Stadt Zürich
Datenschutzstelle

2021–2022

Gemäss § 39 des kantonalen Gesetzes über die Information und den Datenschutz (IDG; LS 170.4) berichtet die oder der Datenschutzbeauftragte dem Wahlorgan periodisch über Umfang und Schwerpunkte der Tätigkeiten, über wichtige Feststellungen und Beurteilungen sowie über die Wirkung des Gesetzes. Der Bericht wird veröffentlicht.

Der vorliegende Bericht bezieht sich auf die zwei **Kalenderjahre 2021 und 2022.**

Veröffentlicht werden die Berichte auf der **Webseite** der Datenschutzstelle der Stadt Zürich.

Zürich, Juni 2023
Marcel Studer, Datenschutzbeauftragter

Inhaltsverzeichnis

Resümee 7

Die Berichtsjahre 2021 und 2022 in Kürze 8

Grundlagen 11

Die Datenschutzstelle der Stadt Zürich kurz vorgestellt 12

Das Datenschutzrecht kurz erklärt 15

Schwerpunkte und Feststellungen 19

Videoüberwachung 20

Gesichtserkennung 23

Rechtsetzung und Stellungnahmen 26

Meldung von Datenschutzvorfällen 30

Digitale Verwaltung 33
– «Once only» 35
– Cloud-Computing 38
– Digitale Partizipation 42

Whistleblowing 44

Schulfotografie 47

Resümee

Die Berichtsjahre 2021 und 2022 in Kürze

Beinahe jedes staatliche Handeln weist heute eine (mehr oder weniger grosse) Datenschutzrelevanz auf. Die Themen, mit welchen sich die Datenschutzstelle beschäftigt, sind daher auch so vielfältig wie die Aufgaben und Tätigkeiten der Stadtverwaltung und ebenso wie diese bestimmt durch gesellschaftliche, politische oder technologische Entwicklungen. Dabei gibt es **Themen und Fragestellungen,** die eine Vielzahl städtischer Verwaltungsstellen betreffen und oft über einen längeren Zeitraum konstante Aktualität aufweisen – wie beispielsweise Videoüberwachung, Digitalisierung oder Cloud-Computing. Es gibt aber immer auch Themen, die nur einzelne Verwaltungsbereiche betreffen und nicht permanent auf der datenschutzrechtlichen Agenda stehen – wie beispielsweise Bodycam, Smartmeter oder Schulfotografie. Einige der Themen aus den Berichtsjahren werden unter Schwerpunkte und Feststellungen näher ausgeführt.

Werden die Tätigkeiten der Datenschutzstelle nicht thematisch oder inhaltlich, sondern nach **Kategorien** betrachtet, kann festgestellt werden, dass sie sich in den Berichtsjahren im Vergleich zu den Vorjahren verändert haben. Der wichtigste Grund dafür ist in der **Revision des kantonalen Informations- und Datenschutzgesetzes (IDG) aus dem Jahr 2020** zu sehen:

– Diese Revision führte die sogenannte **Datenschutz-Folgenabschätzungen** ein. Verwaltungsstellen haben demnach die Risiken, die mit beabsichtigten Datenbearbeitungen einhergehen können, zu bewerten und zu dokumentieren. Um dies zu gewährleisten, müssen die zuständigen Verwaltungsstellen und insbesondere auch deren Rechtsdienste und Projektleiter*innen über das erforderliche Knowhow verfügen. Die Datenschutzstelle investierte deshalb in den Berichtsjahren viel in die Anpassung des städtischen Informations- und Datenschutz-Prozesses (vgl. hierzu **Seite 12**) und in diesbezügliche Workshops und Weiterbildungen.

– Zeigt eine Datenschutz-Folgenabschätzung, dass ein Projekt oder Vorhaben eine erhöhte datenschutzrechtliche Sensitivität aufweist, muss dieses der Datenschutzstelle zur **Vorabkontrolle** (vgl. hierzu **Seite 12**) angemeldet werden. Diese Prüfungspflicht ist an sich nichts Neues. Seit der erwähnten IDG-Revision ist jedoch für die zuständigen Verwaltungsstellen besser erkennbar, welche Projekte oder Vorhaben der Vorabkontrolle unterliegen, was zu einer Reduktion der Anmeldungen bei der Datenschutzstelle führte.

– Eine weitere Neuheit, die mit der erwähnten IDG-Revision eingeführt wurde, ist die sogenannte **Meldepflicht von Datenschutzvorfällen.** Auch hierzu galt es erst einmal, das erforderliche Knowhow zu erarbeiten und in die Verwaltungsstellen zu kommunizieren. Weitere Ausführungen zur neuen Meldepflicht erfolgen auf **Seite 30** ff.

Bedeutsam für die Tätigkeiten der Datenschutzstelle in den beiden Berichtsjahren waren auch zwei Neuerlasse auf städtischer Ebene. Bereits seit längerem beinhaltet die Datenschutzverordnung der Stadt Zürich die Vorschrift, wonach **datenschutzrelevante Anträge an den Stadtrat** der Datenschutzstelle zur Stellungnahme zu unterbreiten sind. Mit zwei neuen stadträtlichen Reglementen wird nun sichergestellt, dass diese Vorschrift in den städtischen Verfahren konsequent berücksichtigt wird. Die Wirkung dieser Reglemente hat sich bereits in den beiden Berichtsjahren klar bestätigt. Nähere Ausführungen dazu erfolgen auf **Seite 26** ff.

Keine nennenswerten Veränderungen im Vergleich zu den Vorjahren sind bei **Anfragen von Verwaltungsstellen, städtischen Mitarbeitenden oder Privatpersonen** zu verzeichnen. Seit Jahren besteht eine grosse Nachfrage für Auskünfte, Beratungen oder Expertisen und regelmässig führen Hinweise oder Beanstandungen zu entsprechenden Untersuchungen durch die Datenschutzstelle.

Grundlagen

Die Datenschutzstelle der Stadt Zürich kurz vorgestellt

Unabhängige Fachstelle

Die Datenschutzstelle der Stadt Zürich ist eine unabhängige und weisungsfreie Fachstelle, die organisatorisch dem Gemeinderat zugeordnet ist. Sie verfügt über drei Vollzeitstellen.

Aufgaben

Ihre wichtigsten Aufgaben bestehen darin, die Stadtverwaltung im Umgang mit Personendaten zu beraten, zu unterstützen und zu kontrollieren.

– **Projekte und Vorhaben prüfen und beraten**
  In der Stadtverwaltung Zürich müssen sämtliche Projekte oder Vorhaben mit Informationsbearbeitungen den sogenannten Informationssicherheits- und Datenschutz-Prozess (ISDS-Prozess) durchlaufen. Bei denjenigen Vorhaben, die aus datenschutzrechtlicher Sicht eine erhöhte Sensitivität aufweisen, führt die Datenschutzstelle eine sogenannte Vorabkontrolle durch. Dabei wird geprüft, ob die Rahmenbedingungen – in rechtlicher, technischer und organisatorischer Hinsicht – eingehalten werden. Bei weniger sensitiven Projekten steht nicht die Prüfung im Vordergrund, sondern vielmehr die Beratung durch die Datenschutzstelle.

– **Anfragen und Gesuche behandeln**
  Regelmässig wird die Datenschutzstelle von Rechtsdiensten, Fach- und Führungskräften oder weiteren Mitarbeitenden der Stadtverwaltung gebeten, bestehende oder erst geplante Informationsbearbeitungen der Stadtverwaltung aus datenschutzrechtlicher Optik zu prüfen und zu beurteilen. Auch Privatpersonen wenden sich oft mit Fragen oder Reklamationen zu Datenbearbeitungen der Stadtverwaltung an die Datenschutzstelle. Solche «Anstösse von aussen» führen nicht selten zu umfangreichen Abklärungen und können Fehler oder Defizite bei Datenbearbeitungen in der Stadtverwaltung aufzeigen und zu entsprechenden Korrekturen führen.

– **Bei Gesetzgebungsverfahren mitwirken**
  Werden rechtliche Grundlagen der Stadtverwaltung mit Datenschutzrelevanz neu geschaffen oder angepasst, ist die Datenschutzstelle regelmässig bereits in die entsprechenden Gesetzgebungsprojekte involviert.

