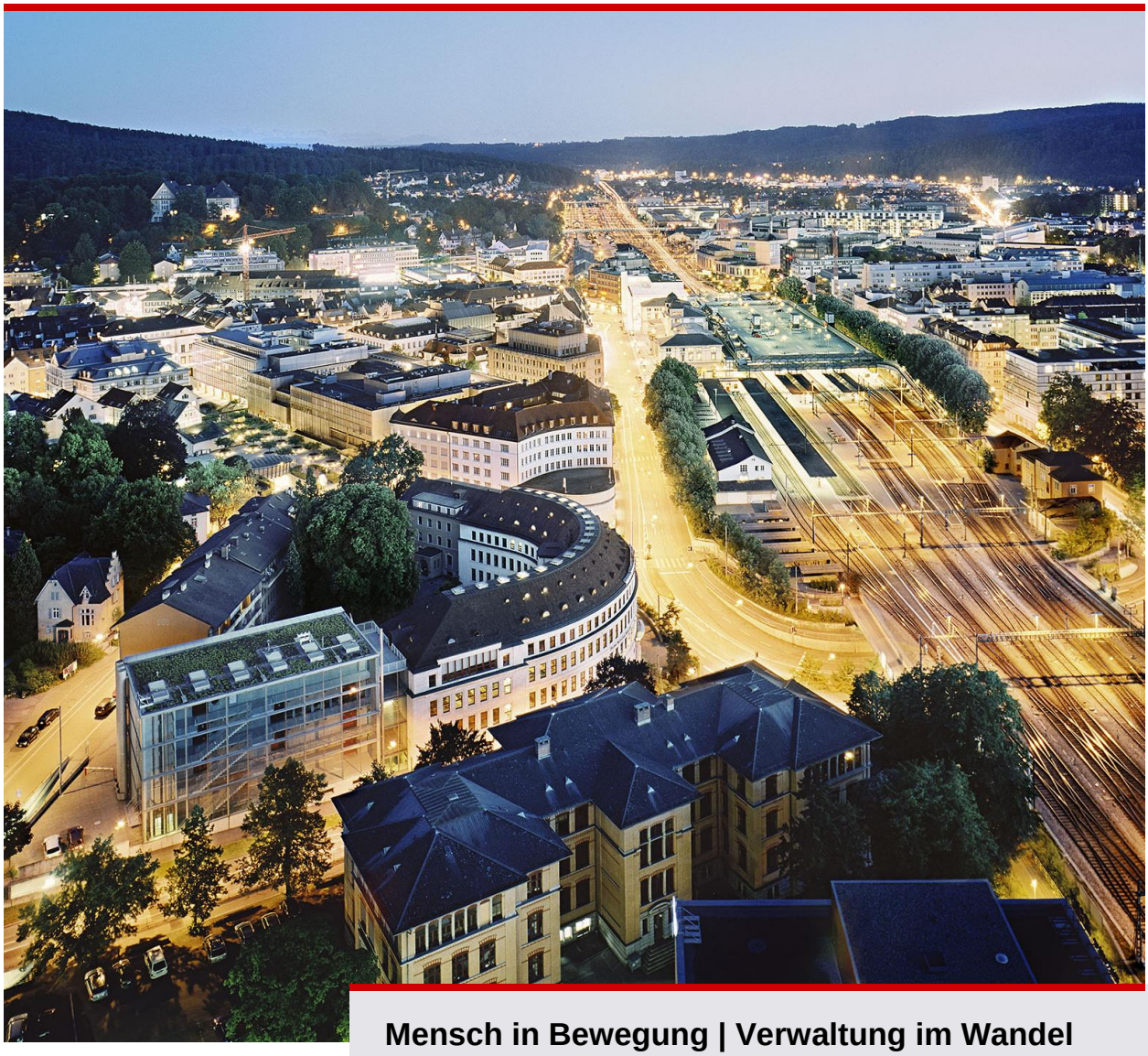
Winterthur, 2. Mai 2022
Parl.-Nr. 2022.32

Stadt Winterthur

Tätigkeitsbericht 2021

Datenschutzbeauftragte der Stadt Winterthur



Mensch in Bewegung | Verwaltung im Wandel

Die Covid-19-Pandemie hat nicht nur negative Auswirkungen: Sie kurbelt auch die Kreativität und den Wandel in der Verwaltung an. Der erhöhte Bedarf an Daten beschleunigt die Weiterentwicklung des Datenzugangs und der Informationsverarbeitung. Die klassische Prüftätigkeit hat sich dadurch über die letzten 10 Jahre hinweg begleitend zur Beratung und zum Datenschutzaudit verlagert.

Narcisa Wolf, Datenschutzbeauftragte

An das Stadtparlament

Sehr geehrte Frau Präsidentin Sorgo
Liebe Kolleginnen und Kollegen
Sehr geehrte Damen und Herren

Ich freue mich, Ihnen den Tätigkeitsbericht der Datenaufsicht der Stadt Winterthur für das Jahr 2021 zu unterbreiten. Nach einer kurzen Betrachtung der Schwerpunkte und einem Überblick über die allgemeinen Grundlagen für die Arbeit der Behörde:

- gehe ich im Besonderen auf die unterschiedlichen Tätigkeiten der Datenschutzbeauftragten an sich ein,
- bringe ich ausgesuchte Fälle aus der Praxis zur Sprache,
- und ergänze den Bericht mit einigen Schlussbemerkungen zu Interna und dem Ausblick 2022/2023.

Aufgrund der Arbeitsintensität und Steuerung des Arbeitspensums unserer Behörde, habe ich mich dazu entschlossen, im Bericht Schwerpunktthemen zu präsentieren. Eine Zusammenfassung auf den ersten Seiten soll Ihnen in aller Kürze einen sinnvollen Überblick über unsere Tätigkeiten verschaffen.

Mit vorzüglicher Hochachtung.

Winterthur, 30. April 2022

Narcisa Wolf
Datenschutzbeauftragte

§ 39 Informations- und Datenschutzgesetz des Kantons Zürich (nachfolgend IDG; LS 170.4)
Gemäss § 39 des kantonalen Gesetzes über die Information und den Datenschutz 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 vorliegende Bericht bezieht sich auf das Kalenderjahr 2021.Veröffentlicht wird der Bericht auf der Webseite der Datenaufsicht der Stadt Winterthur.

Inhaltsverzeichnis

1. Vorwort 4
2. Zusammenfassung 5
3. Die Datenaufsichtsstelle der Stadt Winterthur stellt sich vor 6
4. Fälle aus der Praxis: ausgewählte Dossiers 8
5. Internes 18
6. Anhang 19

Impressum

Herausgeberin
Datenaufsicht Stadt Winterthur
Marktgasse 53
8400 Winterthur
datenaufsicht@win.ch

Quelle Titelbild
© Stadtverwaltung Winterthur

Layout
www.tollkirsch.ch

1. Vorwort

Weltweit stehen Terrorismus-, Geldwäscherei-, Korruptions-, Internetkriminalitätsbekämpfung und die Frage nach der öffentlichen Sicherheit immer noch zuoberst in der Rangordnung auf der Traktandenliste. Im Zentrum dieser Auseinandersetzungen steht damit auch die Frage, wie weit der Datenschutz angesichts dieser Bedrohungen gehen soll bzw. darf. Das ist eine durchaus legitime Frage, denn das Datenschutzrecht bewegt sich keinesfalls im «luftleeren» Raum. In der Rechtswirklichkeit kommt der Datenschutz in der Schweiz bisher ohne ein explizites Grundrecht auf informationelle Selbstbestimmung aus.

Der Datenschutz wird traditionell als Teilbereich des Grundrechts auf Schutz der Privatsphäre konzipiert, und zwar als Schutz vor dem Missbrauch persönlicher Daten durch den Staat oder private Dritte. So heisst es in der Bundesverfassung: *«Jede Person hat Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten».* Personendaten sind nicht nur in materieller, sondern auch in ideeller Hinsicht ein «wertvolles Gut», weil es in einer demokratischen und rechtsstaatlichen Gesellschaft nicht angeht, dass der Mensch nicht einmal mehr über eine minimale Kontrolle über die Verwendung von Daten, die ihn betreffen, verfügt. Das sogenannte informationelle Selbstbestimmungsrecht bildet einen wichtigen Grundsatz unserer gesellschaftlichen Ordnung (siehe auch Once-Only-Prinzip[1] / Nationale Datenbewirtschaftung - NaDB: hier). Dieser Herausforderung hat man sich als Datenschützerin zu stellen. Die positive Wirkung der Digitalisierung wird sich dann für alle entfalten, wenn dieser Wandel in der Mitte der Gesellschaft transparent verankert ist, von allen gesellschaftlichen Gruppen gleich gut angenommen wird und die Chancen der Digitalisierung allen Bevölkerungsgruppen offenstehen. Dabei liegt es an der Gesellschaft selbst, zu definieren, wie viel öffentliche Sicherheit sie wünscht und wie viel Schutz der Privatsphäre sie dafür «opfern» will. Wie fast alles wurde auch der Alltag meiner Behörde Anfang letzten Jahres von der Corona-Pandemie bestimmt. Diese führte uns 2021 eindrücklich vor Augen, wie unabdingbar eine sichere digitale Infrastruktur für das Funktionieren unserer Gesellschaft ist. Ich fragte mich zu Beginn im Mai 2021, wie sich Homeoffice und die anhaltende Pandemie wohl auf die Anzahl Geschäfte für mein Amt auswirken würden.

