Winterthur, 8. Mai 2023
Parl.-Nr. 2023.36

Stadt Winterthur

Tätigkeitsbericht 2022
Datenaufsicht Stadt Winterthur

Digitale Selbstbestimmung | Verwaltung im Wandel

Vertrauen ist ein Schlüsselfaktor für den Erfolg der Digitalisierung, denn es bildet die Grundlage für die Zusammenarbeit und die Schaffung einer stabilen und sicheren digitalen Infrastruktur. Vertrauen ist auch wichtig, um sicherzustellen, dass die Digitalisierung die Bedürfnisse der Menschen erfüllt und nicht zu ihrer Benachteiligung oder Diskriminierung beiträgt. Ohne Vertrauen in die Sicherheit und Integrität der Datenbearbeitungsprozesse kann die Digitalisierung ihre erstaunlichen Vorteile nicht voll ausschöpfen.

Narcisa Wolf, Datenschutzbeauftragte

An das Stadtparlament Winterthur

Sehr geehrter Herr Präsident Diener
Liebe Kolleginnen und Kollegen
Liebe Leserinnen und Leser

Ich freue mich, Ihnen den Tätigkeitsbericht der Datenaufsicht der Stadt Winterthur, Berichtsperiode 1. Januar 2022 bis 31. Dezember 2022 zu unterbreiten. Nach einem Überblick über die allgemeinen Grundlagen für die Arbeit der Behörde gehe ich näher auf folgende Punkte ein:

- Aufgaben der Datenaufsicht bzw. der Datenschutzbeauftragten
- ausgesuchte Dossiers aus der Praxis
- zwei Schwerpunktthemen im Zeitalter der Digitalisierung
- Schlussbemerkungen zu Interna samt Ausblick 2023

Mit vorzüglicher Hochachtung
Winterthur, 5. Mai 2023

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 2022. Veröffentlicht wird der Bericht auf der Webseite der Datenaufsicht der Stadt Winterthur: Link.

§ 10 Verordnung über die/den Datenschutzbeauftragten/n der Stadt Winterthur
Der oder die Datenschutzbeauftragte erstattet dem Parlament jährlich Bericht über seine bzw. ihre Tätigkeit: Link.

Inhaltsverzeichnis

I. Zusammenfassung 4
II. Die Datenaufsicht der Stadt Winterthur stellt sich vor....5
III. Fälle aus der Praxis: ausgewählte Dossiers....6
IV. Schwerpunktthema: Microsoft 365....11
V. Schwerpunktthema: Auditprogramm....12
VI. Interne Zusammenarbeit mit anderen Datenschutzbehörden und Verbänden schweizweit 13
VII. Interne Schulungen 13
VIII. Ausblick 2023/2024 13
IX. Impulse 13
X. Antrag 14
Anhang **A**: Statistische Auswertungen……..14
Anhang **B**: Abkürzungsverzeichnis und Glossar:……..……15

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

Quelle Titelbild
© Stadtverwaltung Winterthur

Layout
www.tollkirsch.ch

Grusswort

Der Tätigkeitsbericht 2022 ist der zwölfte der Behörde und der zweite in meiner Amtszeit. Er steht im Zeichen des präventiven Datenschutzes in Krisenzeiten und neuer Wertschöpfung durch die fortschreitende Digitalisierung in Winterthur. Auch der Datenschutz-Audit (Seite 12) dürfte zu einer besseren Verankerung des Datenschutzes beitragen.