Zusammenarbeit und Vernetzung

Das Handeln der Datenschutzstelle richtet sich nach dem Ziel, Datenschutz in der Stadtverwaltung wirkungsvoll umzusetzen. Datenschutz lässt sich aber nicht schematisch und abstrakt realisieren, sondern kann nur konkret und in Kenntnis der jeweiligen Verhältnisse und Bedürfnisse umgesetzt werden. Um einen möglichst sachgerechten Umgang mit Daten zu erreichen, bedarf es organisationsübergreifender und interdisziplinärer Zusammenarbeit, insbesondere mit:

– **den Projektverantwortlichen und Rechtsdiensten aus den Departementen und Dienstabteilungen**
  Den korrekten und «passenden» Datenschutz erreicht man nur, wenn die konkreten Anforderungen und Gegebenheiten der jeweiligen Projekte und Verwaltungsbereiche verstanden und berücksichtigt werden. Der direkte Austausch mit den Verantwortlichen der Fach- und Rechtsabteilungen ist deshalb äusserst wichtig.

– **der Fachstelle für Informationssicherheit**
  Diese Fachstelle der städtischen Dienstabteilung Organisation und Informatik (OIZ) prüft alle ICT-Projekte auf die Einhaltung der Vorschriften zur Informationssicherheit. Diese Prüfung erfolgt im Rahmen des erwähnten städtischen ISDS-Prozesses und in enger Koordination mit der Datenschutzstelle.

– **den Beraterinnen und Beratern für Datenschutz der Departemente**
  Alle städtischen Departemente verfügen über eine Beraterin oder einen Berater für Datenschutz. Diese erfahrenen Juristinnen und Juristen aus den Rechtsdiensten der Departementssekretariate beraten ihre Dienstabteilungen und sind für die Datenschutzstelle wichtige Ansprechpersonen.

– **Privatim (Konferenz der Schweizerischen Datenschutzbeauftragten)**
  Die Datenschutzstelle ist in allen Fachgremien von Privatim vertreten.

In Zusammenarbeit mit involvierten Verantwortlichen und Fachleuten will die Datenschutzstelle mit dienstleistungs- und lösungsorientiertem Handeln erreichen, dass die Stadtverwaltung den Schutz der Grundrechte von Personen, über welche Daten bearbeitet werden, gewährleisten kann.

Das Datenschutzrecht kurz erklärt

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.

Das massgebende Datenschutzrecht

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 dazu eine eigene Datenschutzverordnung (DSV). Diese Verordnung ist vor allem für die Videoüberwachung durch städtische Verwaltungsstellen und den Datenbezug aus dem städtischen Einwohnerregister massgebend.

Die Anforderungen des Datenschutzrechts

Datenschutz ist ein Grundrecht. Die Verfassungen von Bund und Kanton verpflichten die Stadtverwaltung, bei der Bearbeitung von Personendaten Privatsphäre und Persönlichkeit der Bürger*innen zu achten und zu schützen. Das IDG konkretisiert dieses Grundrecht, indem es für den Umgang mit Informationen und Personendaten Grundsätze und Prinzipien aufstellt, die rechtlicher, technischer und organisatorischer Natur sein können:

– **Gesetzmässigkeit und Zweckbindung**
  Jede Tätigkeit der Verwaltung muss sich auf eine gesetzliche Grundlage abstützen können. Dies gilt auch für die Bearbeitung von Personendaten. Das Datenschutzrecht verlangt, dass die Verwaltung über eine genügende Legitimation (gesetzliche Grundlage, Einwilligung) für ihre Datenbearbeitungen verfügt und die Daten nur zum gesetzlich bestimmten Zweck verwendet. Ob und zu welchem Zweck die Stadtverwaltung Personendaten bearbeiten darf, ergibt sich aus den Rechtsgrundlagen der jeweiligen Verwaltungsbereiche, also beispielsweise aus der Polizei-, Sozialhilfe-, Gesundheits- oder Schulgesetzgebung.

– **Verhältnismässigkeit**
  «So viel wie nötig, so wenig wie möglich». Dieser Grundsatz der Verhältnismässigkeit ist bei der Bearbeitung von Personendaten von besonderer Tragweite. Er gilt nicht nur in Bezug auf den Umfang der Daten, sondern ist auch für die Festlegung von Löschfristen oder Zugriffsrechten massgebend.

– **Informationssicherheit**
  Personendaten sind in der Regel vertraulich und müssen richtig und verfügbar sein. Durch technische und organisatorische Massnahmen (TOM) wie beispielsweise Verschlüsselung oder Zugriffskonzepte müssen Informationen geschützt werden. Welche Massnahmen konkret umgesetzt werden müssen, ist stets kontextabhängig, insbesondere nach Massgabe der Sensitivität der Daten, des Verwendungszwecks und des Stands der Technik.

– **Transparenz**
  Datenbearbeitungen der Verwaltung dürfen keine «Black-boxes» sein. Sie müssen erkennbar, nachvollziehbar und verständlich sein. Das bedeutet, dass die Stadtverwaltung insbesondere über sensitive Datenbearbeitungen adressatengerecht informieren und allenfalls Organisationsvorschriften erlassen muss.

Schwerpunkte und Feststellungen

Videoüberwachung

Das Thema Videoüberwachung stellt seit Jahren für die Datenschutzstelle ein eigentliches Schwerpunktthema dar. Da sich die rechtlichen Voraussetzungen und die Zuständigkeiten für Aufsicht und Beratung danach richten, wer eine Videoüberwachung betreibt, ist die Videoüberwachung durch die Stadtverwaltung von derjenigen durch Privatpersonen zu unterscheiden.

Videoüberwachung durch die Stadtverwaltung

Die Stadt Zürich hat für Videoüberwachung der städtischen Verwaltungsstellen eigene gesetzliche Regelungen in der städtischen Datenschutzverordnung erlassen. Diese Verordnung sieht vor, dass die Stadtverwaltung bei erheblichen Gefahrensituationen Videoüberwachung einsetzen darf. Erfolgt eine Videoüberwachung mit Aufzeichnungen, muss die verantwortliche Dienstabteilung ein Videoreglement erlassen und dieses der Datenschutzstelle zur Prüfung vorlegen. Betrifft die Videoüberwachung der städtischen Verwaltungsstelle öffentlichen oder allgemein zugänglichen Raum, ist das Videoreglement amtlich zu publizieren und in die Amtliche Rechtssammlung der Stadt Zürich aufzunehmen.

In den Berichtsjahren hatten 13 Dienstabteilungen Videoüberwachung gestützt auf die städtische Datenschutzverordnung im Einsatz.

Videoüberwachung durch Private

Für Videoüberwachung durch Private sind die privatrechtlichen Bestimmungen des Bundesgesetzes über den Datenschutz massgebend. Für Beratung und Aufsicht bei Videoüberwachung durch Private ist damit grundsätzlich der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) zuständig. In Ergänzung zu dieser Bundeszuständigkeit bietet auch die Stadt Zürich bei Videoüberwachung durch Private ein Beratungsangebot an. Seit November 2020 können sich Privatpersonen bei Fragen oder Anliegen zur Videoüberwachung auch an die städtische Datenschutzstelle wenden. Voraussetzung ist, dass die fragliche Videoüberwachung öffentlichen Grund der Stadt Zürich tangiert. Die städtische Datenschutzverordnung wurde hierfür um eine entsprechende Beratungs- und Vermittlungskompetenz der Datenschutzstelle erweitert.

In den Berichtsjahren gingen je ca. 15–20 Anfragen bei der Datenschutzstelle ein, die Videoüberwachung durch Private betrafen. Je nachdem, ob die anfragenden Personen selber eine Videoüberwachung betreiben wollten oder von einer fremden Videoüberwachung betroffen waren, wünschten sie insbesondere Antworten auf folgende Fragen: Unter welchen Voraussetzungen dürfen Videokameras überhaupt eingesetzt werden? Muss eine Videoüberwachung bewilligt werden? Wie muss auf sie vor Ort hingewiesen werden? Wie kann man sich gegen eine Videoüberwachung zur Wehr setzen? An welche Behörde muss man sich hierfür wenden? Die Datenschutzstelle beantwortet diese und ähnliche Fragen im Rahmen ihrer neuen Beratungsaufgabe den anfragenden Personen telefonisch oder per E-Mail und stellt die wichtigsten Informationen rund um Videoüberwachung durch Private auch auf ihrer **Webseite** zur Verfügung.