Grusswort

Der Tätigkeitsbericht 2021 ist der 11. der Behörde, aber der 1. in meiner Amtszeit. Er steht im Zeichen des Schutzes der Grundrechte in Krisenzeiten und neuer Wertschöpfung durch fortschreitende Digitalisierung. Das europäische Datenschutzrecht beeinflusst die Rechtsentwicklungen in der Schweiz erheblich. Wohin steuert das europäische Datenschutzrecht? Und welchen Spielraum hat die Schweiz bei dessen Übernahme? Stehen wir bei Datenschutz und Sicherheit am Beginn einer neuen Ära?

Sie finden den Tätigkeitsbericht 2021: hier.

Trotz Corona schnellten vor allem die Beratungszahlen in der Sommerzeit weiter in die Höhe.

Mein Vorgänger, Herr Philipp Glass, dem ich an dieser Stelle für seine Arbeit als Datenschutzbeauftragter meine Anerkennung und meinen Dank aussprechen möchte, hat bereits in seinem ersten Tätigkeitsbericht darauf hingewiesen, dass eine der Aufgaben des Datenschutzbeauftragten sei, aktiv zur Entwicklung des Datenschutzbewusstseins beizutragen. Ich werde in diesem Bemühen konsequent weiterfahren und freue mich schon jetzt auf die enge Zusammenarbeit in der Stadtverwaltung sowie auf Sie, liebe Leserinnen und Leser, die ich gerne in meiner Montags-Sprechstunde begrüsse.

Narcisa Wolf
Datenschutzbeauftragte der Stadt Winterthur

[1] *Once-Only* ist eine der Säulen der Strategie für den Digitalen Binnenmarkt und eines der Grundprinzipien des EU-eGovernment-Aktionsplans 2016–2020. Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Strategie für einen digitalen Binnenmarkt für Europa, abgerufen am 2. Mai 2022: hier.

2. Zusammenfassung

Immer wieder stellt sich angesichts der Einzelfälle die Frage, wie es gelingen kann, dass meine Behörde nicht durch andere wichtige Projektaufgaben gelähmt wird. Denn auch diese werden nicht weniger umfangreich – im Gegenteil: Die Komplexität von Beratungsanfragen nimmt analog zu immer komplexeren Datenbearbeitungsmodellen und Verwaltungsprozessen kontinuierlich zu.

Folgerichtig soll das Vertrauen der Bürgerinnen und Bürger, bei Geschäftspartnern, IT-Providern und kantonalen Behörden durch konforme Datenschutzpraktiken gestärkt werden. Die Digitalisierung geniesst somit eine ausgeprägte Eigendynamik: Veraltete Verfahren werden modernisiert, ganz neue Services, wie etwa Cloud-Computing oder KI-Lösungen überschwemmen den Markt. Eine agile Beratung, Vorkontrollen und ein jährliches Datenschutzauditprogramm sollen in der Verwaltung sicherstellen, dass Datenbearbeitungsprozesse den datenschutzrechtlichen Anforderungen genügen und beispielsweise CRM-Systeme oder HR-Applikationen sowie App-Entwicklungen den Datenschutzvorgaben mit hoher Akzeptanz entsprechen.

Im Fokus eines Datenschutzaudits stehen aber auch der Mensch und seine Sensibilisierung für Datenschutz und Datensicherheit. Geschäfte, die aufgrund Datenschutzverstösse eine schnelle Reaktion erfordern, sollen rechtskonform und zeitnah abgeschlossen werden können. Durch die Sensibilisierung für einen digitalen Selbstschutz sollen «Betroffenenrechte» gestärkt und das Beschwerde-Risiko in der Verwaltung minimiert werden.

Digitale Verwaltung

Kein Datenschutz ohne technische und organisatorische Massnahmen (TOM)! Damit Technik und Verwaltungs-Organisation synchron ineinandergreifen, arbeitet die Datenschutzbeauftragte eng mit allen Fachbereichen und den Teams der IT- und der Informationssicherheit etc. zusammen. Das Resultat dieses Zusammenwirkens: massgeschneiderte und griffige Datenschutzlösungen für die Verwaltung. Die Datenschutzbeauftragte berät in diversen Datenschutzbelangen rund um die kantonalen, nationalen und internationalen regulatorischen Anforderungen. Zum Zug kommen nach ISO/IEC 27701 Best-Practice-Empfehlungen und ISO/IEC 27001 als sinnvolle Ergänzung zu ISDS/ISMS-Konzepten und Datenschutzfolgeabschätzungen (DPIA). Im Bereich Datenschutz und Datensicherheit hat die Arbeitsauslastung kontinuierlich zugenommen und wird weiter zunehmen (+ 15% bis + 20%). Allerdings sind nicht nur zahlenmässig mehr Geschäftsfälle zu bearbeiten, sondern sie sind auch komplexer geworden und erfordern: Zeit, Schulung, Vorbereitung, Sachverständigung und spezifische Kenntnisse bezogen auf verschiedene Akteure.

Die operativ-technische Umsetzung des Datenschutzes stellt viele Fachbereiche der Stadt Winterthur vor grosse Herausforderungen. Die Digitalisierung der Winterthurer Verwaltung ist weiter fortgeschritten und hat immer wieder zu neuen und komplexen Projekten geführt. Gleichzeitig hat die Corona-Pandemie die Digitalisierung vorangetrieben, was zu einem breit angelegten Einsatz von IT-Lösungen und Kommunikationsmitteln geführt und die Arbeitsweise der Verwaltung verändert hat. Sie hat auch grosse Veränderungen und drastische Einschränkungen der Privatsphäre und der Selbstbestimmung mit sich gebracht, da systematisches Beschaffen von persönlichen Daten durch den Staat, aber auch durch private Akteure die Frage der Selbstbestimmung nachhaltig verändert haben dürften. In dieser Zeit hat die Datenschutzbeauftragte pragmatisch und eng mit den Fachbereichen und anderen Datenschutzbehörden von Kantonen zusammengearbeitet.

Datenschutzaudit durch Stadtparlamentsbeschluss

Die Datenaufsicht erarbeitete 2021 eine Datenschutzstrategie und ein Auditprogramm für das kommende Jahr 2022. Die für den Datenschutz sachlich zuständige Aufsichtskommission und die Datenaufsicht einigten sich im Oktober 2021 darauf, das Arbeitspensum während drei Monaten (3) um fünfzehn Prozent (15%) zu erhöhen, damit vom Stadtparlament das gewünschte Datenschutzaudit durchgeführt werden kann. Dieses soll gewährleisten, dass einzelne Datenschutzkonzepte oder Produkte den Massgaben des IDG genügen und ein Höchstmass an Sicherheit gewährleisten.

Das Audit dient damit auch als Indikator für das Digitalisierungsvorhaben der Verwaltung. Formell ist der Entscheid zur Pensumerhöhung von der Parlamentsleitung[2] gefallen. Dagegen gab es keinerlei Opposition im Stadtparlament.

Die Datenaufsicht hat am 1. März 2022 die Arbeit aufgenommen. Ich danke dem Fachbereich für das entgegengebrachte Vertrauen. Über das Audit-Resultat wird im Tätigkeitsbericht 2022 vollumfänglich berichtet.

3. Die Datenaufsicht der Stadt Winterthur stellt sich vor

Wer sind wir?

Die Datenaufsichtsstelle der Stadt Winterthur besteht im Moment nur aus der Datenschutzbeauftragten und operiert autark. Organisatorisch ist die Datenaufsichtsstelle dem Stadtrat, also dem Parlament der Stadt Winterthur, zugeordnet; in administrativer Hinsicht der Ratsleitung des Grossen Gemeinderates.

Mit der Ratsleitung findet in der Regel ein jährliches Gespräch statt. Die Datenschutzbeauftragte übt das Amt unabhängig aus und untersteht keinem inhaltlichen Weisungsrecht.

Was tun wir?

Bei der Stadtverwaltung Winterthur arbeiten rund 5000 Angestellte. Die Stadtverwaltung besteht aus sieben Departementen, die jeweils von einem Stadtratsmitglied geleitet werden. So vielfältig und unterschiedlich die Aufgaben und Tätigkeiten der Stadtverwaltung sind, eine Gemeinsamkeit teilen die meisten Angestellten dennoch: Sie alle arbeiten mit unterschiedlichen Datensätzen bzw. Informationen, die sie erhalten oder beschaffen, weiterbearbeiten und mit anderen austauschen. Zahlreiche dieser Informationen betreffen uns Bürgerinnen und Bürger, Patientinnen und Patienten, Kundinnen und Kunden, Schülerinnen und Schüler, Mitarbeiterinnen und Mitarbeiter in direkter oder indirekter Weise. Wann immer die Stadtverwaltung personenbezogene Informationen bearbeitet, gilt es, mit diesen richtig umzugehen. Dabei ist nicht nur die Einhaltung gesetzlicher Regelungen anzustreben; Ziel ist es auch, ethisch «richtige» und damit nachhaltige Ergebnisse zu ermöglichen. Data Governance braucht Datenethik als Bestandteil und auch als Systemgrenze[3]. Es gehört folgerichtig zu den wichtigsten Aufgaben der Datenschutzbeauftragten, die Stadtverwaltung Winterthur im Umgang mit Personendaten zu beraten, zu unterstützen und neu zu auditieren. Konkret gehören folgende Aufgaben zum Tätigkeitsbereich der Datenaufsicht

[2] SRS 3.1-1 – Verordnung über die/den Datenschutzbeauftragte/n der Stadt Winterthur – Stadt Winterthur – hier.