Vorwort

Das Thema digitale Selbstbestimmung[1] war 2022 allgegenwärtig. Das Konzept der digitalen Selbstbestimmung gewinnt in der heutigen vernetzten Welt immer mehr an Bedeutung, da immer mehr Daten über uns gesammelt werden und diese oft für kommerzielle oder politische Zwecke eingesetzt werden. Wir alle sind Konsumentinnen und Konsumenten, auch in der digitalen Welt, und identifizieren uns als solche im Alltag vermehrt mit unseren Daten-Aktiva. Über deren Nutzung entscheiden wir als Dateneigner nicht immer selbstbestimmt. Vertrauenswürdige Datenräume und Datenkanäle unterschiedlicher Verwaltungseinheiten sollen, auf Basis unserer direkt-demokratischen Werte, Bürgerinnen und Bürger befähigen, ihre Daten selbstbestimmt zu navigieren. Zwischen Datensammlerinnen und -sammlern sowie Nutzniesserinnen und Nutzniessern digitaler Medien besteht oftmals eine Informationsasymmetrie, die es den Nutzerinnen und Nutzern zunehmend erschwert, selbstbestimmte Entscheidungen bei der Verwendung digitaler Medien zu treffen bzw. selbstbestimmt im digitalen Umfeld zu handeln[2]. 2022 war auch anderweitig ein aktives Jahr: Im März hat der Regierungsrat des Kantons Zürich einen Entscheid zu Microsoft 365 gefällt. Mit Beschluss vom 8. Juni 2022 hat die Zürcher Regierung zudem die Direktion der Justiz und des Innern ermächtigt, das Vernehmlassungsverfahren für die Totalrevision des Gesetzes über die Information und den Datenschutz (IDG) durchzuführen. Positiv lässt sich festhalten, dass in vielen Verwaltungsstellen die Sensibilisierung für Fragen des Datenschutzes hoch bleibt.

I. Zusammenfassung

Vermehrt ist die Datenschutzbeauftragte in Prozessabläufe eingebunden, die typischerweise datenschutzrechtlicher Abklärungen bedürfen. Dazu gehören beispielsweise die Beschaffung neuer Software, Tooling, die Auslagerung von Informatikdienstleistungen oder die Einführung neuer digitaler Systeme samt Rechtsberatung. Die frühzeitige Einbindung bewirkt, dass datenschutzrechtlich sensible Projekte bereits in der Pilot- oder Planungsphase beurteilt werden können, was Zeit, Kosten und Aufwand einspart. Vielfach fanden Beratungsgespräche im Beisein von Vertreterinnen und Vertretern der jeweiligen Partnerfirmen statt, da diese einerseits über das Knowhow verfügen, um sensible Fragen zu beantworten, und anderseits die vereinbarten Massnahmen direkt (mit) umsetzen konnten. Die Datenschutzbeauftragte war zwar nicht umfassend, aber ausreichend in relevante Abläufe der Verwaltung integriert, um bei wichtigen Fragen rechtzeitig konsultiert zu werden.

Begleitung von Projekten/Vorabkontrollen

Im Berichtsjahr 2022 wurden der Datenschutzbeauftragten mehrere Projekte erneut zur Vorprüfung vorgelegt. Mehrere Informationssicherheits- und Datenschutzkonzepte (ISDS-Konzepte) sind geprüft worden bzw. weiterhin in Bearbeitung. Die Datenschutzbeauftragte prüfte mitunter die Rechtmässigkeit und Verhältnismässigkeit von Scolaris, Schoolfox, Microsoft 365 und diversen digitalen Vorhaben. Darüber hinaus wirkte sie beratend bei einem Open-Data-Governance-Projekt mit. Der Einsatz von Videoüberwachungsmassnahmen erfordert, wie bereits 2021, einen unverändert hohen Beratungsaufwand.

Präventiver Datenschutz 2022 gestärkt durch die Revision des IDG

Einer der zukunftsweisenden Ansätze des Datenschutzes ist der präventive Datenschutz. Die Datenschutzbeauftragte hat den präventiven Datenschutz mittels Vorabkonsultationen innerhalb der Verwaltung kontinuierlich umgesetzt und wird dies konsequent im laufenden Jahr fortsetzen. Die aktuelle Revision des IDG stärkt den präventiven Datenschutz durch die Verpflichtung öffentlicher Stellen, Datenschutz-Folgenabschätzungen (nachfolgend DSFA) für datenschutzrelevante Projekte zu erstellen.

Präventiver Datenschutzaudit durch Stadtparlamentsbeschluss

Die Datenaufsicht erarbeitete 2021 eine Datenschutzstrategie, auf Basis derer 2022 ein Auditprogramm in Angriff genommen wurde. Die für den Datenschutz sachlich zuständige Aufsichtskommission und die Datenaufsicht einigten sich im Oktober 2021 darauf, das Arbeitspensum während drei Monaten in 2022 um 15 Prozent zu erhöhen, damit das vom Stadtparlament gewünschte Datenschutzaudit parallel zum Tagesgeschäft durchgeführt werden konnte. Das Audit diente als Pre-Indikator für die Digitalisierungsvorhaben der Verwaltung. Die Datenaufsicht hat am 1. März 2022 die Arbeit aufgenommen. Ein Dank gilt dem Vermessungsamt bzw. der Fachstelle Geoinformation für das entgegengebrachte Vertrauen und die gute Zusammenarbeit (siehe Schwerpunktthema).