Bei einer Anfrage beschränkte sich die Datenschutzstelle nicht nur auf eine Beratung, sondern führte eine eigentliche Vermittlung zwischen den involvierten Personen durch. Die fragliche Videoüberwachung betraf einen grösseren Strassenraum, so dass eine Besichtigung vor Ort durchgeführt wurde. Die Beratung und Vermittlung der Datenschutzstelle führte dazu, dass die Videoüberwachung örtlich eingeschränkt und mit einer Beschilderung versehen wurde. Ausserdem erstellte die Betreiberin ein internes Reglement, welches die Modalitäten wie insbesondere die Löschung der Aufnahmen festlegt.

Revision der städtischen Videobestimmungen

Im Laufe der letzten Jahre wurden zum Thema Videoüberwachung in der Stadt Zürich mehrere parlamentarische Vorstösse eingereicht und auch der Stadtrat und die Datenschutzstelle haben wiederholt darauf hingewiesen, dass für die städtischen Regelungen zur Videoüberwachung in diversen Belangen Anpassungsbedarf besteht. Der Stadtrat beschloss deshalb, die Datenschutzverordnung hinsichtlich der Videobestimmungen umfassend zu überarbeiten. In diese Gesetzgebungsarbeiten war die Datenschutzstelle während beider Berichtsjahre massgeblich involviert. Mit Weisung vom 07.12.2022 beantragte der Stadtrat dem Gemeinderat eine entsprechende Revision der Datenschutzverordnung (**GR Nr. 2022/629**). Die Empfehlungen und Vorschläge der Datenschutzstelle sind umfassend und sachgerecht in der Vorlage des Stadtrats berücksichtigt worden.

Gesichtserkennung

Mit Videoüberwachung zunehmend eng verbunden ist die Technologie der Gesichtserkennung. Mit derartigen Technologien werden typischerweise biometrische Daten von Gesichtsbildern bearbeitet, um Personen durch Abgleich mit anderen Datenbanken zu identifizieren (eindeutige Feststellung der Identität) oder zu authentifizieren (Überprüfung bestimmter Eigenschaften beispielsweise zwecks Zutrittskontrolle). Technologien für Identifikation oder Authentifikation können auch auf der Bearbeitung anderer biometrischer Daten basieren, wie Fingerabdruck, Iris, Stimme oder Gangart.

Datenschutzrechtliche Anforderungen

Personendaten, die mit derartigen Erkennungstechnologien erhoben werden, sind gemäss dem Informations- und Datenschutzgesetz des Kantons Zürich (IDG) als äusserst sensitiv zu qualifizieren. Die Stadtverwaltung darf deshalb derartige Technologien oder Systeme erst dann einsetzen, wenn sie hierzu durch formell-gesetzliche Grundlagen – das heisst durch Gesetze, die von Parlamenten auf Bundes-, Kantons- oder Stadtebene erlassen wurden – legitimiert wird. An diese Gesetze werden in inhaltlicher Hinsicht hohe Anforderungen gestellt: Der Gesetzgeber muss den Einsatz solcher Technologien und die damit verbundenen Bearbeitungen von Personendaten klar und präzise bestimmen. Was dies konkret bedeutet, kann beispielsweise aus der Rechtsprechung des Bundesgerichts zur automatisierten Fahrzeug- und Verkehrskontrolle hergeleitet werden. Damit die Polizei Fahrzeug-Kontrollschilder automatisiert erfassen und mit polizeilichen Datenbanken abgleichen darf, verlangt das Bundesgericht Rechtsgrundlagen, die den Zweck der Überwachung, deren Voraussetzungen und Beschränkungen sowie den Umgang mit den Daten präzise und verständlich umschreiben. Wenn das Bundesgericht bereits den Einsatz automatisierter Überwachungstechnologien im Strassenverkehr als schweren Grundrechtseingriff qualifiziert und gestützt darauf hohe Anforderungen an die Rechtsgrundlagen stellt, muss dies erst recht für den Einsatz von Technologien wie Gesichtserkennung im öffentlichen Raum gelten.

Politische Vorstösse für Verbote

Werden biometrische Erkennungstechnologien im öffentlichen Raum eingesetzt, kann dies zu eigentlichen Massenüberwachungen führen. Um damit verbundenem Missbrauchspotential und ungerechtfertigter Einschränkung von Grundrechten entgegenzuwirken, hat das Europaparlament einer Resolution zugestimmt, die ein Verbot der Verarbeitung biometrischer Daten verlangt, wenn diese Verarbeitung zu einer Massenüberwachung in öffentlich zugänglichen Räumen führt. Auch in der Schweiz verlangen politische Vorstösse und diverse zivilgesellschaftliche Organisationen ein Verbot von automatisierter Gesichtserkennung und biometrischer Massenüberwachung. Auf Bundesebene hat der Bundesrat einen Bedarf für diesbezügliche Verbotsregelungen verneint (Interpellation 21.3580). Dies vor allem unter Hinweis darauf, dass Behörden des Bundes und der Kantone die Gesichtserkennung zur Identifizierung im öffentlichen Raum nur dann einsetzen dürfen, wenn eine ausreichende Rechtsgrundlage dafür besteht. Der Gemeinderat der Stadt Zürich überwies im Sommer 2022 eine Motion (GR Nr. 2021/450) mit dem Auftrag, den Einsatz biometrischer Erkennungssysteme zum Zweck der Überwachung und die Speicherung biometrischer Daten zu verbieten. Im Rahmen der vorstehend erwähnten Revision der städtischen Videobestimmungen schlägt der Stadtrat eine entsprechende Umsetzung dieser Motion vor.

Aus verfassungs- und datenschutzrechtlicher Sicht sind die Voraussetzungen für einen Einsatz derartiger Technologien und Systeme klar: Verlangt werden legitimierende und genügend präzise Grundlagen auf formell-gesetzlicher Ebene. Ob zusätzlich dazu Verbotsbestimmungen angezeigt und von Nutzen sein können, ist weniger eine (datenschutz-)rechtliche als vielmehr eine politische Frage, die von den jeweiligen Gesetzgebern zu beantworten sein wird.

Der Fall Clearview

Im September 2021 berichteten verschiedene Medien, die Stadtpolizei Zürich habe mutmasslich eine in der Schweiz nicht zulässige Gesichtserkennungssoftware der US-Firma Clearview eingesetzt. Gestützt darauf verlangte die Datenschutzstelle eine entsprechende Untersuchung. Das Sicherheitsdepartement bestätigte der Datenschutzstelle, dass die Stadtpolizei Gesichtserkennungstechnologie weder einsetzt noch evaluiert und – sollte ein derartiger Einsatz je zur Diskussion stehen – die rechtlichen Anforderungen vorgängig detailliert geprüft werden.

Rechtsetzung und Stellungnahmen

Mitwirkung im Gesetzgebungsprozess

Das Datenschutzrecht beinhaltet Voraussetzungen und Prinzipien für den Umgang der Verwaltung mit Personendaten. Grundlegend ist dabei die Forderung, wonach sich Datenbearbeitungen im behördlichen Kontext auf genügende rechtliche Grundlagen abzustützen haben. Zur Sicherstellung dieses Gesetzmässigkeitsprinzips ist es wichtig, den Fokus nicht nur auf bereits bestehende rechtliche Grundlagen zu richten, sondern ebenso dafür zu sorgen, dass Rechtsgrundlagen bei Revision oder Neuerlass die verlangten datenschutzrechtlichen Anforderungen erfüllen. Aus diesem Grund sehen sowohl das kantonale als auch das städtische Datenschutzrecht folgerichtig vor, dass die oder der Datenschutzbeauftragte Erlasse, die den Datenschutz betreffen, beurteilt und dass alle Anträge an den Stadtrat, die Belange des Datenschutzes betreffen, ihr oder ihm zur Stellungnahme zu unterbreiten sind. Um aber tatsächlich einen genügenden Datenschutz in die rechtlichen Grundlagen der jeweiligen Verwaltungsstellen zu bringen, genügt es oft nicht, erst am Schluss des Rechtsetzungsprozesses eine Beurteilung oder Stellungnahme der Datenschutzstelle abzuholen. Stehen sensitive Datenbearbeitungen zur Diskussion, ist es unerlässlich, den Datenschutz von Beginn an und in Kenntnis der jeweiligen Gegebenheiten und Anforderungen umfassend «mitzudenken». Nur so ist in den zu schaffenden Bestimmungen eine sachgerechte Abbildung des Datenschutzes überhaupt möglich. Dabei geht es in erster Linie um die Umsetzung der gesetzlichen Forderung, wonach die Rechtsgrundlagen den Umgang mit «heiklen» Personendaten genügend bestimmt zu regeln haben. Diese Forderung nach klaren und präzisen Bestimmungen, die gewährleisten sollen, dass das Verwaltungshandeln verständlich und nachvollziehbar ist, stellt regelmässig eine grosse Herausforderung dar. In der Stadt Zürich wird deshalb die Datenschutzstelle in der Regel nicht nur rechtzeitig über Rechtsetzungsvorhaben mit datenschutzrechtlicher Relevanz informiert, sondern wenn möglich auch frühzeitig in diese involviert.