[3] EDSA: Entwurf von Leitlinien zum «Verantwortlichen» und zum «Auftragsverarbeiter» *(Link: Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 1.0, 2. September 2020)*

Anfragen und Gesuche aus der Stadtverwaltung behandeln

Regelmässig wird die Datenaufsichtsstelle von Fachmitarbeitenden, Rechtsdiensten oder Führungskräften der Stadtverwaltung gebeten, Informationsgewinnung bzw. Informationsbearbeitungen der Stadtverwaltung aus datenschutzrechtlicher Perspektive zu beurteilen. Dabei geht es beispielsweise darum, ob Personendaten mit anderen Verwaltungsstellen ausgetauscht oder ob Informationen veröffentlicht werden dürfen, über welche Personendaten Auskunft zu erteilen oder wie bei Videoüberwachungsmassnahmen umzugehen ist.

Projekte der Stadtverwaltung

Heutzutage gibt es kaum noch Daten, die nicht mittels moderner Informations- und Kommunikationstechnik (ICT) bearbeitet werden. In der Stadtverwaltung Winterthur müssen sämtliche Projekte, die ICT betreffen, den sogenannten Informationssicherheits- und Datenschutz-Prozess (ISDS-Prozess) durchlaufen. Bei denjenigen Projekten, die aus datenschutzrechtlicher Sicht eine erhöhte Sensibilität aufweisen, führt die Datenaufsicht eine sogenannte Vorabkontrolle vor Umsetzung einer Datenbearbeitung gemäss § 10 IDG und in Abstimmung mit dem Fachbereich durch. Dabei wird geprüft, ob sämtliche Rahmenbedingungen – in rechtlicher, organisatorischer und technischer Hinsicht – eingehalten werden. Bei weniger sensiblen Projekten steht nicht die Prüfung der datenschutzrechtlichen Anforderungen im Vordergrund, sondern vielmehr die «*begleitende Beratung*» durch die Datenschutzbeauftragte. Im Berichtsjahr stellte die Stadtverwaltung der Datenaufsichtsstelle rund 12 Projekt-beurteilungen und Vorabkontrollen zur Prüfung und/oder Beratung zu.

Videoüberwachungsmassnahmen der Stadtverwaltung überprüfen

Das Thema Videoüberwachung stellt für die Datenaufsicht eine Schwerpunktthematik für das Jahr 2021 dar. Mit Beschluss vom 10. Juli 2013 hat der Stadtrat eine Videoordnung erlassen, die den städtischen Ämtern und Bereichen im Sinne einer generellen Dienstanweisung darlegt, welche Voraussetzungen beim Einsatz von Videoüberwachungsanlagen im öffentlichen Raum zu berücksichtigen sind. In der Verordnung ist vorgeschrieben, dass städtische Verwaltungsstellen für ihre Überwachungsmassnahmen Reglemente erlassen und diese der Datenaufsichts-stelle zur Prüfung unterbreiten. Mittlerweile setzen mehrere städtische Verwaltungsstellen Videoüberwachung ein und haben hierfür Reglemente erlassen. Der Beratungs- und Prüfungsaufwand der Datenaufsichtsstelle in diesem Bereich ist gestiegen, auch weil die Reglemente von Zeit zu Zeit neu geschrieben oder angepasst werden müssen, aber auch weil die Datenschutzbeauftragte vermehrt Augenschein vor Ort (*Hot-Spot* Entwicklung) nehmen muss. Weitere Ausführungen zum Thema Videoüberwachung folgen *im Kapitel 4.*

Bei Stadtratsgeschäften und Gesetzgebungsverfahren mitwirken

Bei Anträgen an den Stadtrat, welche Belange des Datenschutzes betreffen, wird die Datenaufsichtsstelle zur Stellungnahme bzw. zum Mitberichtsverfahren eingeladen. Werden rechtliche Grundlagen der Stadtverwaltung neu geschaffen oder angepasst und beinhalten diese auch datenschutzrechtlichen Themen, ist die Datenaufsichtsstelle in die entsprechenden Gesetzgebungsprojekte involviert.

Anfragen und Gesuche von Privatpersonen beantworten

Wenden sich Privatpersonen mit Fragen oder Beschwerden an die Datenaufsichtsstelle, führt dies oft zu umfangreichen Abklärungen, auch im Hinblick auf

Zuständigkeiten und Weiterleitung an den Kanton, gegebenenfalls an den Bund. Solche «Anstösse von aussen» haben einen positiven Synergie-Effekt, können Fehler oder Lücken bei Datenbearbeitungen in der Stadtverwaltung aufzeigen und zu entsprechenden Korrekturen führen.

Internes Auditprogramm durchführen
Ein Datenschutzaudit ist eine «freiwillige» Prüfung der Datenschutzkonformität der Verwaltungsstellen, die Daten bearbeiten. Es dient dazu, den Ist-Zustand hinsichtlich Erfassung, Speicherung und Weitergabe personenbezogener Daten festzustellen. Ein solches Audit umfasst Gespräche mit Mitarbeitenden, Dokumentenprüfungen und Untersuchungen der Systeme und Prozesse. Basierend auf den Ergebnissen werden dann Massnahmen vorgeschlagen und Handlungsempfehlungen ausgesprochen, die zu einem idealen Soll-Zustand in der Verwaltungseinheit führen sollen. Die Zielvorgabe besteht darin, im Jahreszyklus ein Auditprogramm durchzuführen. Eine regelmässige Überprüfung der Datenschutzkonformität in der Verwaltung dient nicht nur der rechtlichen Absicherung gegenüber der IDG-Anforderungsspanne. Die Audits stärken zudem das Vertrauen von Bürgerinnen und Bürgern, Kundschaft, Partnern und Mitarbeitenden in der Stadtverwaltung. Ein Auditbericht wird für 2022 zur Verfügung stehen.

Aus- und Weiterbildung durchführen
In unserer Gesellschaft sind Daten zu einem der wichtigsten Güter geworden. Das Datenschutzrecht und die Datensicherheit betreffen das gesamte Spektrum der Stadtverwaltung Winterthur und bringen aufgrund des gesellschaftlichen und technologischen Wandels neue Fragestellungen mit sich, wobei Schulungen unabdingbar sind. Ein entsprechendes Schulungsmodul wurde für «My Learn» seitens Personalentwicklung als Weiterbildungsangebot initiiert und wird mit Unterstützung der Datenschutzbeauftragten zurzeit erarbeitet.

4. Fälle aus der Praxis: ausgewählte Dossiers

Parkuhren mit Kontrollschildereingabe

Im Zuge des städtischen Gesamtverkehrskonzepts hat die Stadtpolizei Winterthur den Auftrag erhalten, eine moderne digitale Lösung für das Beantragen von Parkkarten und das Bezahlen von Parkgebühren einzuführen. Der Zuschlag für diesen Auftrag wurde ans Schweizer Parkplatzbewirtschaftungs-Unternehmen Digitalparking AG in Dietikon vergeben. Deren Anwendung «Parkingpay» funktioniert sowohl als App auf dem Handy wie auch als Lösung auf dem Computer.

Was ist eigentlich ein digitales Parkbewirtschaftungssystem?
Ein Parkplatzbewirtschaftungssystem beinhaltet neben Daten über die eigentliche Bewirtschaftung auch Daten über den Zahlungs- und den Kontrollvorgang. Daneben verläuft eigenständig das Bussenverfahren. An diesen modernen Systemen, sind die Stadt, der App-Anbieter und die Nutzenden beteiligt. Mit Bezug

Digitales Parkieren

Der Datenschutz ist eine heikle Frage im Zusammenhang mit Parking-Apps: Angegeben werden muss zum Parkieren nämlich das Kontrollschild des Autos. Es bräuchte wenig, um daraus ein Bewegungsprofil des Nutzers zu erstellen.

auf das Verhältnis zwischen der Stadt und dem App-Anbieter handelt es sich um einen typischen Fall von Outsourcing. Der App-Anbieter handelt im Auftrag der Stadt, erhebt die Daten, bietet diverse Zahlungsabwicklungen an und betreibt die Datenbank. Wichtig ist, dass dieser Vertrag den Zweck möglichst genau umschreibt, Bestimmungen betreffend die Sicherheit beinhaltet und insbesondere die regelmässige Löschung der Daten bestimmt. Will ein Nutzender die Parkgebühr via App bezahlen, tritt er in eine eigenständige Vertragsbeziehung mit dem App-Anbieter. Dabei handelt es sich um ein privatrechtliches Verhältnis. Diese Unterscheidung ist insbesondere in Bezug auf die Aufbewahrung von Daten wichtig. Zu unterscheiden ist im Weiteren zwischen der Abwicklung der Parkplatzbenützung und dem Bussenverfahren. Es handelt sich dabei um zwei unterschiedliche Verfahren, welche auf unterschiedlichen gesetzlichen Grundlagen beruhen.