[1] Bericht des UVEK und des EDA an den Bundesrat: Schaffung von vertrauenswürdigen Datenräumen basierend auf der digitalen Selbstbestimmung – Link.
[2] Grimm Petra/Krah Hans (2014): Ende der Privatheit? Eine Sicht der Medien- und Kommunikationswissenschaft.
Grimm, P./Krah, Hans (2016): Privatsphäre. In: Heesen, J. (Hrsg.), Handbuch Informations- und Medienethik. Stuttgart, S. 178–185.

II. Die Datenaufsicht[3] der Stadt Winterthur stellt sich vor

Im Kanton Zürich ist der durch die öffentlichen Organe zu gewährleistende Datenschutz in erster Linie im IDG[4] geregelt. Eine agile Datenaufsicht ist unerlässlich, um die Vertraulichkeit, Integrität und Verfügbarkeit von Datenbearbeitungen sicherzustellen und das Risiko von Datenschutzverletzungen zu minimieren. Die Aufsichtsstelle hat zum Ziel, sicherzustellen, dass personenbezogene Daten rechtmässig, verhältnismässig und transparent verarbeitet werden und dass die Datenschutzrechte der betroffenen Personen gewahrt bleiben. Es gibt jedoch bestimmte Aufgaben, die eine Datenaufsicht nicht übernehmen kann:

- **Rechtliche Vertretung:** Eine Datenschutzbeauftragte kann die Organisation in Datenschutzfragen beraten, aber sie kann die Organisation nicht rechtlich vertreten.
- **Alleinige Entscheidungen treffen:** Die Datenaufsicht kann Empfehlungen aussprechen, aber sie kann keine Entscheidungen im ausschliesslichen Alleingang treffen.
- **Verstoss gegen andere Zuständigkeiten:** Eine Datenaufsichtsstelle sollte nicht in Konflikt mit anderen Zuständigkeiten innerhalb der Organisation geraten.
- **Aufsichtsbehörden oder Gerichte ersetzen:** Eine Datenschutzbeauftragte kann die Organisation bei der Zusammenarbeit mit Aufsichtsbehörden unterstützen, aber sie kann diese nicht ersetzen.

Die städtische Datenaufsicht muss grundsätzlich dieselben Aufgaben übernehmen wie die kantonale Datenaufsicht, da diese in den Gemeinden mit kommunaler Datenaufsicht nur die Oberaufsicht[5] ausübt. Entsprechend hält die Verordnung über die/den Datenschutzbeauftragten/n der Stadt Winterthur vom 30. August 2010 (SRS 3.1-1) in Art. 2 Abs. 1 fest, dass die oder der Datenschutzbeauftragte der Stadt Winterthur die Aufgaben des oder der Beauftragten für Datenschutz gemäss kantonaler Gesetzgebung über die Information und den Datenschutz wahrnimmt[6]. Die Datenaufsicht der Stadt Winterthur hat demzufolge die Aufgaben gemäss § 34 IDG zu erfüllen:

- Beratung der öffentlichen Organe in Fragen des Datenschutzes und der Datensicherheit
- Beratung von Privatpersonen über ihre Rechte
- Monitoring der Anwendung der Vorschriften über den Datenschutz
- Vermittlung zwischen betroffenen Personen und öffentlichen Organen bei Streitigkeiten betreffend den Datenschutz
- Information der Öffentlichkeit über Anliegen des Datenschutzes
- Beurteilung von Erlassen und Vorhaben, die den Datenschutz betreffen
- Aus- und Weiterbildungen in Fragen des Datenschutzes
- Eine weitere Aufgabe ergibt sich aus § 10 IDG, wonach die Datenaufsicht eine Vorabkontrolle einer beabsichtigten Personendatenbearbeitung vornehmen muss, wenn das zuständige öffentliche Organ im Rahmen der DSFA zum Schluss kommt, dass besondere Risiken für die Grundrechte der betroffenen Personen bestehen[7].