Reglement über die Geschäftserledigung des Stadtrats (RGE)

Im Rahmen der Revision der Geschäftsordnung des Stadtrats hat die Stadt Zürich ein neues Reglement über die Geschäftserledigung des Stadtrats (RGE) erlassen. Dieses Reglement regelt die Grundzüge der Geschäftsorganisation und -erledigung des Stadtrats. Es setzt die eingangs erwähnte Forderung des Datenschutzrechts erstmals in städtisches Verfahrensrecht um und verlangt, dass die zuständigen Departemente ihre Erlassentwürfe mit einer Frist von mindestens 20 Tagen der Datenschutzstelle zur Stellungnahme zu unterbreiten haben. Unter Erlass gemäss RGE sind sämtliche Rechtsetzungsvorhaben der Stadtverwaltung zu verstehen. Von Interesse für die Datenschutzstelle sind solche Stadtratsgeschäfte, wenn sie die Bearbeitung von Personendaten – insbesondere deren Erhebung/Bezug, Verwendung/Verarbeitung oder Bekanntgabe/Weitergabe – direkt zum Gegenstand haben oder wenn eine derartige Bearbeitung von Personendaten mit der Verwaltungstätigkeit, für die eine Rechtsgrundlage geschaffen wird, verbunden ist.

In den beiden Berichtsjahren war die Datenschutzstelle in rund 30 städtische Gesetzgebungsverfahren involviert. Die wichtigsten betrafen

- Neuerlass eines Reglements über offene Verwaltungsdaten (OGD)
- Revision der städtischen Videobestimmungen (DSV)
- Neuerlass einer Richtlinie betreffend Nutzung von Cloud-Services
- Ausführungsbestimmungen zur Bodycam-Verordnung
- (mehrere) Stipendienvorlagen
- Wasserabgabevorlagen (Einführung von elektronischen Wasserzählern)

Revision des kantonalen IDG

Das aufwendigste Gesetzgebungsverfahren der beiden Berichtsjahre, bei welchem die Datenschutzstelle mitwirkte, war kein städtisches, sondern ein kantonales: Der Regierungsrat des Kantons Zürich erteilte 2020 den Auftrag, das kantonale Informations- und Datenschutzgesetz (IDG) einer Totalrevision zu unterziehen. Der Datenschutzbeauftragte der Stadt Zürich ist seit Beginn an Mitglied der entsprechenden Arbeitsgruppe. Es ist vorgesehen, dass der Regierungsrat die diesbezügliche Vorlage im Verlaufe des Kalenderjahrs 2023 an den Kantonsrat überweisen wird.

Neubeurteilungsreglement (NBR)

Zusätzlich zum RGE hat der Stadtrat das Neubeurteilungsreglement (NBR) erlassen. Dieses Reglement regelt das stadtinterne Verfahren bei Anfechtung von Anordnungen (Verfügungen) der Dienstabteilungen oder Departemente. Das Datenschutzrecht sieht für Personen, deren Daten durch die Stadtverwaltung bearbeitet werden, verschiedene Rechtsansprüche vor – so insbesondere das Recht, Auskunft über die eigenen Personendaten zu erhalten oder das Recht, unrichtige Personendaten berichtigen oder vernichten zu lassen. Entsprechen städtische Verwaltungsstellen nicht oder nur teilweise diesbezüglichen Gesuchen, müssen im Rahmen des städtischen Neubeurteilungsverfahrens die entsprechenden Anordnungen und Verfahrensakten auch der Datenschutzstelle zum Mitbericht vorgelegt werden. Mit dieser Involvierung der Datenschutzstelle in das städtische Neubeurteilungsverfahren geht die Stadt Zürich weiter als vom kantonalen IDG verlangt. Letzteres sieht nur eine Prüfung von Erlassen, nicht aber von Anordnungen und Verfügungen, vor. Mit der städtischen Datenschutzverordnung und dem NBR verstärkt die Stadt den Rechtsschutz betroffener Personen in Datenschutzangelegenheit erheblich.

In den beiden Berichtsjahren war die Datenschutzstelle in rund 10 Neubeurteilungsverfahren involviert. Nach Prüfung der Verfahrensakten bestand in keinem dieser Verfahren Anlass, den vorgesehenen Neubeurteilungsentscheid aus datenschutzrechtlicher Sicht zu kritisieren bzw. zuhanden des Stadtrats eine davon abweichende Beurteilung abzugeben. Wichtig in diesem Zusammenhang ist der Hinweis auf die sogenannte Kognitionsbefugnis der Datenschutzstelle in derartigen Verfahren: Für die Beurteilung von datenschutzrechtlichen Ansprüchen wie beispielsweise von Auskunftsrechten sind regelmässig die im konkreten Fall relevanten (privaten und/oder öffentlichen) Interessen zu ermitteln und gegeneinander abzuwägen. Hierfür müssen die zuständigen Verwaltungsstellen über einen gewissen Ermessensspielraum verfügen. Übt eine verfügende Verwaltungsstelle ihr Ermessen im rechtskonformen Rahmen aus, steht der Datenschutzstelle (richtigerweise) keine Befugnis zu, in der Sache selber einen anderen Entscheid zu verlangen. Der Datenschutzstelle steht somit keine Billigkeitskontrolle zu. Ihre Kompetenz beschränkt sich auf die Prüfung der Rechtswidrigkeit.

Meldung von Datenschutzvorfällen

Gesetzliche Melde- und Informationspflicht

Das kantonale Informations- und Datenschutzgesetz (IDG) verpflichtet Behörden und Verwaltungsstellen, bei bestimmten Datenschutzvorfällen eine Meldung an die Datenschutzstelle zu erstatten und betroffene Personen zu informieren. Unter Datenschutzvorfällen sind Ereignisse oder Sachverhalte zu verstehen, bei denen die Datensicherheit verletzt wurde oder Personendaten unbefugt bearbeitet wurden. Meldepflichtig sind solche Vorfälle immer dann, wenn Grundrechte betroffener Personen gefährdet sind. Verlangt wird somit, dass die Konsequenzen eines Vorfalls eine gewisse Schwere oder Intensität aufweisen. Die Meldepflicht gegenüber der Datenschutzstelle stellt ein aufsichtsrechtliches Rechenschaftsinstrument dar. Demgegenüber ist das primäre Ziel der Informationspflicht in der (raschen) Schadensbegrenzung durch die jeweils Betroffenen zu sehen.