Die datenschutzrechtlichen Grundsätze des IDG sind von den Datenbearbeitern einzuhalten und zu gewährleisten. Das IDG des Kantons Zürich bezweckt, das Handeln öffentlicher Organe transparent zu gestalten, um damit die freie Meinungsbildung sowie die Wahrnehmung der demokratischen Rechte zu fördern und die Kontrolle des staatlichen Handelns zu erleichtern (§ 1 Abs. 2 lit. a IDG). Zudem sollen mit dem IDG die Grundrechte von Bürgerinnen und Bürgern geschützt werden, deren Daten von öffentlichen Organen bearbeitet werden (§ 1 Abs. 2 lit. b IDG). Diese Bestimmungen (Auftragsbearbeitung) gelten im Rahmen einer Übertragung an Dritte nach § 6 Abs. 1 und Abs. 2 IDG letztlich auch synchron für den Park-App-Betreiber. Die Stadt Winterthur ist – als Auftraggeber und verantwortlich bleibendes öffentliches Organ – gesetzlich dazu verpflichtet, sicherzustellen, dass die Datenbearbeitung durch den «Parking-App»-Betreiber in Übereinstimmung mit den öffentlich-rechtlichen Bestimmungen des/r IDG/IDV erfolgt und muss diesen vertraglich entsprechend verpflichten.

Aktivitäten der Datenaufsicht

Die Datenaufsicht hat diverse Risikoabschätzungen sowohl regulatorisch als auch technisch überprüft und im Kontext diverser Anfragen von Bürgerinnen und Bürgern Empfehlungen an den Stadtrat abgegeben. Grundsätzlich lässt sich als primärer Zweck für die Stadt Winterthur die Zahlung von Parkierungsgebühren mittels App, aber auch die Kontrolle der erfolgten Zahlung ausmachen. Da Bewegungsprofile bei Dauerparkieren heikel sind, sollte ein «Anonymes Parkieren» ohne Online-Registrierungs-Zwang weiterhin möglich sein. Allerdings muss dieser Zweck für die betroffenen Personen erkennbar sein, resp. sie sind darüber sowie über den Kennzeichen-Erfassungs-, Speicherungs- und Löschungs-Zyklus zu informieren. Im Rahmen der Auftragsbearbeitung sollte zur Erfüllung des Grundsatzes der Erkennbarkeit bzw. der Informationspflicht die Stadt dafür sorgen, dass keine problematische Vermischung von Zwecken der Stadtverwaltung mit Zwecken der privaten Anbieter erfolgt, welche für die Nutzenden nicht erkennbar ist. Es ist zu empfehlen, dass die Stadt Winterthur die Nutzenden selbst mittels Datenschutzerklärungen und Datenschutzfolgeabschätzungen darüber in Kenntnis setzt, wie, von wem unter Verantwortung der Verwaltung und zu welchem Zweck die Daten (darunter die Kfz-Nummer) bearbeitet werden (resp. die Betreiber der Park-Apps entsprechend dazu verpflichtet). Grundsätzlich ist es ferner möglich, Park-Apps verhältnismässig und holistisch auszugestalten. Allerdings sollte im Einzelfall geprüft werden, welche Daten zu den vorgesehenen Zwecken (Bezahlung von Parkierungsgebühren mittels App und Kfz-Kontrolle) erforderlich sind und wie (und wie lange) sie bearbeitet werden müssen – 48h, 72h oder 7 Tage oder 15 Tage.

Als Fazit meinerseits lässt sich festhalten, dass die zunehmende digitale Parkplatzbewirtschaftung die Stadt Winterthur vor eine erhebliche rechtliche Herausforderung stellen wird. Technische Hilfsmittel wie Smartphone-Apps können das bargeldlose Bezahlen von Parkgebühren zwar attraktiv machen. Für eine verantwortungsvolle Digitalisierung braucht es jedoch flächendeckende Transparenz über die Rechtsverhältnisse zwischen der (i) Stadt Winterthur als Verantwortliche, (ii) den «Parking-App»-Betreibern, (iii) dem Kontrollorgan, (iv) der Datenaufsicht sowie (v) den Parkplatz-Nutzenden.

Schwerpunktthema: Videoüberwachungsmassnahmen

Digitale Technologien prägen zunehmend Kindheit und Jugend: von der Videoüberwachung im Säuglingsalter über den Lernroboter im Kindergarten bis hin zum durch Künstliche Intelligenz gesteuerten Lernassistenten für den individuellen Bildungserfolg. Worüber jedoch wenig reflektiert wird, sind Privatheit-, Überwachungs- und Datenschutzfragen in diesem sensiblen und wichtigen gesellschaftlichen Bereich. Videoüberwachungsmassnahmen nehmen im Winterthurer Alltag rasant zu, sei es in den Schulen, Spitälern, Bibliotheken, Bussen, im Theater, in der Eishalle, Tiefgaragen, Wohnhäusern, mit Drohnen oder Dashcams, bei der Abfallproblematik oder zwecks Einbruch-Prävention, oder in Schwimmbädern. Wer Menschen so aufnimmt, dass sie identifizierbar sind, bearbeitet Personendaten und muss deshalb das Datenschutzrecht zwingend berücksichtigen. Die Datenschutzbeauftragte hat sich 2021 intensiv mit solchen Anfragen befasst:

Videoüberwachung

Die Videoüberwachung ist im öffentlichen Raum grundsätzlich unzulässig. Menschen haben oft keine Wahl, ob sie ein überwachtes Gebiet betreten wollen –der Datenschutz beginnt genau am Perimeter. Privatpersonen können sich nicht auf die Sicherheit als Überwachungsgrund berufen. Denn das ist Aufgabe der Polizei und untersteht somit nicht der Entscheidung des Einzelnen. Grundrechte und Sicherheit müssen sich allerdings nicht gegenseitig ausschliessen. Wenn Videoüberwachungssysteme pragmatisch auf der Basis der beiden Grundsätze der Selektivität und der Verhältnismässigkeit eingesetzt werden, können sie den Sicherheitserfordernissen gerecht werden und zugleich unsere Privatsphäre achten.

- **Einsatz Videoüberwachung**
  Anfahrt auf Baustellenperimeter
  Bezirksanlage Winterthur
  Ort: Baustelle Hermann-Götz-Strasse, Winterthur
  Zweck der Installation: Regelung
  und Überwachung der Baustellenzufahrt

Das Ziel dieser Videoüberwachung ist, dass der Logistiker auf der Baustelle einen erweiterten Blick erhält, wann exakt ein Lastwagen auf die Hermann-Götz-Strasse einbiegt. Die erweiterte Sicht ist als relevantes Überwachungssystem einzustufen, weil ansonsten eine Komponente im gesamten Ausführungsprozess der Logistik nicht gesteuert werden kann, nämlich die vorhandene kritische Verkehrssituation. Es gilt sicherzustellen, dass keine gefährlichen Kreuzungsmanöver stattfinden. Gerade auch bei geschlossener Baustellenzufahrt muss dies eng überwacht werden, weil sonst die Lastwagen einen gefährlichen Stau verursachen. Die Verkehrs- und Personensicherheit bzw. die Aufrechterhaltung des Verkehrsflusses auf der Hauptstrasse (Lindstrasse) soll gewährleistet bleiben, der öffentliche Verkehr darf nicht beeinträchtigt werden, zudem dürfen keine Blockierungen und Rückstaus insbesondere im Bereich des unter Betrieb stehenden Gefängnisses und des Bezirksgerichts (Interventions-Zufahrt für Blaulichtorganisationen) verursacht werden. Die Videoüberwachung für die besagte Baustelle wurde demnach auf die datenschutzrechtlichen Anforderungen individuell überprüft. Zurzeit prüft die Datenaufsicht eine erweiterte Lösung, um per Analytics-Software (KI-Algorithmus) grössere Fahrzeuge detektieren zu können, um bei der Baustellenausfahrt automatisch eine «Ampel» zu steuern.

- **Einsatz Videoüberwachung(en)**
  des Polizeigebäudes POM[4], Winterthur
  Ort: Polizeigebäude Obermühlestr., Winterthur
  Zweck der Installation: Sicherheitsmassnahmen

Die Datenaufsicht hat diesbezüglich die ersten Schritte einer Vorabkontrolle und eines Datenschutzkonzepts samt Empfehlungen vor Ort im Rohbau vorgenommen. Eine End-Abnahme ist für 2022 geplant. Das entsprechende Reglement wird auf der Website der Stadtverwaltung und eine direkte Veröffentlichung der Dienstanweisung auf der Website der Stadtpolizei demnächst publiziert.

[4] Informationen hier verfügbar: pombau.ch

Projektarbeit

Schnittstelle NEST EWK – ZLPro – Beurteilung technischer Datenschutz

Im Projekt «Schnittstelle NEST EWK – ZLPro» geht es um die Realisierung einer Schnittstelle aus dem NEST-EWK-System der Einwohnerkontrolle der Stadt Winterthur für die Fallführungsapplikation ZLPro des Bereichs Zusatzleistungen innerhalb der Hauptabteilung Sozialversicherungen. Bislang erfolgte die Datenübernahme aus dem NEST-EWK-System durch die Fallführenden im Bereich Zusatzleistungen mittels Zugriff über das NEST EWK Web-Info-Center. Die Daten wurden anschliessend manuell übernommen. Dies wurde nun durch eine applikatorischen Schnittstelle automatisiert – sowohl der initiale Import der betreffenden EWK-Daten beim Anlegen eines neuen Falls/Dossiers in ZLPro als auch die Verarbeitung von Mutationsmeldungen inkl. Erstellung der Dispositionen in ZLPro. Ein Informationssicherheits- und Datenschutzkonzept (ISDS) wurde auf Basis einer Schutzbedarfsanalyse erstellt, wobei datenschutzrechtliche Anforderungen sowie Datenflussanalysen gemäss Risikomatrix abgefangen und miteinbezogen wurden. Die implementierte Schnittstelle sowie die notwendigen applikatorischen Anpassungen in ZLPro orientierten sich an der entsprechend für die Stadt Zürich implementierten Lösung. Neben diesen projektbezogenen Massnahmen, welche erfüllt wurden, gab es «departementsbezogene» bzw. längerfristige Massnahmen, welche dem zuständigen Fachbereich adressiert wurden, u. a. die risikobasierte Kategorisierung der in ZLPro verwalteten Daten. Dieser und allfällige weitere Punkte sollen ausserhalb des Projekts längerfristig angegangen werden, beispielsweise innerhalb eines IT-Audits bzw. Datenschutzaudits.