a. Unterstützung und Beratung der öffentlichen Organe in Fragen des Datenschutzes (§ 34 lit. a IDG)
Die Beratung und Unterstützung öffentlicher Organe beinhalten ein breites Spektrum an Tätigkeiten der Beauftragten (siehe Anhang A/B). Die Beratungstätigkeit wird meistens in Form einer persönlichen Sprechstunde und/oder online wahrgenommen sowie durch die Beantwortung jeder Anfrage mittels schriftlicher Stellungnahmen. Die Unterstützung kann eine Hilfestellung im Einzelfall oder auch die Mitwirkung in einer Projektgruppe umfassen, aber auch aus einer Vermittlung an die richtige Stelle bestehen. Im Jahr 2022 hat die Datenaufsicht nebst 28 interne Managementaufgaben 57 komplexe Beratungen, 3 Projekt Begleitungen, und 23 vertiefte Anfragen sowie 2 einfache Auskünfte von öffentlichen Organen durchgeführt bzw. erledigt.

b. Überwachung der Anwendung der Vorschriften über den Datenschutz (§ 34 lit. c IDG)
Die Aufgabe beinhaltet einerseits ein Monitoring und ein generelles Beobachten der Datenbearbeitungen durch die öffentlichen Organe. Anderseits ist die Überprüfung von konkreten Datenbearbeitungen vorzunehmen. Erhält die Datenaufsicht einen konkreten Hinweis, so hat sie die Pflicht, eine entsprechende Kontrolle durchzuführen. Die Datenaufsicht hat 32 Beurteilungen im Jahr 2022 vorgenommen. Ausserdem sind 7 Kontrollen im Zusammenhang mit Datenschutzverletzungsmeldungen bzw. Warnungen durchgeführt worden.

c. Vermittlung zwischen betroffenen Personen und öffentlichen Organen bei Streitigkeiten betreffend den Datenschutz (§ 34 lit. d IDG)
Die Vermittlungsfunktion nimmt die Datenschutzbeauftragte im Ermessen wahr. Die Vermittlung zwischen einem öffentlichen Organ und einer betroffenen Person durch die Datenaufsicht bei Streitigkeiten betreffend den Datenschutz kann von einer Privatperson oder von einem öffentlichen Organ verlangt werden. In diesem Fall nimmt die Datenschutzbeauftragte ihre Vermittlungsfunktion neutral wahr.

[3] Gemäss RRB Nr. 3304/1996 sind die Städte Zürich und Winterthur zur Führung einer eigenen Datenaufsicht verpflichtet.
[4] § 33 Abs. 1 IDG sieht vor, dass die Gemeinden eigene Datenschutzbeauftragte bestellen können und dass der Regierungsrat Gemeinden mit mindestens 50k Einwohnerinnen und Einwohnern dazu verpflichten kann, eine eigene Datenschutzbeauftragte oder einen eigenen Datenschutzbeauftragten zu bestellen.
[5] Glaser, a.a.O., § 33 N. 10.
[6] Vgl. dazu auch Weisung zur Verordnung über die/die Datenschutzbeauftragten/n der Stadt Winterthur vom 30. August 2010, Antrag des Stadtrates vom 16. Juni 2010, S. 2.
[7] Vgl. dazu auch § 24 Abs. 1 Verordnung über die Information und den Datenschutz (IDV, LS 170.41).

d. Beurteilung von Erlassen und Vorhaben, die den Datenschutz betreffen (§ 34 lit. f IDG)
Bei der Beurteilung von Erlassen und Vorhaben, die den Datenschutz betreffen, handelt es sich bereits nach den bundesrechtlichen Vorgaben [8] um eine Sorgfaltspflicht, die vollumfänglich wahrgenommen wird. Die Datenaufsicht hat 6 Stellungnahmen samt 3 Berichte vorgenommen.

e. Information der Öffentlichkeit über Anliegen des Datenschutzes (§ 34 lit. e IDG)
Der gesetzliche Auftrag zur Öffentlichkeitsarbeit ist breit formuliert. Er dient der Sensibilisierung der Öffentlichkeit. Mit welchen Mitteln die Informationsaufgabe erfüllt wird, ist im IDG nicht näher umschrieben, allerdings ist ein relativ grossen Ermessensspielraum zu bejahen. Sie bedient sich medialer Instrumente wie etwa Interviews oder neutralen Stellungnahmen in den Medien zum konkreten Fall. Die Datenaufsicht hat diesbezüglich 4 Dossiers erledigt.