Datenschutzvorfälle

In den beiden Berichtsjahren hat die Stadtverwaltung der Datenschutzstelle rund ein Dutzend Datenschutzvorfälle gemeldet. Die Hälfte der Meldungen betraf bloss geringfügige Vorfälle wie beispielsweise das Zustellen einzelner Dokumente an falsche Empfänger*innen oder die Versendung von E-Mails mit Erkennbarkeit aller Adressen der jeweiligen Verteilerliste. Derartige Bagatellfälle müssen der Datenschutzstelle grundsätzlich nicht gemeldet werden. Die übrigen Meldungen erfolgten zu Recht und betrafen Sachverhalte wie

- unberechtigte Bekanntgabe von vertraulichen Informationen an Verfahrensbeteiligte
- nicht korrekter Entzug von Zugriffsrechten, so dass ehemalige Mitarbeitende weiterhin Zugriff auf vertrauliche Informationen erhielten
- nicht korrekte Vergabe von Zugriffsrechten auf elektronischer Dokumentenablage, so dass Unberechtigte Zugriff erhielten
- Aufnahme und Veröffentlichung von Bildern von Klienten durch Mitarbeitende

Werden derartige Vorfälle der Datenschutzstelle gemeldet, ist jeweils unverzüglich und prioritär zu prüfen, welche Sofortmassnahmen zur Verhinderung oder Begrenzung (weiteren) Schadens bereits ergriffen wurden und noch zu ergreifen sind. Regelmässig steht zum Zeitpunkt der Meldungen noch zu wenig klar fest, was genau passiert ist, so dass die zuständigen Verwaltungsstellen – zum Teil auch auf Veranlassung der Datenschutzstelle – den relevanten Sachverhalt detaillierter abklären müssen. Steht dieser fest, gilt es nicht nur, eine adäquate Lösung für den konkreten Einzelfall zu finden, sondern vor allem auch zu prüfen, ob weitere Massnahmen zur Optimierung bestehender Prozesse und damit zur Verhinderung derartiger Vorfälle zu ergreifen sind.

Erste Erfahrungen

Die Meldepflicht von Datenschutzvorfällen ist eine neue Forderung aus dem kantonalen Datenschutzrecht, die erst seit Juni 2020 besteht. Die Datenschutzstelle hat in ihrem Tätigkeitsbericht 2020 über diese Meldepflicht und die diesbezüglichen Umsetzungsmassnahmen berichtet. Sowohl die eingegangenen Meldungen als auch die diesbezüglichen Anfragen bei der Datenschutzstelle zeigen, dass es für die Verwaltung schwierig zu erkennen ist, welche Vorfälle meldepflichtig sind und welche als Bagatellfälle zu bewerten sind, für die keine Meldung erforderlich ist. Unsicherheit besteht aber nicht nur in Bezug darauf, ob ein bestimmter Vorfall gemeldet werden muss, sondern auch hinsichtlich der Frage, für welche weiteren Handlungen oder Massnahmen die jeweiligen Verwaltungsstellen nach erfolgter Meldung zuständig und verantwortlich sind (bzw. bleiben) und wie mit dem Informationsanspruch (potentiell) Betroffener umzugehen ist.

Diese Unsicherheit erstaunt angesichts der gesetzlich wenig präzis formulierten Meldepflicht nicht. Umso wichtiger ist es, die Erkenntnisse, die sich aus den einzelnen Vorfällen ergeben, laufend für die Konkretisierung und Schärfung der Meldepflicht zu nutzen. Die Datenschutzstelle informiert diesbezüglich die Stadtverwaltung regelmässig, insbesondere durch Mitteilung an die Datenschutzverantwortlichen und Rechtsdienste der Departemente und Dienstabteilungen sowie durch Fortführung ihres diesbezüglichen Merkblatts. Im Rahmen der laufenden Revision des kantonalen IDG hat sie beantragt, den Wortlaut der Meldepflicht (§ 12a IDG) entsprechend anzupassen.

Da mittlerweile die meisten kantonalen Datenschutzgesetze eine derartige Meldepflicht von Datenschutzvorfällen kennen, beschäftigt sich auch eine Arbeitsgruppe der Konferenz der Schweizerischen Datenschutzbeauftragten (Privatim) mit diesem Thema. Die Datenschutzstelle der Stadt Zürich ist Mitglied dieser Arbeitsgruppe.

Digitale Verwaltung

Mit zahlreichen Strategien und Projekten wird auf allen Staatsebenen der Forderung nach Digitalisierung der Verwaltung Nachdruck verliehen. Begriffe wie Prozessoptimierung oder Effizienzsteigerung sollen dabei zum Ausdruck bringen, was von der digitalen Verwaltung erwartet wird. An dieser Stelle wird – wie dies bereits in den vorangegangenen Jahresberichten auch der Fall war – fokussiert auf datenschutzrechtliche Aspekte, die sich in Zusammenhang mit der digitalen Verwaltung ergeben. Die Idee, einleitende Ausführungen dazu durch Künstliche Intelligenz (KI) schreiben zu lassen, drängt sich im spezifischen Kontext der digitalen Verwaltung geradezu auf. Auf die (bewusst offen formulierte) Frage **Welche Rolle spielen datenschutzrechtliche Aspekte bei der digitalen Verwaltung?** antwortete ChatGPT des Unternehmens OpenAI Mitte Mai 2023:

«Datenschutzrechtliche Aspekte spielen bei der digitalen Verwaltung eine sehr wichtige Rolle, da bei der Verarbeitung personenbezogener Daten von Bürgerinnen und Bürgern deren Rechte geschützt werden müssen. Die digitale Verwaltung sammelt, speichert und verarbeitet eine Vielzahl von personenbezogenen Daten, wie z. B. Namen, Adressen, Sozialversicherungsnummern, E-Mail-Adressen, Bankverbindungen und Gesundheitsdaten. Diese Daten müssen gemäss den geltenden Datenschutzgesetzen geschützt werden, um sicherzustellen, dass sie nicht missbraucht werden. Die Datenschutz-Grundverordnung (DSGVO) und andere Datenschutzgesetze geben den Bürgerinnen und Bürgern Kontrolle über ihre personenbezogenen Daten und verpflichten die öffentliche Verwaltung, bestimmte Datenschutzprinzipien einzuhalten. Dazu gehören die Einhaltung von Transparenz, Zweckbindung, Datensparsamkeit, Rechtmäßigkeit, Fairness und Sicherheit bei der Verarbeitung personenbezogener Daten. Die digitale Verwaltung muss daher sicherstellen, dass sie die Datenschutzgesetze einhält, indem sie die Einhaltung der Datenschutzgrundsätze sicherstellt, Datenschutzverfahren implementiert, Datenschutz-Folgenabschätzungen durchführt, datenschutzrechtliche Bestimmungen in ihre

Verträge aufnimmt und Schulungen zum Datenschutz durchführt. Insgesamt ist die Einhaltung der datenschutzrechtlichen Bestimmungen bei der digitalen Verwaltung von grosser Bedeutung, um das Vertrauen der Bürgerinnen und Bürgern in die öffentliche Verwaltung zu erhalten und zu stärken. Nur so können die Vorteile der Digitalisierung genutzt werden, ohne dass dabei die Grundrechte der Bürgerinnen und Bürger verletzt werden.»

Auch wenn in diesem Text von ChatGPT in fachlicher Hinsicht das eine oder andere anzupassen, anders zu gewichten oder zu ergänzen wäre – es ist auf alle Fälle beeindruckend, was KI heute zu leisten vermag.

Im vorliegenden Bericht für die Geschäftsjahre 2021 und 2022 werden KI oder ChatGPT nur in Zusammenhang mit diesem kleinen Praxisbeispiel erwähnt (und auch nicht weitergehend genutzt). Nach Kenntnis der Datenschutzstelle spielen diese Technologien im Alltag der Stadtverwaltung bis dato noch keine (datenschutzrechtlich) relevante Rolle, was sich aber mit Sicherheit schon bald ändern wird.

Nachfolgend näher betrachtet werden drei datenschutzrechtliche Aspekte, die bei der digitalen Verwaltung aktuell und von Relevanz sind, nämlich

– «Once only»
– Cloud-Computing
– Digitale Partizipation

«Once only»

Eines der Kernelemente für eine erfolgreiche Digitalisierung sind die Informationen und Daten, die ihrer Bedeutung wegen zunehmend als strategische Ressource bezeichnet werden. Was schon immer galt, erhält mit der Digitalisierung neuen Schub: Die Verwaltung ist zur Erfüllung ihrer gesetzlichen Aufgaben auf richtige, vollständige, aktuelle und rasch verfügbare Daten angewiesen.