Mobile App: Trendentwicklung

Zum Sachverhalt

Der Fachbereich Soziales hat in Kooperation mit dem Verein «*Jugendarbeit.digital*» eine Applikation erstellt, die den Klientinnen und Klienten der sozialen Dienstleistungsinstitution via «privatem» Mobiltelefon und den Betreuungspersonen via Geschäfts-Computer Zugriff auf Inhalte der Fallbearbeitung erlauben soll. Dabei erhalten sowohl die Betreuungsperson als auch die Klientin bzw. der Klient online Zugang zu diversen Datenverarbeitungsprozessen. Ein funktionsfähiger Prototyp wurde entwickelt und die Synergien der Features in der JugendApp (jugendinfo.ch) genutzt, sodass die App in die technische Infrastruktur eingebunden werden kann.

Beurteilung

Die geplante App-Nutzung betrifft eine *grosse Anzahl* von Personen bzw. Personenkreise. Durch das Teilen der Inhalte (insbesondere sind dies Informationen aus bzw. zu der Fallbearbeitung, Chat-Inhalte, Zielvereinbarungen sowie Informationen zu vereinbarten Terminen) werden sowohl personenbezogene Daten, sensible als auch besonders schützenswerte Daten wie Gesundheitsdaten, Religionszugehörigkeit, Massnahmen sozialer Hilfe und/oder Sanktionen aufbewahrt. Diese Daten sind gemäss § 3 Abs. 4 lit. a und lit. b IDG zu qualifizieren. Das Projekt unterlag aus diesen Gründen der Vorabkontrolle durch die Datenschutzbeauftragte i. S. d. § 10 IDG i. V. m. § 24 Abs. 1 lit. b und e IDV, was sich als grosse Herausforderung für den Fachbereich herausstellte.

Im Hinblick auf die Nutzung der App waren verschiedene Mechanismen zur Sicherheit zu beachten und entsprechende Schutzmassnahmen vorzubereiten. Vorausgesetzt war eine sichere Konfiguration des mobilen Gerätes auf der Anwenderseite. Es wurden technische Parameter mittels Datenschutz-Assessment geprüft: Registrierungsmerkmale, Server-Performance, Datentransfer und Datenzugriff, Schnittstellen, Sicherheitsanforderungen des Datenbearbeitungskanals, Verschlüsselungen. Rechtliche Anforderungen sind ebenfalls geprüft worden. Gleichzeitig sind Nutzungsbedingungen und eine Datenschutzerklärung gemäss Empfehlungen der Datenschutzbeauftragten ausgearbeitet worden. Hauptaugenmerk war der Umstand, dass durch die Bearbeitung zahlreicher Personendaten ein Persönlichkeitsprofil entstehen könnte. Ein Persönlichkeitsprofil entsteht bei der Zusammenstellung von Informationen, die dann unmittelbar eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer Person erlaubt. Persönlichkeitsprofile sind besondere Personendaten per se, für deren Bearbeitung höhere datenschutzrechtliche Anforderungen zu erfüllen sind. Das Projektteam hat nach der Vorabkontrolle grünes Licht zum Pilottest erhalten mit der dringenden Auflage um Verzicht von Biometrie. Es wurde ausserdem in den Nutzungsbedingungen festgehalten, dass ein

«Screen Lock» mit automatischer Sperre bei Inaktivität standardmässig aktiviert sein muss. Sofern Passwörter dennoch auf dem Gerät gespeichert werden, sollte auf den Einsatz von starken kryptografischen Verfahren nach dem Stand der Technik zu achten sein. Bei erhöhtem Schutzbedarf wie etwa bei biometrischen Daten ist eine Speicherung der Zugangsdaten im Allgemeinen nicht zulässig, da mit dieser Funktion, die meist als Komfortmerkmal zur App-Bedienung eingesetzt wird, das notwendige Schutz-niveau bei Verlust des Gerätes nicht erreicht werden kann.

Schlussfolgerung
Eine zentrale Rolle bei der datenschutzgerechten Gestaltung (sog. «Privacy by Design»-Grundkonzept) spielte die Datenschutz-Compliance und -Awareness eine grosse Rolle im Projekt. Bereits im Entwicklungsprozess der App war zu erwarten, dass zur Vermeidung erhöhter Entwicklungs- und Nachbesserungskosten darauf hingewirkt werden muss, kritische Schwachstellen im Vornherein zu vermeiden und die Sicherheit der App auf ein Niveau zu setzen, das den datenschutzrechtlichen Anforderungen entspricht (§ 7 IDG). Dieser Umstand wurde leicht überschätzt, allerdings mit Unterstützung der Datenaufsicht und Mitwirkung der IDW korrigiert. Die Datenaufsicht bietet weiterhin Unterstützung und behält sich vor, gemäss § 35, 36 IDG eine zyklische Kontrolle (Datenschutzaudit) vorzunehmen.

Begleitende Beratung: Beurteilung der Datenbearbeitung zur Anstrengung eines Strafverfahrens im Schulwesen

Zum Sachverhalt
Eine Strafverfolgungsbehörde aus Winterthur hat in der Untersuchung einer Straftat darum ersucht, dass folgende Akten herausgegeben werden: aktuelle Klassenspiegel (Fotos) inkl. dazugehöriger Klassenlisten. Es stellte sich die Frage, unter welchen Voraussetzungen eine Schule solche Anfragen datenschutz-konform beantworten sollte.

Aktivitäten der Datenaufsicht
Ende September 2021 wurde die Datenschutzbeauftragte der Stadt Winterthur beauftragt, die «bereits erfolgte» Datenaushändigung zu bewerten. Eine Erstempfehlung wurde unmittelbar telefonisch ausgesprochen. Im Oktober 2021 wurde die entsprechende Amtsstelle vor Ort seitens Datenschutzbeauftragte aufgesucht und datenschutzrechtliche Parameter wurden aufgefangen. Damit eine Massnahme, welche in den Persönlichkeitsbereich einer privaten Person eingreift, als verhältnismässig eingestuft werden kann, muss diese im Hinblick auf den zu erreichenden Zweck geeignet und notwendig sein. Ausserdem muss der angestrebte Zweck in einem vernünftigen Verhältnis zum Eingriff in den Persönlichkeitsbereich der privaten Person stehen. Grundsätzlich gilt: Bei begründetem Verdacht einer Straftat leitet die Staatsanwaltschaft zunächst ein Ermittlungsverfahren ein. Mit Unterstützung durch verschiedene Ermittlungspersonen sammelt die zuständige Staatsanwaltschaft nach dem sog. Freibeweisverfahren alle Informationen, die den Verdacht bestätigen oder ausräumen könnten. Ein zulässiges Mittel zur Informationsbeschaffung kann dabei auch die Abfrage von Daten bei den Schulen sein:

Attribut Geeignetheit: Diese Massnahme ist geeignet, um den Täterkreis auf diejenigen Personen einzuschränken, welche die Taten tatsächlich begangen haben, und um basierend hierauf weitere Massnahmen (z. B. Einvernahmen) zu ergreifen, um die Täterschaft feststellen zu können. Daher ist die angeforderte Datenbearbeitung geeignet gewesen, um eine Strafuntersuchung einzuleiten.

Attribut Erforderlichkeit: Die ergriffenen Massnahmen zielen auf die Identifikation der Täter. Für eine Anzeige bei den zuständigen Strafverfolgungsbehörden ist grundsätzlich ein erster Anhaltspunkt nötig, damit ein Strafverfahren gegen eine bestimmte Person eingeleitet werden kann. Daher kann es erforderlich sein, in diesem Rahmen eine «Schranke des Datenschutzes» zu öffnen, sprich eine «Persönlichkeitsverletzung» festzustellen, da somit die Erfolgswahrscheinlichkeit der Überführung des Täters erheblich gesteigert wird, so auch im vorliegenden Fall.

Attribut Verhältnismässigkeit/Zumutbarkeit: Unabhängig von urheberrechtlichen Überlegungen besteht bei Fotos das Recht am eigenen Bild. Dies bedeutet, dass die abgebildeten Personen in der Regel darüber entscheiden, ob und in welcher Form ein Bild aufgenommen und veröffentlicht werden darf. Aus diesem Grund dürfen Fotos meist nur dann veröffentlicht/bekannt gegeben werden, wenn die darauf Abgebildeten ihr Einverständnis gegeben haben. Zur Feststellung einer Straftat vertritt der Eidgenössische Datenschutz-

und Öffentlichkeitsbeauftragte (EDÖB) allerdings die Meinung, dass es zuzumuten ist, einer Strafuntersuchung ausgesetzt zu werden, solange der Person hierdurch – bei Unschuld – keine ernsthaften Nachteile erwachsen, in casu nicht ersichtlich.

