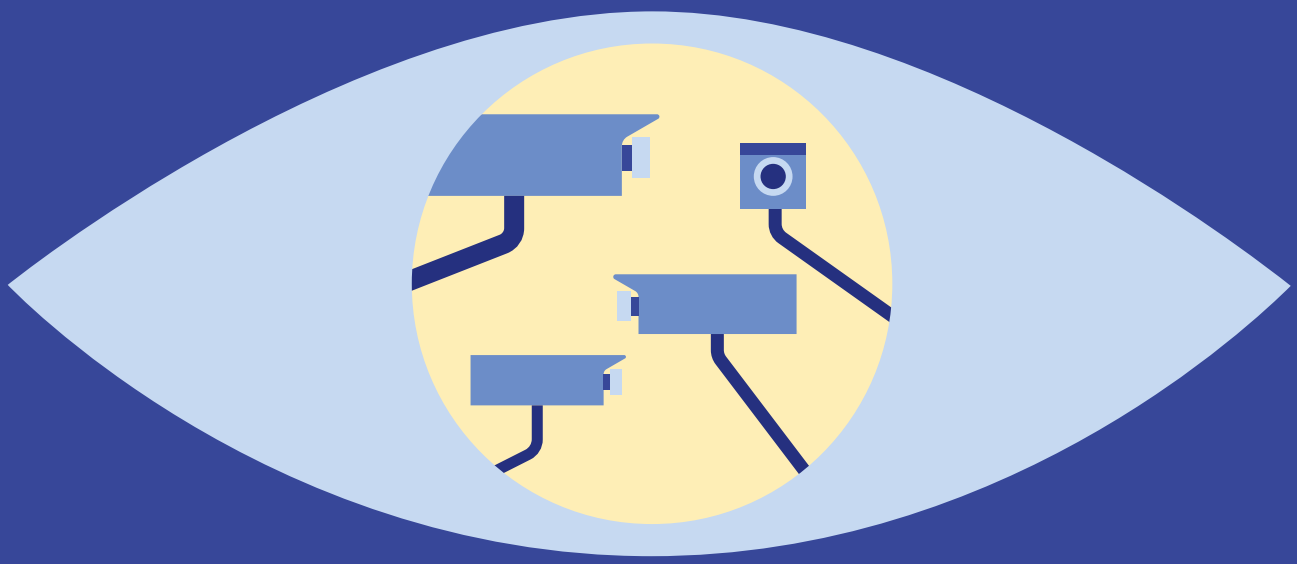
Die Datenschutzstelle ist von den Departementen unabhängig. Organisatorisch ist sie dem Gemeinderat zugeordnet. In der Aufgabenerfüllung ist die Datenschutzstelle weisungsfrei. Sie ist ausschliesslich dem Gesetz und der Verfassung verpflichtet.

Welche Aufgaben haben wir?

Bei der Stadtverwaltung Zürich arbeiten ca. 36 000 Angestellte in neun Departementen mit insgesamt über fünfzig Dienstabteilungen. Zur Stadtverwaltung im weiteren Sinne gehören zudem zahlreiche öffentliche-rechtliche Anstalten, Vereine, Stiftungen und weitere Organisationen mit Leistungsaufträgen der Stadt. So vielfältig die Aufgaben der Stadtverwaltung sind, eine Gemeinsamkeit besteht dennoch: Alle Mitarbeitenden arbeiten mit Informationen. Zahlreiche dieser Informationen betreffen die Bürger*innen, Patient*innen, Klient*innen und Mitarbeitenden in direkter oder indirekter Weise. Wann immer die Stadtverwaltung personenbezogene Informationen – Personendaten – bearbeitet, gilt es, den Datenschutz zu beachten.

Es gehört zu den Aufgaben der Datenschutzstelle, die Stadtverwaltung im Umgang mit Personendaten zu beraten, zu unterstützen, zu schulen und zu beaufsichtigen. Der Tätigkeitsbereich der Datenschutzstelle lässt sich konkret in folgende Aufgaben unterteilen:

- Kontrolle der Stadtverwaltung bei der Umsetzung und der Anwendung des Datenschutzes
- Beratung der Stadtverwaltung und der Bevölkerung in Datenschutzbelangen
- Beratung Betroffener über ihre Rechte im Datenschutz
- Konzeption und Durchführung von Weiterbildungen im Datenschutz
- Prüfung und Begleitung von IT-Projekten der Verwaltung
- Entgegennahme von meldepflichtigen Datenschutzvorfällen



8 Datenschutzrecht – Eine kurze Einführung

Obwohl der Datenschutz in den letzten Jahren ein fast schon omnipräsentes Thema in den Medien aber auch am Arbeitsplatz geworden ist, ist dennoch für viele Menschen schwierig zu verorten, worum es beim Datenschutzrecht eigentlich geht und wann es beachtet werden muss. Im Folgenden soll eine kurze Einführung aufzeigen, wann das Datenschutzrecht zur Anwendung kommt und was es beinhaltet:

Datenschutz ist ein Grundrecht

Datenschutz ist ein Grundrecht. Es ist sowohl in Art. 13 der Bundesverfassung als auch in Art. 8 der Europäischen Menschenrechtskonvention verankert. Schränkt der Staat ein Grundrecht ein, braucht er dafür immer eine gesetzliche Grundlage, ein öffentliches Interesse und die Beachtung der Verhältnismässigkeit.