Ein Ansatz, um diese Forderungen in einer digitalisierten Welt zu erfüllen, wird darin gesehen, Daten von Privatpersonen oder Unternehmen wenn immer möglich nur einmal zu erheben, um sie dann verwaltungsintern verwenden und austauschen zu können («Once only»). Durch Vermeidung von Redundanzen soll die Qualität der Daten erhöht und der Aufwand sowohl für die Verwaltung als auch die Personen, die mit Behörden in Kontakt stehen, vermindert werden. Auch wenn das Prinzip «Once only» mittlerweile in fast allen Digitalisierungsstrategien oder –vorhaben als Voraussetzung oder Lösungsansatz erwähnt wird, steht noch lange nicht fest, was genau darunter zu verstehen ist. Auch müssen die Bedingungen, unter denen dieses Prinzip verfassungs- und datenschutzkonform ausgestaltet und umgesetzt werden kann, erst noch weiter geklärt werden.

Rechtliche Anforderungen

Klarheit und Einigkeit besteht immerhin soweit, dass eine Bearbeitung von Personendaten nach dem Prinzip «Once only» als zentrale und automatisierte Sammlung und Bekanntgabe von Daten zu gelten hat, wodurch das Risiko für Persönlichkeitsverletzungen entsprechend erhöht wird (Stichworte «Schaffung von Persönlichkeitsprofilen» oder «Gläserne Bürger*innen»). Für derartige Bearbeitungen von Personendaten stellen Bundesverfassung und Datenschutzrecht hohe Anforderungen an die erforderlichen gesetzlichen Grundlagen: Sensible Datenbearbeitungen müssen sich auf genügend bestimmte, das heisst präzise und klare Regelungen abstützen können. Grundlagen, die ein Prinzip «Once only» mit bloss allgemein formulierten Bestimmungen vorsehen würden, genügen nicht. Diese hohen Anforderungen werden auch durch das Bundesgericht konstant eingefordert: Es verlangt, dass systematische Datenerfassungen und -aufbewahrungen von wirkungsvollen rechtlichen Schutzvorkehrungen begleitet werden, um Missbräuchen und Willkür vorzubeugen. Die grösste Herausforderung für «Once only» wird wohl die Vereinbarkeit mit dem datenschutzrechtlichen Prinzip der Zweckbindung sein. Danach darf die Verwaltung Personendaten nur für gesetzlich vorgesehene Zwecke bearbeiten. Das Spannungsverhältnis ist offensichtlich: Statt Daten nach dem datenschutzrechtlichen Prinzip «only once», also nur einmal oder mindestens nur eingeschränkt auf bestimmte Zwecke zu verwenden, sollen bei «Once only» die Daten nur einmal erhoben und anschliessend verwaltungsintern für viele Zwecke verwendet werden.

TOM

Bei sensiblen Datenbearbeitungen spielen die technischen und organisatorischen Massnahmen (TOM) eine zentrale Rolle. Die Digitalisierung der Verwaltung bringt mit sich, dass auch die erforderlichen TOM entsprechend ausgestaltet werden – vor allem, weil Digitalisierung auch vermehrter Datenaustausch bedeutet, was in der Regel mit erhöhter Sensitivität verbunden ist. Es reicht nicht mehr, bloss Einzelmassnahmen wie Verschlüsselungstechnologie oder Regelung von Zugriffsrechten ins Auge zu fassen. Gefordert sind zunehmend – vor allem mit Blick auf allfällige «Once only»-Anwendungen – Massnahmen in einem eigentlich systemischen Sinne wie die Etablierung einer Datenlogistik oder die Einführung von Data Governance.

Stand in der Stadtverwaltung

Wann und in welchem Ausmass die Stadtverwaltung ihre Daten nach dem Prinzip «Once only» bearbeiten kann, wird in erster Linie von Regelungen und Vorgaben auf Bundes- und Kantonsebene abhängig sein. Auf städtischer Ebene bestehen Informationssysteme, denen das Prinzip «Once only» ansatzweise und eingeschränkt auf bestimmte Verwaltungsbereiche zugrunde liegt. So insbesondere die Datendrehscheibe OMEGA mit Personendaten aus dem Einwohnerregister, das System GAMMA mit Informationen zu Gebäuden und Grundstücken oder das Energiedaten-Projekt, das Informationen zu Energiebezug zur Verfügung stellt. Des Weiteren bestehen in der Stadt Zürich Vorhaben zu Datenlogistik und Data Governance. Die Datenschutzstelle war beziehungsweise ist in allen diesen Projekten und Vorhaben involviert, in der Regel durch unmittelbare Mitwirkung in der Projektorganisation.

Cloud-Computing

Bereits vor über zehn Jahren hat sich abgezeichnet, dass IT-Infrastrukturen und –Dienstleistungen in Zukunft nicht mehr nur vor Ort auf eigenen Rechnern (on premises) betrieben und zur Verfügung gestellt, sondern vermehrt auch als externe Dienste angeboten und genutzt werden. Aufgrund dieses technologischen Trends formulierte die Stadt Zürich in ihrer IT-Strategie 2016 das Ziel, externe Cloud-Services auf rechtskonforme, sichere und risikoarme Weise nutzen zu wollen, um von Innovationen und Kostenvorteilen zu profitieren. Mittlerweile ist diese technologische Entwicklung in einer Weise Realität geworden, dass zahlreiche Hersteller und Anbieterinnen ihre Dienstleistungen nur noch über Cloud anbieten (Cloud only).

Richtlinie Cloud-SSA

Der Stadtrat hat am 1. August 2022 die Richtlinie zur Nutzung von Cloud-Services für standardisierte stadtweite Service-Angebote (Richtlinie Cloud-SSA) erlassen. Diese Richtlinie stellt aus datenschutzrechtlicher Sicht eine zentrale Grundlage dar. Sie regelt bei der Nutzung externer Cloud-Services klar und verbindlich die Pflichten der Dienstabteilung Organisation und Informatik (OIZ) als zentrale IT-Dienstleisterin und grenzt diese Pflichten von denjenigen der anderen städtischen Organisationseinheiten ab. So hat die OIZ während der gesamten Nutzungsdauer von stadtweiten Cloud-Services die Einhaltung der erforderlichen vertraglichen, technischen und organisatorischen Massnahmen zu gewährleisten und das verlangte Sicherheitsniveau fortlaufend zu überprüfen. Die Richtlinie klärt nicht nur Zuständigkeiten und Verantwortlichkeiten, sondern gibt auch inhaltliche Vorgaben. Die standardisierten stadtweiten Cloud-Service-Angebote haben über ein derart hohes Sicherheitsniveau zu verfügen, das sämtliche rechtlichen und infrastrukturellen Anforderungen erfüllt, die sich aus datenschutzrechtlichen Vorschriften und dem Amtsgeheimnis ergeben können (Basisschutz+). Besondere Abklärungen und allfällige zusätzliche Massnahmen sind damit für städtische Organisationseinheiten nur dann erforderlich, wenn sie Informationen bearbeiten, für die weitergehende Geheimhaltungs- oder Sicherheitsvorschriften gelten.

Microsoft 365 / Microsoft Teams

Zu den weltweit dominierenden Anbieterinnen für digitale Arbeitsplätze gehört die Firma Microsoft, deren Produkte und Dienstleistungen zunehmend (nur noch) über Cloud zur Verfügung gestellt werden. Auch die IT-Infrastrukturen zahlreicher schweizerischer Verwaltungen basieren je länger je mehr auf dieser Technologie. Die Stadtverwaltung führte Microsoft Teams in den Berichtsjahren ein – wohl auch, um den Anforderungen an digitale Kommunikation und Kooperation, wie sie sich spezifisch in der Coronazeit gestellt haben, gerecht zu werden. Der Einsatz war jedoch nur zugelassen für Informationen ohne erhöhten Schutzbedarf, das heisst für Informationen, die öffentlich oder verwaltungsintern ohne besondere Geheimhaltungsanforderungen zugänglich gemacht werden konnten. Im März 2023 bestätigte die OIZ, dass Microsoft Teams den Basisschutz+ gemäss vorstehend erwähnter Richtlinie Cloud-SSA erfüllt.