Die Amtshilfe/Privilegierung der Aufdeckung oder Verfolgung von Straftaten: In gerichtlichen Verfahren, wie in casu Anfragen von Polizei/Staatsanwaltschaft, benötigen Lehrpersonen eine schriftliche Ermächtigung (als Entbindung vom Amtsgeheimnis) von der vorgesetzten Stelle (in casu wohl: Schulpräsidentin). Bei solchen gerichtlichen Verfahren sind nicht die kantonalen Datenschutzbestimmungen, sondern ist die jeweilige Prozessordnung anwendbar, hier Art. 44 i. V. m. Art. 194 StPO.

Schlussfolgerung
Verlangt eine Strafverfolgungsbehörde im Rahmen eines Strafverfahrens Bilder und stützt sich dabei auf eine Verfügung, so ist das Herausgeben der Bilder gerechtfertigt. Stellt die Behörde die Anfrage ausserhalb eines Strafverfahrens, kann ein überwiegendes öffentliches Interesse die Herausgabe auch ohne Verfügung rechtfertigen. Ob ein solches vorliegt, muss aufgrund einer Interessenabwägung beurteilt werden. Dieser Entscheid kann heikel sein und sollte sich stets auf die nachfolgenden Überlegungen stützen: Zunächst wird geprüft, wer die Herausgabe verlangt. Anschliessend muss geprüft werden, zu welchem Zweck die Bilder benötigt werden. Daher sollte die schriftliche Anfrage stets eine Begründung enthalten. Eine Herausgabe ohne Verfügung ist nur dann gerechtfertigt, wenn damit schwerwiegende Interessen geschützt werden sollen; bei Anfragen ohne Begründung oder zu Bagatellzwecken sollte die Herausgabe begründet *verweigert* werden.
.

Beratung von Privaten

Die Datenschutzstelle ist auch Ansprechstelle für Privatpersonen, soweit deren Daten durch die städtischen Organe oder private Institutionen mit Leistungsvereinbarungen bearbeitet werden. Die Datenschutzstelle gibt Privaten Auskunft über ihre Rechte und kann, falls erforderlich, auch zwischen Organen und betroffenen Personen vermitteln, gegebenenfalls zuständigkeitshalber weiterleiten.

Die Anfragen von Privatpersonen nahmen 2021 stetig zu. Dies hängt mit der zunehmenden Digitalisierung zusammen, da im Rahmen der Umstellung auf neue Systeme, z. B. im Bereich der Videoüberwachung und Parkplatzbewirtschaftung, zunehmend Personendaten bekannt zu geben sind bzw. digital erfasst werden. Die für eine materielle Beurteilung der Anfragen vorzunehmenden Sachverhaltsabklärungen können dabei für die Datenaufsicht teilweise mit grossem Aufwand verbunden sein. Erwähnenswert ist in dem Zusammenhang die Datenschutzbeschwerde samt Aufsichtsbeschwerde einer Privatperson betreffend Zustellung eines Zahlungsbefehls an eine vermeintliche geschäftliche E-Mail-Adresse.

Zum Sachverhalt
Gemäss Schilderung des Bürgers habe das betreffende Betreibungsamt eine E-Mail unautorisiert an eine «Dienstadresse» gesendet. Dass diese E-Mail-Adresse zu einem Gemeinschaftspostfach führt, sei gemäss Betreibungsamt nicht unmittelbar ersichtlich gewesen, da ebendiese personalisiert war. In der besagten Mail wurde mitgeteilt, dass ein Zahlungsbefehl offenstehe, es wurden fünf (5) Varianten der Kontaktaufnahme vorgeschlagen, mitunter als «ultima ratio» der Polizeieinsatz am Arbeitsort angekündigt. Durch den Umstand, dass es sich hierbei angeblich um eine Gemeinschafts-Inbox handelte, wurde die E-Mail von weiteren unautorisierten Personen gelesen. Da die Umstände, die in dieser E-Mail dargestellt wurden, geeignet waren, den Ruf zu schädigen, wenn Drittbeteiligte dies mitbekommen, handelt es sich um eine Bearbeitung von Personendaten, die ein Risiko für die Persönlichkeitsrechte des Betroffenen begründen könnte. Im Ergebnis lag somit eine Bekanntgabe von besonderen Personendaten im Sinne von § 17 Abs. 1 lit. b IDG vor. Die Datenaufsicht hat allerdings in Abklärung mit dem besagten Betreibungsamt die Datenbearbeitung zur Erfüllung «gesetzlicher Aufgaben» i. S. d. § 17 Abs. 2 IDG feststellen können.

Bewertung der Sachlage

Die Stellungnahme des besagten Betreibungsamtes hat die Datenaufsicht erhalten und im kontinuierlichen Dialog geprüft. Darin wird ausgeführt, dass die nochmalige Einladung zur Abholung an die Geschäftsadresse ein geringeres Risiko für die Persönlichkeitsrechte darstellte als die im Schuldbetreibungs- und Konkursrecht formell gesetzlich verankerten Handlungsmassnahmen: (i) Zustellung der Urkunde an die Geschäftsadresse durch Weibel/in oder (ii) Polizei sowie (iii) öffentliche Publikation mit breitem Wirkungskreis. Dies insbesondere deshalb, da es sich im Gegensatz zur allgemeinen anonymisierten E-Mail-Adresse (z. B. info@xmail.com) um eine private/persönliche Geschäfts-Adresse handelte. Der Personenkreis mit Zugriff auf eine solche Sammeladresse ist üblicherweise auf wenige Schlüsselpersonen beschränkt, um die Vertraulichkeit zu gewährleisten. Daher erscheint das Argument des Betreibungsamtes als durchaus schlüssig bzw. plausibel, dass nicht damit gerechnet werden musste, dass nach mehrfach erfolglosen Zustellversuchen mehr Personen Kenntnis vom Inhalt erlangen würden, als bei einer (i) Geschäftszustellung via Polizei am Arbeitsplatz oder (ii) öffentlichen Publikation. Das Betreibungsamt war formell gesetzlich befugt, die Zustellungsart im Ermessen der Verhältnismässigkeit und Erforderlichkeit vorzunehmen, was es auch tat, indem es ein milderes Mittel wählte, als die Zustellung vor Ort via Polizei. Die Zustellmassnahme via E-Mail, die nicht gekennzeichnet war, ist aus datenschutzrechtlicher Perspektive als verhältnismässig einzustufen. Folgerichtig erachtete die Datenaufsicht das Vorgehen im Hinblick auf das Datenschutzrecht als durchaus vertretbar. Ein Datenschutzverstoss durch eine etwaige unbefugte Offenlegung und/oder einen unbefugten Zugang zu personenbezogene Daten war nicht ersichtlich. Inwiefern dadurch andere gesetzliche Vorschriften verletzt wurden, wie etwa der SchKG-Wirkungskreis, konnte die Datenaufsicht mangels Zuständigkeit nicht beurteilen.

Schlussfolgerung

Eine Datenschutzbeschwerde per se sieht das IDG nicht vor, die Datenschutzstelle hat indes die Möglichkeit, eine Untersuchung einzuleiten, um künftig die korrekte Bearbeitung von Personendaten sicherzustellen. Beide Datenschutzbeauftragte (2021) haben diesbezügliche Abklärungen mehrfach vorgenommen und das Betreibungsamt noch stärker sensibilisiert. Der Bürger selbst hat gemäss § 21 IDG das Recht, vom Betreibungsamt zu verlangen, das etwaige widerrechtliche Bearbeiten von Personendaten zu unterlassen, die Folgen des widerrechtlichen Bearbeitens zu beseitigen oder die Widerrechtlichkeit des Bearbeitens festzustellen. Da die Bekanntgabe der Betreibung an Kolleginnen und Kollegen sowie damit zusammenhängende Umstände beim Arbeitgeber bereits erfolgt sind und die Kenntnisnahme nicht mehr rückgängig gemacht werden kann, blieb Anfang Jahr lediglich die Möglichkeit der Feststellung einer widerrechtlichen Datenbearbeitung offen. Eine Widerrechtlichkeit der erfolgten Bekanntgabe wie oben ausgeführt konnte nicht festgestellt werden, weder seitens Betreibungsamt durch eigene interne Überprüfung noch seitens Datenaufsicht der Stadt Winterthur.

Melde- und Abwicklungsprozess Datenschutzverletzungen

Öffentliche Organe müssen Datenschutzvorfälle unverzüglich melden – soweit eruirbar, wenn die Grundrechte auf informationelle Selbstbestimmung beziehungsweise auf Privatsphäre der betroffenen Personen gefährdet sein könnten. Ein Datenschutzvorfall liegt vor, wenn personenbezogene Daten unwiederbringlich vernichtet werden, verloren gehen, unbeabsichtigt oder unrechtmässig verändert oder Unbefugten zugänglich gemacht werden. In zwei Fällen wurden nicht nur personenbezogene Daten, sondern auch sensible Daten Unbefugten zugänglich gemacht.