Das Gesetz über die Information und den Datenschutz des Kantons Zürich (IDG) konkretisiert dieses Grundrecht und regelt den Umgang der öffentlichen Organe mit Informationen. Es hält unter anderem die allgemeinen Grundsätze fest, die beim Bearbeiten von Personendaten zu beachten sind.

Dazu zählen die folgenden Grundsätze:

Gesetzmässigkeit

Jede Tätigkeit der Verwaltung muss sich auf ein Gesetz abstützen können. Dies gilt auch für die Bearbeitung von Personendaten: Das Datenschutzrecht verlangt, dass die Verwaltung über eine genügende Berechtigung für die Datenbearbeitung verfügt. Ob und zu welchem Zweck die Stadtverwaltung Informationen über die Stadtbevölkerung bearbeiten darf, ergibt sich aus den gesetzlichen Grundlagen der jeweiligen Verwaltungsbereiche, also beispielsweise aus der Polizei-, Sozialhilfe-, Gesundheits- oder Schulgesetzgebung.

Zweckbindung

Die Verwaltung darf Personendaten nur zu dem Zweck bearbeiten, zu dem sie sie erheben durfte. Jede Verwendung von Personendaten zu anderen Zwecken muss wiederum durch eine rechtliche Bestimmung oder durch eine Einwilligung gerechtfertigt sein.

Verhältnismässigkeit

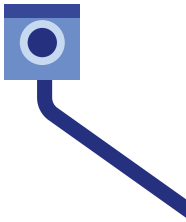
«Nicht mehr als notwendig»: Dieser allgemeine Grundsatz der Verhältnismässigkeit ist bei der Bearbeitung von Personendaten besonders zentral. Er gilt nicht nur in Bezug auf den Umfang der Daten (Datensparsamkeit), sondern ist beispielsweise auch für die Festlegung der Löschfristen und Zugriffsrechte massgebend.

Informationssicherheit

Die Verwaltung muss Personendaten vertraulich behandeln und sicherstellen, dass sie richtig und verfügbar sind. Sie hat die Informationen durch geeignete Technologien (wie Verschlüsselung) und organisatorische Massnahmen zu schützen. Welche Massnahmen konkret verlangt sind, ist abhängig von der Sensitivität der Daten, dem Verwendungszweck und dem Stand der Technik. Der Stadtrat hat für die Stadtverwaltung die technischen und organisatorischen Vorgaben im «Handbuch für Informationssicherheit der Stadt Zürich» definiert. Dieses Handbuch ist für alle städtischen Verwaltungsstellen verbindlich und bei allen Informationsbearbeitungen und ICT-Systemen zu beachten. Sämtliche Vorhaben und Projekte, die eine Bearbeitung von Informationen beinhalten, sind im Rahmen des ISDS-Prozesses (ISDS = Informationssicherheit/Datenschutz) der städtischen Fachstelle Informationssicherheit – und bei erhöhter Datenschutzrelevanz auch der Datenschutzstelle – zur Prüfung vorzulegen.

Transparenz

Datenbearbeitungen der Verwaltung dürfen keine «Blackboxes» sein. Sie müssen erkennbar, nachvollziehbar und verständlich sein. Das bedeutet, dass die Stadtverwaltung insbesondere über sensitive Datenbearbeitungen zielgruppengerecht informieren und allenfalls Organisationsvorschriften erlassen muss.



Personendaten als Anknüpfungspunkt

Das Datenschutzrecht kommt immer dann zur Anwendung, wenn die Stadtverwaltung Personendaten bearbeitet. Alle Informationen oder Angaben, die sich auf Personen beziehen oder sich Personen zuordnen lassen, stellen Personendaten dar. Dabei spielt es keine Rolle, in welcher Form diese Daten vorhanden sind (Wort, Bild, Ton) oder mit welcher Technik sie bearbeitet werden (analog oder digital). Die meisten Informationen, die in der Stadtverwaltung bearbeitet werden, sind Personendaten. Das Datenschutzrecht ist deshalb für die gesamte Stadtverwaltung relevant.

Datenschutzrecht – aber welches?

Datenschutzgesetze werden in der Schweiz vom Bund, den Kantonen und zum Teil auch von den Gemeinden erlassen. Für die Stadtverwaltung ist in erster Linie das Datenschutzrecht des Kantons Zürich massgebend, konkret das Gesetz über die Information und den Datenschutz (IDG) und die dazugehörende Verordnung (IDV). Die Stadt Zürich kennt zusätzlich eine eigene Datenschutzverordnung (DSV). Diese Verordnung ist vor allem für die Videoüberwachung durch städtische Verwaltungsstellen und den Datenbezug aus dem städtischen Einwohnerregister massgebend.

Stadt Zürich
Datenschutzstelle
Beckenhofstrasse 59
8006 Zürich
T +41 44 412 16 00
datenschutz@zuerich.ch
stadt-zuerich.ch/das

PDF 04.2026