In den letzten Jahren führten wohl keine anderen Standard-IT-Infrastrukturen zu derart heftigen und kontroversen Diskussionen wie dies bei Microsoft 365 bzw. Microsoft Teams der Fall war (und nach wie vor ist). Im Vordergrund steht dabei die (datenschutz-)rechtliche Auseinandersetzung, ob und unter welchen Bedingungen Schweizer Verwaltungen Cloud-Dienstleistungen einsetzen dürfen, bei denen Zugriffe auf Daten durch ausländische Behörden nicht vollumfänglich ausgeschlossen werden können. Der Umstand, dass ein absoluter Ausschluss derartiger Zugriffe weder durch vertragliche Abmachungen noch durch technische Massnahmen erreicht und sichergestellt werden kann, führt zu unterschiedlichen Einschätzungen und Haltungen hinsichtlich Zulässigkeit und Voraussetzungen des Einsatzes derartiger Technologien im öffentlichen Bereich. Die Datenschutzstelle vertritt die Auffassung, dass für den Zugriff ausländischer Behörden kein Null-Risiko-Ansatz gelten muss und dass auch dieser Aspekt der datenschutzrechtlichen Forderung nach Vertraulichkeit mittels Risikoanalyse zu prüfen und mittels verhältnismässiger technischer und organisatorischer Massnahmen zu gewährleisten ist. Damit teilt sie diesbezüglich die Haltung des Regierungsrats des Kantons Zürich, nicht aber die davon abweichende Haltung einzelner anderer Datenschutzaufsichtsbehörden.

Digitale Souveränität

Die Tatsache, dass die IT-Infrastrukturen von Unternehmen und Staat zunehmend von proprietären und cloudbasierten Produkten beherrscht werden, darf nicht nur zu datenschutzrechtlichen Fragen und Auseinandersetzungen führen. Massgebend und richtungsweisend müssen letztendlich vielmehr die staats- und gesellschaftspolitischen Überlegungen hinsichtlich Unabhängigkeit, Sicherheit und Verfügbarkeit sein. Im Fokus müssen deshalb vermehrt Fragen und Auseinandersetzungen zur digitalen Souveränität des Staates an sich sein.

Digitale Partizipation

An der Zukunft der Stadt Zürich sollen nicht nur Politik und Verwaltung, sondern auch die Zivilgesellschaft mitwirken. Es ist erklärtes Ziel der Stadt, Partizipationsprozesse durch die Nutzung und Weiterentwicklung digitaler Angebote zu erweitern. Auf dem eigens hierfür erstellten Partizipationsportal der Stadt Zürich wird die Bevölkerung aufgefordert, selber aktiv zu werden, Einfluss zu nehmen und mitzugestalten. In mittlerweile rund 40 Mitwirkungsvorhaben können (bzw. konnten) sich Interessierte im Dialog einbringen oder an Debatten und Umfragen teilnehmen.

Datenschutzrechtliche Relevanz

Digitale Partizipation bedeutet Austausch von Informationen. Können Äusserungen oder Mitteilungen direkt oder auch nur indirekt den jeweiligen Verfasser*innen zugeordnet werden, ist regelmässig auch eine datenschutzrechtliche Relevanz gegeben. Werden über Plattformen beispielsweise politische, weltanschauliche oder religiöse Äusserungen mitgeteilt, muss sogar von einer erhöhten datenschutzrechtlichen Sensitivität ausgegangen werden, da solche Informationen mit besonderen Risiken für die Grundrechte der betroffenen Personen verbunden sind. Das Gleiche gilt, wenn digitale Mitwirkungsplattformen auch Kinder und Jugendliche ansprechen und diese auffordern, sich zu äussern. Hier besteht bereits aufgrund der Zielgruppe an sich ein erhöhtes Risiko für Persönlichkeitsverletzungen. Es rechtfertigte sich deshalb, dass die Datenschutzstelle bereits in die Pilotprojekte involviert wurde, um sicherzustellen, dass entsprechende Anforderungen aus Datenschutz und Informationssicherheit frühzeitig erkannt, geprüft und berücksichtigt werden.

Partizipationsportal der Stadt Zürich

Wer sich über das städtische Partizipationsportal «Mitwirken an Zürichs Zukunft» aktiv an Vorhaben oder Ideen beteiligen will, muss sich mittels Kontoeröffnung registrieren. Ganz im Sinne des Prinzips der Datensparsamkeit werden dafür nur minimale Angaben benötigt (Name, E-Mailadresse, Passwort). Die Teilnehmer*innen können dabei frei wählen, ob sie für den Namen ihres Kontos ihren eigenen Namen oder ein Pseudonym verwenden wollen. Da zusätzlich dazu die zur Registrierung verwendete E-Mailadresse auf der Plattform nicht sichtbar ist, kann auf einfache Art eine anonyme Mitwirkung ermöglicht werden.

Ein Rückschluss auf die jeweiligen Verfasser*innen kann je nach Inhalt der Beiträge nicht immer ausgeschlossen werden oder sogar gewollt sein. Aufgrund solcher Konstellationen kommt der datenschutzrechtlichen Forderung nach Transparenz besondere Bedeutung zu. Nur wenn die Teilnehmer*innen wissen beziehungsweise wissen können, nach welchen Spielregeln sie (freiwillig) mitwirken, ist die Stadtverwaltung berechtigt, Informationen auf diese Art und Weise zu erheben. Sichergestellt wird dies durch Nutzungsbestimmungen, die die User*innen im Rahmen der Kontoeröffnung akzeptieren. Dabei werden sie darauf hingewiesen, dass die Inhalte der Plattform grundsätzlich öffentlich einsehbar sind und personenbezogene Aussagen im Text eines Beitrags oder eines Kommentars nicht anonymisiert werden können. Des Weiteren geben die Nutzungsbestimmungen Auskunft darüber, durch wen und wo die erfassten Angaben bearbeitet werden.

Die stadtinternen Massnahmen

Zahlreiche Anforderungen, die das Datenschutzrecht an Informationsvorhaben stellt, treten nach aussen kaum in Erscheinung und bleiben in diesem Sinne verwaltungsintern. Eine der wichtigsten ist dabei regelmässig die Regelung der Verantwortlichkeiten und Zuständigkeiten. Dies gilt auch für das städtische Partizipationsportal, da diese Plattform zwar zentral betrieben, aber dezentral durch diverse städtische Organisationseinheiten für deren Mitwirkungsprozesse genutzt wird. Wie üblich wurden auch für das städtische Partizipationsportal die Pflichten, Prozesse und Rahmenbedingungen verbindlich in einem Datenschutzkonzept geregelt.

Whistleblowing

Nicht korrektes Verhalten, Unregelmässigkeiten oder gar strafbare Handlungen müssen verhindert und aufgedeckt werden. Die Stadt Zürich bekennt sich zu Offenheit und Transparenz und fordert ihre Mitarbeitenden auf, Missstände zu melden. Sie verlinkt hierfür auf ihrer Webseite auf eine Plattform für Whistleblowing, welche allen Personen ermöglicht, auf einfache und vertrauliche Weise einen Hinweis oder Verdacht zu melden. Empfängerinnen der Meldungen sind die Ombudsstelle und die Finanzkontrolle, zwei von der Stadtverwaltung unabhängige Behörden. Whistleblower*innen haben dabei die Möglichkeit, ihre Mitteilungen anonym zu erstatten und auch weitergehend mit der Ombudsstelle oder der Finanzkontrolle im Dialog zu bleiben, ohne ihre Identität preisgeben zu müssen.

Fokussierung auf meldende Mitarbeitende

Im Rahmen des städtischen ISDS-Prüfprozesses (vgl. dazu **Seite 12**) konnte die Datenschutzstelle feststellen, dass das Whistleblowing-Tool die erforderlichen rechtlichen und sicherheitstechnischen Rahmenbedingungen erfüllt. Es zeigte sich aber, dass beim Thema Whistleblowing – allgemein, aber auch in der Stadt Zürich – beinahe ausschliesslich auf die Anliegen der meldenden Mitarbeitenden fokussiert wird: Diejenigen, die auf einen Missstand hinweisen, dürfen aufgrund zulässiger Meldungen im Anstellungsverhältnis nicht benachteiligt werden. Diese Forderung ist ohne Zweifel von grundlegender Bedeutung und dementsprechend unbedingt zu gewährleisten, darf aber nicht dazu führen, dass den übrigen verwaltungs- und datenschutzrechtlichen Vorgaben nicht genügend Beachtung geschenkt wird.