Ein Datenschutzvorfall muss gemeldet werden, wenn er zu einer Gefährdung der Grundrechte auf informationelle Selbstbestimmung beziehungsweise auf Privatsphäre von betroffenen Personen führen kann. Bestehen Zweifel, ob Grundrechte gefährdet sind, ist ebenfalls Meldung zu erstatten. Die Bestimmung über die Meldepflicht ist mit dem revidierten IDG am 1. Juni 2020[5] in Kraft getreten. Eine Meldung an die Aufsichtsbehörde hat bei einer Datenschutzverletzung immer zu erfolgen. Ausnahme: Die Datenpanne führt «voraussichtlich nicht zu einem Risiko» für den Betroffenen. Eine betroffene Person muss nur benachrichtigt werden, wenn ein hohes Risiko für ihre Rechte und Freiheiten besteht. Neben der Meldefrist, nämlich unmittelbar ab Kenntnisnahme, gibt es bestimmte Inhalte, die die Meldung an die zuständige Aufsichtsbehörde berücksichtigen muss, mitunter eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze. Können die Informationen nicht zur gleichen Zeit bereitgestellt werden, können sie ohne unangemessene weitere Verzögerung schrittweise zur Verfügung gestellt werden. Es zeigt sich: Sich auf eine Meldefrist allein zu konzentrieren, reicht nicht aus. Es ist notwendig, den kompletten Meldeprozess zu überprüfen und anzupassen. Der verantwortliche Fachbereich muss jede Datenschutzverletzung dahingehend überprüfen, ob die Datenpanne «voraussichtlich nicht zu einem Risiko» für den Betroffenen führt. Und das nicht nur bei einer Datenpanne mit besonders sensiblen Daten. Die Datenaufsicht wird ab Juli 2022 ein internes Merkblatt zur Verfügung stellen. Verwaltungsintern sollte im Intranet die Möglichkeit geschaffen werden, dass sich Mitarbeitenden darüber informieren können, wie im Falle eines Datenschutzvorfalles vorzugehen ist.

Prüfung Erlass einer neuen Verordnung «Parkieren Winterthur» – Velostationen

Mit dem Erlass einer neuen Verordnung «Parkieren Winterthur» soll für den bestehenden Eigenwirtschaftsbetrieb eine saubere rechtliche Grundlage in Form eines generell-abstrakten Erlasses geschaffen werden. Neu soll auch der Betrieb von Velostationen in den Eigenwirtschaftsbetrieb integriert werden. Dadurch kann auf ein Synergiepotenzial bei den Parkhäusern zurückgegriffen werden.

Die Datenaufsicht wurde mit der Bitte um Prüfung ersucht, ob es sich im vorliegenden Fall der Bereitstellung von Veloabstellplätzen um eine Teilnahme am wirtschaftlichen Wettbewerb i. S. v. § 2 Abs. 2 IDG handelt bzw. ob dem gewählten Vorgehen – Beizug Swiss-Pass der SBB – datenschutzrechtliche Bedenken im Weg stehen.

[5] Datenschutzvorfälle sind zu melden, wenn die Grundrechte von betroffenen Personen gefährdet sind (§ 12a Abs. 1). § 12a Abs. 2 und 3 IDG regeln die Information an die betroffenen Personen.

Geltungsbereich IDG

Ein öffentliches Organ fällt nicht in den Anwendungsbereich des IDG, soweit es am (i) wirtschaftlichen Wettbewerb teilnimmt und dabei (ii) nicht hoheitlich handelt. Beide Voraussetzungen müssen kumulativ vorliegen. Ziel dieser Bestimmung ist es, öffentliche Organe, die ihre Leistungen in Konkurrenz mit anderen privaten Personen am Markt anbieten, nicht durch spezifische, auf den öffentlich-rechtlichen Sektor ausgerichteten Bestimmungen zu Datenschutz so einzuschränken, dass allenfalls ein Wettbewerbsnachteil entstehen könnte. Ob ein öffentliches Organ am wirtschaftlichen Wettbewerb teilnimmt, ist aufgrund einer Gesamtbetrachtung zu entscheiden. Als Kriterien sind diverse Beurteilungsparameter seitens Datenaufsicht kommuniziert worden.

Hinweis bzgl. Anwendbarkeit DSG-Bund: Der Gesetzgeber geht davon aus, dass mit dem Ausschluss eines öffentlichen Organs aus dem Geltungsbereich des IDG automatisch das DSG-Bund zur Anwendung kommt. Dies ist allerdings nicht offensichtlich, da das DSG-Bund nur für private Personen und Bundesorgane gilt, weshalb öffentlich-rechtlich organisierte Organe des Kantons nach Wortlaut als Datenbearbeiter nicht darunterfallen. Dass sie hingegen privatrechtlich handeln, davon muss in weiter Auslegung des DSG-Bund und unter Berücksichtigung der konkreten Umstände ausgegangen werden, sodass sie folglich in den Wirkungskreis ebendieser fallen. Die Frage ist nicht nur für das öffentliche Organ von Bedeutung, da es wissen muss, nach welchen Bestimmungen es sich zu richten hat, sondern auch für die betroffenen Personen in Bezug auf die Geltendmachung ihrer Rechte, da ein Verfahren sich hier nach dem Zivilrecht richtet. Die datenschutzrechtliche Aufsicht müsste dann durch den EDÖB sichergestellt werden.

Schlussfolgerung
IDG ist gemäss obgenannten Kriterien in der Gesamtheit kumulativer Beurteilungskriterien anwendbar.

SwissPass – anhaltende Datenschutz-Problematik und -Risiken

Der neue SwissPass geriet frühzeitig im Hinblick auf den Datenschutz unter hohe Kritik. Beispielsweise hiess es 2016, die Sammlung der Daten (Big Data) ermögliche es zu jeder Zeit, ein Bewegungsprofil (Profiling/Tracking) von Kundinnen und Kunden zu erstellen. Das potenzielle Bewegungsprofil von Fahrradfahrern bleibt somit kritisch im Wirkungskreis des Datenschutzes zu betrachten. Wenn die Velo-App mit der SwissPass-Kalibrierung in einer gemeinsamen Schnittstelle münden, werden unmittelbar nach der Datenerhebung und vor der weiteren Verarbeitung IP-Adressen gesammelt. Pseudonymisierungs- und Anonymisierungsanforderungen sollten überprüft werden bei der technischen Datenschutzumsetzung («Privacy by Design/Default»-Anforderungen). Wenn die letzten drei Stellen der IP-Adresse gelöscht und die Informationen so anonymisiert werden, sind die Datenschutzrechtlichen Anforderungen konform abgefangen. Wenn keine Verknüpfung der IP-Adresse via Velo-App mit anderen Informationen via SwissPass erfolgt, die eine Identifikation und/oder Commerce-Tracking von Besuchern ermöglichen, so ist der Data-Governance-Zyklus nicht mit dem Risiko behaftet, Betroffenenrechte zu verletzen. Diese Kalibrierungen müssten in den Nutzungsbedingungen und in der Datenschutzerklärung der Velo-App nachzulesen sein.

Schlussfolgerung
Die Datenaufsicht steht der Verknüpfung der Velo-App mit dem SwissPass-Kanal punktuell leicht kritisch gegenüber. Datensicherheit (Bewegungs-Profiling stark ausgeprägt) und Datenschutztransparenz würden dem Datenminimierungs-Grundsatz entgegenstehen. Ob genügend Transparenz im Bereich der Datensammlung und Datenbearbeitung via SwissPass/EDÖB erreicht wurde, kann meinerseits nicht abschliessend bestätigt werden.

Arbeitsrechtliche Datenschutzberatung

Umgang mit Covid-19-bedingt erfassten Gesundheitsdaten von Mitarbeitenden

Aufgrund der aktuellen Pandemie sind Personalämter vermehrt mit datenschutzrechtlichen Fragestellungen in Zusammenhang mit dem Umgang von Gesundheitsdaten ihrer Mitarbeitenden konfrontiert. Konkret ging es um die Frage, ob und wie bspw. positive Covid-19-Testresultate, behördliche Anordnungen zur Quarantäne/Isolation, Abrechnungen zu Erwerbsersatzentschädigungen und Impfzertifikate in Zusammenhang mit Corona im Personaldossier zu behandeln sind, und ob diese im Personaldossier abgelegt und aufbewahrt werden müssen.

Ich beschränke mich auf eine von zehn beantworteten Fragen vom letzten Jahr zum Thema positive Covid-19-Testresultate. Hierbei stellen sich zwangsläufig die Fragen, (i) ob Arbeitgeber Tests anordnen können, (ii) ob sie Anspruch darauf haben, das Testergebnis zu erfahren und (iii) wie mit den Testergebnissen aus datenschutzrechtlicher Sicht umzugehen ist. Auch wenn der Arbeitgeber Corona-Tests zur Verfügung stellt, sind die Mitarbeitenden nicht zwangsläufig dazu verpflichtet, diese Tests durchzuführen. Bei Corona-typischen Symptomen darf der Arbeitgeber allerdings einen Corona-Test anordnen, da die allgemeine Fürsorgepflicht des Arbeitgebers es bei konkretem Verdacht einer möglichen Ansteckung zum Schutz der anderen Beschäftigten gebietet. Ohne konkreten Anlass können Arbeitgebende in der Schweiz ihre Mitarbeitenden in der Regel nicht verpflichten, einen Corona-Schnelltest durchzuführen. Wenn Mitarbeitende sich einem Corona-Selbsttest unterziehen, schliesst sich die Frage an, ob sie das Ergebnis – insbesondere dann, wenn es positiv ist – ihrem Arbeitgebenden melden müssen. Das BAG vertritt derzeit noch die Auffassung, dass «keine Verpflichtung [besteht], den Arbeitgeber über das Testergebnis zu informieren».