f. Beratung von Privatpersonen
Wenden sich Privatpersonen mit Fragen an die Datenaufsichtsstelle, führt dies oft zu umfangreichen Abklärungen, auch im Hinblick auf Zuständigkeiten und die Weiterleitung an den Kanton, gegebenenfalls an den Bund. Solche «Anstösse von aussen» haben einen positiven Synergie-Effekt. Die Datenschutzbeauftragte dankt an dieser Stelle allen Personen, die mit ihrer Anfrage wichtige Prozessprüfungen angeregt haben. Die Datenaufsicht hat 38 Geschäftsfälle in 2022 erledigt.

g. Datenschutzmanagement
Internes Auditprogramm
Ein Datenschutzaudit ist eine freiwillige Prüfung der Datenschutzkonformität der Verwaltungsstellen, die Daten bearbeiten. Die Audits stärken zudem das Vertrauen von Bürgerinnen und Bürgern, Kundschaft, Partnern und Mitarbeitenden in der Stadtverwaltung. Eine Auditstrategie und ein erster Auditprozess wurden im Herbst 2021 etabliert sowie 2022 ausgeführt. Er diente dazu, den Ist-Zustand hinsichtlich Erfassung, Speicherung, Löschung, Archivierung und Weitergabe personenbezogener Daten im Geoinformationsbereich des Vermessungsamtes festzustellen. Das Audit umfasste Beratungsgespräche, Dokumentenprüfungen und Untersuchungen der Systeme und Prozesse. Basierend auf den Ergebnissen wurden Massnahmen vorgeschlagen und Handlungsempfehlungen (Aktionskatalog) ausgesprochen, die zu einem idealen Soll-Zustand in der Verwaltungseinheit führen.

h. Angebot von Aus- und Weiterbildungen in Fragen des Datenschutzes (§ 34 lit. g IDG)
Das Angebot von Aus- und Weiterbildungen zu Fragen des Datenschutzes stellt eine vom kantonalen Recht vorgegebene Pflicht der Datenaufsicht dar. Es muss sichergestellt werden, dass der Datenaufsicht ein gewisser Spielraum belassen wird, um unabhängig entscheiden zu können, welche Aus- und Weiterbildungen notwendig sind. Die Datenaufsicht hat 9 Schulungen bzw. Beratungen im Kontext von Kaderschulungen vorgenommen.

i. Datenschutzmanagement: Risikoabschätzung mittels Vorabkontrolle
Die Datenaufsicht hat 6 Geschäftsfälle vorgenommen (vgl. dazu auch Beurteilungen). Eine Vorabkontrolle gemäss IDG ist ein Verfahren, das Fachbereiche der Verwaltung durchführen müssen, bevor sie personenbezogene Daten verarbeiten. Die Vorabkontrolle ist eine Risikobewertung und umfasst eine umfassende Analyse der Datenverarbeitung, einschliesslich der Art und Weise, wie die Daten gesammelt, gespeichert, gestreut und gelöscht werden. Ziel der Vorabkontrolle ist es, Schwachstellen aufzudecken und Massnahmen zu ergreifen, um das Risiko einer Datenschutzverletzung zu minimieren. Die Risikoabschätzung ist somit ein wichtiger Bestandteil des Datenschutzmanagements. Zudem ergeben sich auch Konkretisierungen zur Vorabkontrolle aus der IDV, sprich auf Verordnungsstufe (30-Tage Frist, vgl. § 24 Abs. 3 IDG).

j. Zusammenfassung der Tätigkeit der Datenaufsicht
Zusammenfassend ist festzuhalten, dass die gesetzlichen Aufgaben der Datenaufsicht, die sich aus den Vorgaben des übergeordneten Rechts ergeben, relativ umfassend und klar bestimmt sind. Dabei ist stets darauf zu achten, dass die Unabhängigkeit der Datenaufsicht im Sinne von § 33 Abs. 3 IDG gewährleistet ist. Abschliessend ist darauf hinzuweisen, dass Winterthur gemäss RRB Nr. 3304/1996 dazu verpflichtet ist, eine den Vorgaben des kantonalen Rechts ausreichende Datenaufsicht nachzuweisen.