Rechte Betroffener

Nebst dem Schutz der Whistleblower*innen gilt es auch, die Rechte derjenigen Personen zu gewährleisten, die von Meldungen betroffen sind (insbesondere wenn sie namentlich erwähnt oder auf andere Weise identifizierbar sind). Für sie können Whistleblowing-Meldung schwerwiegende negative Konsequenzen mit sich bringen, so dass dem Grundrechts- und Persönlichkeitsschutz dieser Personen entsprechende Bedeutung beizumessen ist. Klarheit muss insbesondere darüber bestehen, nach welchen Verfahrensregeln Untersuchungen zu führen sind und welche Auskunfts- und Informationsrechte den involvierten Personen zustehen.

Legitimation der Meldestellen

Whistleblowing-Meldungen beinhalten regelmässig gravierende Vorwürfe, die es abzuklären oder zu verifizieren gilt und die sich (auch) gegen bestimmte Mitarbeitende, Vorgesetzte oder weitere Personen richten. Verwaltungsstellen, die derartige Meldungen entgegennehmen und weiter behandeln, müssen für diese Aufgaben und den damit verbundenen Kompetenzen – wozu insbesondere auch die Bearbeitung sensitiver Personendaten gehört – über genügende Rechtsgrundlagen verfügen. Für die beiden städtischen Stellen, an die die Meldungen aus dem erwähnten Whistleblowing-Tools zugestellt werden, ist dies gegeben. Gemäss Gemeindeordnung gehört es zu den Hauptaufgaben der Ombudsstelle, Beschwerden gegen die Stadtverwaltung zu prüfen, unabhängig davon, ob diese als Whistleblowing-Meldungen bezeichnet werden oder nicht. Meldungen und Hinweisen nachzugehen, gehört auch zu den Aufgaben der Finanzkontrolle. Ihre Rechtsgrundlagen sind diesbezüglich zwar weniger explizit, genügen aber aus datenschutzrechtlicher Sicht, sofern sich die Abklärungen auf finanztechnische Belange beschränken und dazu keine sensitiven Personendaten bearbeitet werden.

Rechtsgrundlage für Whistleblowing

Die Stadt Zürich hat für Whistleblowing keine spezifischen Rechtsgrundlagen erlassen (wie dies beispielsweise der Bund oder die Kantone Bern oder Basel-Stadt getan haben). Vor über zehn Jahren wurde ein Postulat, welches eine klare Regelung für das Melden von Missständen verlangte, mit dem Verweis auf eine diesbezügliche Broschüre der Dienstabteilung Human Resources Management abgeschrieben. Ohne den Nutzen einer solchen Broschüre in Frage zu stellen, muss dennoch bezweifelt werden, ob Zuständigkeiten und Kompetenzen für Whistleblowing in der Stadtverwaltung auf genügenden Rechtsgrundlagen beruhen, wenn nicht nur die Ombudsstelle und die Finanzkontrolle, sondern zusätzlich dazu noch weitere Organe als Meldestellen bezeichnet werden.

Schulfotografie

Der korrekte Umgang mit Fotografien im Schulbereich ist ein eigentliches «Datenschutzdauerthema». Bild- oder Filmaufnahmen tangieren Grund- und Persönlichkeitsrechte von Schulkindern, weshalb es wichtig ist, dass Lehrpersonen und Institutionen im Schulalltag wissen, was zu beachten ist. Schulbehörden und Datenschutzstellen stellen mittlerweile zahlreiche Merkblätter und sonstige Hilfsmittel zur Verfügung, die Tipps und Antworten auf Fragen rund um Fotografie im Lebensraum Schule geben.

In den beiden Berichtsjahren beschäftigte sich die Datenschutzstelle mit einem spezifischen Aspekt der Schulfotografie, der zwar schon seit längerem immer wieder Anlass zu Anfragen gibt, bis dato aber dennoch nur vage und wenig verlässlich geklärt war.

Klassenfotografie

Wer in der Schweiz die Schule besucht(e), kennt die Klassenfotografien aus eigener Erfahrung. Solche Bilder sind regelmässig interessante und auch amüsante Zeitdokumente persönlicher Lebensgeschichte. Diese an sich positive Konnotation der Klassenfotografie mag Grund dafür sein, weshalb Schulbehörden kaum Grund für (datenschutz-)rechtliche Aspekte oder Klärungen erkennen mochten. Ein weiterer Grund ist wohl auch darin zu sehen, dass oft nicht klar ist, was genau in Zusammenhang mit Klassenfotografie geschieht und wer für was zuständig ist. Diese Unklarheiten widerspiegeln sich in den Fragen und Vorbehalten der Eltern, die regelmässig auch an die Datenschutzstelle adressiert werden:

- Wer ist die Person oder die Firma, die von unserem Kind Fotografien erstellt?
- Wir sind zu wenig genau über die unterschiedlichen Arten von Fotografien (Portrait, Klassenfoto, Klassenspiegel) informiert worden.
- Uns ist nicht klar, zu was genau wir eingewilligt haben.
- Dürfen Produkte mit Fotografien unseres Kindes wie Tassen, Sticker, Magnete oder dgl. erstellt werden, bevor wir solche bestellt haben?

Verantwortung übernehmen, Klarheit schaffen und informieren

Nicht alle Fragen von Eltern rund um Klassenfotografien sind jeweils datenschutzrechtlicher Natur. Aber sie zeigen die Notwendigkeit auf, dass über Abläufe, Zuständigkeiten und rechtliche Anforderungen Klarheit zu schaffen ist und die Beteiligten – allen voran die Eltern – diesbezüglich rechtzeitig und verständlich zu informieren sind.

Das Schul- und Sportdepartement der Stadt Zürich hat auf Empfehlung und unter Mitwirkung der Datenschutzstelle Hilfsmittel und Vorlagen für eine rechtskonforme Erstellung von Klassenfotografien in der Volksschule erstellt. Diese beinhalten den wichtigen Hinweis, dass die Schule, die Klassenfotografien durch externe professionelle Fotounternehmen ermöglicht, eine Mitverantwortung bei der Gewährleistung des Datenschutzes trägt, auch wenn am Schluss der Kauf der Produkte ein zivilrechtliches Geschäft zwischen Eltern und Produzenten darstellt. Das Schul- und Sportdepartement erklärt den Schulen nicht nur rechtliche Regelungen und Anforderungen, es stellt ihnen vor allem auch einfach handhabbare Vorlagen für das Einholen von Zustimmungserklärungen zur Verfügung. Die Eltern erhalten dadurch übersichtlich und einfach verständlich die für sie wichtigsten Informationen rund um die Herstellung von Klassen- oder Portraitfotografien ihrer Kinder. Sie können mit wenig Aufwand, aber dennoch differenziert zu Fotoaufnahmen und zum Kauf von Produkten einwilligen. Und zu guter Letzt erkennen die Eltern, wie das Fotounternehmen mit den Bildern der Kinder umgeht und dass dieses sich gegenüber der Schule zur Einhaltung datenschutzrechtlicher Rahmenbedingungen verpflichtet hat.

Die Datenschutzstelle begrüsst diese Hilfsmittel und Vorlagen des Schul- und Sportdepartement der Stadt Zürich. Da in der Volksschule der Stadt Zürich jede Schule frei darüber entscheiden kann, welches Fotounternehmen sie mit der Erstellung von Klassenfotografien beauftragen will, ist es umso wichtiger, dass diese Instrumente auch tatsächlich zum Einsatz gelangen.

Im Berichtsjahr setzte sich die Datenschutzstelle personell wie folgt zusammen:

Marcel Studer, RA lic. iur.
Wirtschaftsinformatiker NDS
Datenschutzbeauftragter (100 %)

Patrizia Schwarz, Dr. iur.
Stellvertretende Datenschutzbeauftragte (60 %)

Katrin Gisler, MLaw
Juristische Mitarbeiterin (80 %)

Jürg von Flüe, lic. iur.
Juristischer Mitarbeiter (60 %)

Christine Dickey
Sekretariat (20 %)

Impressum

Herausgeberin
Stadt Zürich
Datenschutzstelle
Beckenhofstrasse 59
8006 Zürich

Juni 2023

Gestaltung
Züriblau, Stadt Zürich

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