Diese Ansicht hält die Datenaufsicht für sehr bedenklich und im Ergebnis widersinnig, denn Sinn und Zweck der Testangebotspflicht und weitergehender Teststrategien in den Unternehmen ist es gerade, etwaig infizierte Mitarbeitende zu identifizieren und so zu isolieren, dass eine Ansteckung weiterer Personen im Arbeitsumfeld und darüber hinaus verhindert wird. Wenn Arbeitnehmerinnen und Arbeitnehmer nicht gehalten sind, ihre positiven Testergebnisse dem Arbeitgebenden zu melden, können diese ihrer Fürsorgepflicht gegenüber allen Mitarbeitenden nicht nachkommen; die Testangebotspflicht läuft ins Leere. Dem Arbeitgeber muss folglich in diesem Zusammenhang ein Auskunftsrecht auf Grundlage der Wahrnehmung der Fürsorgepflicht zustehen. Auch aus Sicht der Mitarbeitenden muss man meines Erachtens nach zu dem Ergebnis kommen, dass die Mitteilung eines positiven Selbsttests im Rahmen der arbeitsvertraglichen Nebenpflicht verpflichtend sein muss, denn die Mitarbeitenden sind unter anderem gehalten, die Arbeitsschutzmassnahmen zu begleiten, soweit ihnen dies möglich und zumutbar ist. Hierzu zählt auch, der Ansteckung mit übertragbaren Krankheiten entgegenzuwirken.

5. Internes

Zusammenarbeit mit anderen Datenschutzbehörden und Verbänden schweizweit

Privatim, die Konferenz der schweizerischen Datenschutzbeauftragten, ist insbesondere für schwach dotierte Behörden von grosser Wichtigkeit und grossem Nutzen. In regelmässigen Abständen beschäftigt sich der Fachverband mit aktuellen Themen. Die Exponenten von Privatim stehen im Austausch mit den Anbietern von IT-Lösungen (z. B. Microsoft) und setzen sich für einheitliche schweizweit gültige Lösungen ein. Daneben werden für eine breite Bevölkerungsschicht Leitfäden und Merkblätter erarbeitet (zu nennen ist etwa das «Merkblatt über Cloud-spezifische Risiken und Massnahmen»), Vernehmlassungen verfasst und Resolutionen verabschiedet. Privatim gibt dem Datenschutz eine Stimme und fördert den Informations- und Wissensaustausch unter den Datenschutzbeauftragten. Die Datenschutzbeauftragte der Stadt Winterthur nahm 2021 an zwei Privatim-Veranstaltungen teil.

Vernehmlassungen und Mitberichte

Im Berichtsjahr 2021 äusserte sich die Datenschutzbeauftragte im Rahmen von zwei Mitberichtsverfahren, namentlich zu den Ausführungsbestimmungen zur Informationsverordnung und zur Vernehmlassung zum Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG). Eine weitere Stellungnahme der Datenaufsicht wurde zum Geschäft «Städtische Wohnpolitik: Wohnmonitoring» erarbeitet.

Interne Schulungen

Im Berichtsjahr nahm die Datenschutzbeauftragte an den üblichen Einführungsveranstaltungen für neue Kader-Mitglieder der Stadtverwaltung teil. Des Weiteren ist ein Online-Schulungsangebot in Arbeit.

Ausblick 2022/2023

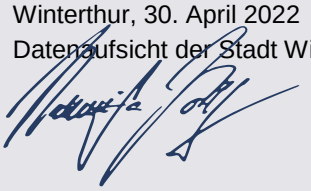
Zurzeit findet ein Datenschutzaudit statt, wobei ein Schlussbericht per Ende Juli 2022 zu erwarten sei.

Persönliche Dankesworte

Mein Dank gilt im ersten Berichtsjahr der gesamten Winterthurer Stadtverwaltung und auch allen Mitgliedern der Aufsichtskommission, insbesondere Herrn AK-Präsident Felix Helg, für die stets sehr angenehme und konstruktive Zusammenarbeit. Für die tatkräftige Unterstützung beim Start danke ich ebenso allen Mitarbeiterinnen und Mitarbeitern der Staatskanzlei, besonders Herrn Parlamentsschreiber Marc Bernhard.

Abschliessend gebührt auch Ihnen, werte Leserin, werter Leser, der Dank für Ihr Interesse an einem umsetzbaren Datenschutz. Es ist davon auszugehen, dass der Datenschutz auch in den kommenden Jahren weiterhin eine hohe Bedeutung haben wird. Es besteht zweifellos ein hohes Interesse, dass die Persönlichkeitsrechte der betroffenen Personen weiterhin geschützt werden. Dies kann aber nicht nur durch eine einzelne Stelle geschehen, sondern bedarf weiterhin der bewussten Mitwirkung jedes Einzelnen bei der Bearbeitung von Personendaten. Danke, dass Sie sich um die Einhaltung des Datenschutzes kümmern!

Winterthur, 30. April 2022
Datenaufsicht der Stadt Winterthur



Narcisa Wolf
Datenschutzbeauftragte der Stadt Winterthur

6. Anhang

Thematische Übersicht – Auszug

Im Berichtsjahr legte die Datenschutzbeauftragte auf Anfragen von Behörden und Privatpersonen hin in den folgenden Themenfeldern neue Geschäfte und Aktivitäten an:

- Anfrage Cloud-Lösung, ECM-Ausschreibung
- Beantwortung von Bürgeranfragen: Parkplatzuhren mit Erhebung des Kfz-Kennzeichens
- Beratung beim Wechsel der Lehrstelle, Einsicht Praktikumsberichte
- Beratung betreffend App-Projekt (smartes Kollaborationstool für die Soziale Arbeit)
- Beratung betreffend Personalakte: Arbeitszeugnisse, Aufbewahrungspflichten und Fristen
- Beratung betreffend Projekt Naturfundbüro, Datenbank Naturmuseum Winterthur
- Beratung PAKAPO-Projekt
- Beratung Videoüberwachungsmassnahmen Bibliotheken
- Beratung Weitergabe digitaler Schülerdossiers
- Beratung DaZ-Unterricht: Datenschutzbestimmungen, Erarbeitung eines Merkblatts für Schulen
- Beurteilung, Jugendanwaltschaft Winterthur: Untersuchung einer Straftat mittels Editionsverfügung
- Beurteilung betreffend «Paralleldatenbank», Polizeibussen
- Datenschutzrechtliche Beratung betreffend Datenweitergabe bzw. Datentransfer via Timify
- Datenschutzrechtliche Beratung betreffend generelle Bevollmächtigung zum Datenaustausch mit Drittstellen und generelle Entbindung von der Schweigepflicht
- Datenschutzrechtliche Beurteilung einer Zufriedenheitsbefragung
- Erarbeitung einer Auditstrategie und eines Auditprozesses samt Pensumerhöhung
- Gesuch Freischaltungen Content-Filter
- Gesuch um Daten aus dem Steuer-Pool Privatunternehmen
- Gesuch um Informationen für nicht personenbezogene Zwecke, statistikrelevant
- Gesuch um Informationen für nicht personenbezogene Zwecke zwecks Unternehmensbefragung
- Gesuche und Vorabkontrollen von Videoüberwachungsmassnahmen
- Kontrollen behördliche Sorgfaltspflichtverletzung, Meldung Datenschutzvorfälle
- Prüfung Datenauszug für Neukunden-Akquise, Privatunternehmen
- Prüfung der Anforderungen für den digitalen Bestellvorgang beim medizinischem Verbrauchsmaterial
- Sozial Monitoring, Steuer- und Sozialdaten, Gesuch um Informationen für nicht personenbezogene Zwecke
- Stellungnahme betreffend Datenbekanntgabe von Stadtwerk an Serviceprovider / Telekom-Verordnung
- Stellungnahme Vorabkontrolle Stadtwerk Winterthur, CRM-Lösung
- Stellungnahme zu Konzept Schnittstelle Eigentum-Baumkataster
- Vernehmlassung zum Entwurf zur Totalrevision der VDSG, Stadtkanzlei
- Videokamera und Parkplatzüberwachung, Gewerbe
- Videoüberwachung Abfallproblematik
- Videoüberwachung Privatgrund
- Videoüberwachungsreglement Schwimmbad-Genossenschaft
- Vorabkontrolle der Einführung von School Fox bei den Schulen der Stadt Winterthur
- Weiterleitung an Kanton: Bienenimport aus EU-Ländern, Akteneinsichtsgesuch
- Zugang zu behördlichen Informationen
- Zugriff auf Mitarbeitenden-Outlook-Postfach bei Abwesenheit im Krankheitsfall
- Zugriff auf Web-Info-Center, SBB-Tageskarten, Datenaustausch innerhalb Verwaltungseinheiten.

Statistik

Bearbeitungsstand der Geschäfte per 31. Dezember 2021

Jahr	Eingänge	Erledigungen	Pendent	Total bearbeitet
2011	75	59	16	75
2012	59	54	21	75
2013	80	65	36	101
2014	68	58	46	104
2015	64	66	44	110
2016	75	59	60	119
2017	77	71	66	137
2018	83	73	66*	149
2019	111	80	97	177
2020	116	76	137	213
2021	83	73	10	83
Total	**890**	**733**	**10***	**1242****

Kein Geschäft in Verzug.-
* 10 Geschäfte wurden auf 2022 verlagert bzw. auf die Kontrollliste gesetzt, inkl. Datenschutzaudit.
** Über ein Drittel der Geschäfte wurde über mehrere Jahre hinweg bearbeitet.

Übersicht Geschäfte Datenschutzbeauftragte 2021 (Erfassung)

Auflistung aller Geschäfte mit Erfassungsdatum (Persistierung in Datenbank) zwischen 01.01.2021 und 31.12.2021 (unabhängig, ob Geschäft offen ist, erledigt oder sistiert wurde wie auch unabhängig vom Sachbearbeiter).

Quelle: Geschäftskontroll-Datenbank Stadt Winterthur