III. Fälle aus der Praxis: ausgewählte Dossiers

Kategorie 1: Unterstützung und Beratung der öffentlichen Organe in Fragen des Datenschutzes

Pensionskassen
Die Datenaufsicht wurde zur Abklärung und Stellungnahme gebeten, welches Datenschutzgesetz für öffentliche Pensionskassen (nachfolgend PK) gilt. PK verarbeiten eine grosse Menge an personenbezogenen Daten von Versicherten. Dabei kann es zu unerwünschten Datenverknüpfungen kommen. Der Umgang mit diesen Daten kann eine potenzielle Verletzung der Privatsphäre und anderer Datenschutzrechte darstellen. Welches Datenschutzgesetz gilt, ergibt sich daraus, wer die konkreten Daten bearbeitet. Im obligatorischen Bereich von privaten PK und denjenigen des Bundes gilt das Bundes-DSG mit seinen Bestimmungen für die Datenbearbeitung durch Bundesorgane, für die öffentlichen

[8] Vgl. Art. 31 Abs. 1 lit. b DSG

PK von Kantonen und Städten das jeweilige kantonale Datenschutzgesetz. Die öffentlichen PK von Kantonen oder Städten sind nach Art. 48 Abs. 2 BVG Vorsorgeeinrichtungen des öffentlichen Rechts mit eigener Rechtspersönlichkeit. Auch sie vollziehen das BVG, werden damit allerdings nicht zu Bundesorganen. Sie bleiben kantonale (bzw. kommunale) öffentliche Organe. Damit gilt im obligatorischen Bereich für ihre Datenbearbeitung das jeweilige kantonale Datenschutzgesetz. Falls die Pensionskasse der Stadt Winterthur (PKSW) als öffentliches Organ des Kantons Zürich zu qualifizieren ist, ist sie dem IDG unterstellt, andernfalls dem DSG. Falls die PKSW dem IDG untersteht, sind einzig die Bestimmungen des IDG anwendbar. Eine Protokollierung wird auch vom IDG gefordert (§ 7 IDG) und die DSFA ist in § 10 Abs. 1 IDG ebenfalls vorgesehen. Die PKSW muss alle Bestimmungen des IDG beachten, da sie diesem Gesetz untersteht.

Aktenvernichtung

Die Datenaufsicht wurde aufgesucht bezüglich Entsorgung von alten Papier- Patientendaten. (älter als 20 Jahren). Die konkreten Fragen bezogen sich auf die Schredder- bzw. Entsorgungsprozesse solcher Daten. Bei der Aktenvernichtung ist der Datenschutz von entscheidender Bedeutung, da es darum geht, personenbezogene Daten zu schützen. Gemäss IDG/IDV bedarf es für eine angemessene Datensicherheit der Umsetzung entsprechender technischer und organisatorischer Massnahmen. Hier sind einige wichtige Punkte, die geprüft wurden: Auswahl des richtigen und geeigneten Dienstleisters, Art der Löschung bzw. Vernichtung, Vertraulichkeitsvereinbarungen, Nachweis der Vernichtung. Als Orientierung kamen auch die Anforderungen der ISO 27001 und ISO 27002 zum Zug. Für eine datenschutzkonforme Aktenvernichtung greift seit Oktober 2012 die sog. DIN-Einstufung 66399. Diese gibt sieben Sicherheitsstufen vor - die sog. Kleinteiligkeit geschredderter Akten: Je höher die Schutzklasse betroffener Informationen, desto höher die zu wählende Schutzstufe. Akten, die personenbezogene Daten enthalten, müssen mindestens unter Sicherheitsstufe 3 (z. B. Personaldaten, Bewerbungsunterlagen) bzw. 4 (z. B. Patientendaten, Kanzleiakten) vernichtet werden.

Kategorie 2: Vermittlung zwischen betroffenen Personen und öffentlichen Organen bei Streitigkeiten betreffend den Datenschutz (§ 34 lit. d IDG)

Sozialhilfegelder und Datenschutz

Die Datenaufsicht wurde aufgesucht mit der Fragestellung, ob beim Sozialhilfebezug alle privaten Konten zwingend angegeben werden müssen und wie der Datenschutz in einem solchen Fall Schranken setzt. Im Wesentlichen gibt es zwei Aspekte zu beachten: den Datenschutz des Leistungsempfängers und den Datenschutz der Leistungsbehörde. Zum Schutz des Leistungsempfängers dürfen personenbezogene Daten nur erhoben, verarbeitet und genutzt werden, soweit dies zur Erfüllung der Sozialhilfeleistung erforderlich ist. Im Kanton Zürich wird die Sozialhilfe durch die Sozialhilfebehörden der Gemeinden und der Stadt Zürich geführt. Der Anspruch auf Sozialhilfe wird individuell geprüft und richtet sich nach dem Einkommen und Vermögen der betreffenden Person. Die Rechtslage hat der Kanton Zürich in den sogenannten SKOS-Richtlinien [9] für verbindlich erklärt. Auch das kantonale Sozialhilfegesetz enthält die Bestimmung zur Auskunftspflicht. Die Auskunfts- und Meldepflichten beziehen sich unter anderem auf Einkommens- und Vermögensverhältnisse, samt Verpflichtungen der materiellen Grundsicherung. Zusammenfassend gilt: Der Datenschutz im Zusammenhang mit einem Sozialhilfebezug und Auskunftspflichten ist ein wichtiger Aspekt, der von beiden Seiten beachtet werden muss. Die Leistungsbehörde muss die Daten vertraulich behandeln und darf nur die für die Beurteilung der Sozialhilfeleistung notwendigen Daten erheben und nutzen. Die Leistungsempfängerin respektive der Leistungsempfänger muss die erforderlichen Daten offenlegen, darf aber auf den Schutz der Daten vertrauen.

Kategorie 3: Beratung Privatperson

Verletzung Amtsgeheimnis vs. Datenschutzverletzung

Die Datenaufsicht wurde aufgesucht, um die Sachlage bezüglich einer potenziellen Datenschutz- bzw. Amtspflichtverletzung im Rahmen einer Lehrtätigkeit einzuordnen. Während eine Amtspflichtverletzung eine Verletzung der allgemeinen Pflichten eines Amtsträgers darstellt, bezieht sich eine Datenschutzverletzung auf die Verletzung spezifischer Datenschutzgesetze und -vorschriften. Eine Amtspflichtverletzung kann jedoch eine Datenschutzverletzung einschliessen, wenn sie die Vertraulichkeit oder Integrität personenbezogener Daten betrifft, die im Rahmen der öffentlichen Verwaltung verarbeitet werden. Eine Amtspflichtverletzung bezieht sich auf eine Handlung oder Unterlassung eines öffentlichen Amtsträgers, die gegen seine gesetzlichen Pflichten verstösst. Obwohl beide Verletzungen unterschiedlich sind, können sie sich durchaus überschneiden, was es nicht gerade einfach macht, schnell zu reagieren. Eine entsprechende Schulung oder Beratung hat die Datenschutzbeauftragte bezüglich beider Instrumente vorgenommen.

Potenzielle Observation Subjekt Arbeitsplatz

Die Datenaufsicht wurde aufgesucht, um eine komplexe Situation mit Observationscharakter am Arbeitsplatz zu begutachten. Der Fall wurde an die kantonale Datenschutzbeauftragte weitergeleitet. Eine Observation am Arbeitsplatz kann dann unrechtmässig sein, wenn sie die Persönlichkeitsrechte der Arbeitnehmerin oder des Arbeitnehmers verletzt. Das bedeutet, dass der Arbeitgeber bestimmte Datenschutzvorschriften einhalten muss, um sicherzustellen, dass die Privatsphäre und die Persönlichkeitsrechte der Arbeitnehmer gewahrt bleiben.

[9] Vgl. § 17 Sozialhilfeverordnung Kanton Zürich (Kapitel A.4.1.)

Im Allgemeinen ist eine Observation dann unzulässig, wenn sie ohne Zustimmung des Arbeitnehmers erfolgt oder, wenn sie über das hinausgeht, was erforderlich ist, um legitime Geschäftsinteressen zu schützen. Zum Beispiel kann eine verdeckte Videoüberwachung am Arbeitsplatz unter bestimmten Umständen zulässig sein, wenn der Arbeitgeber ein berechtigtes Interesse hat, seine Mitarbeitenden und das Unternehmen vor Diebstahl, Betrug oder anderen strafbaren Handlungen zu schützen. Es ist jedoch wichtig zu beachten, dass der Einsatz von Überwachungsmassnahmen am Arbeitsplatz strengen rechtlichen Anforderungen unterliegt. Arbeitgeber sollten daher immer sicherstellen, dass sie die geltenden Datenschutzbestimmungen einhalten und die Mitarbeitenden darüber informieren, welche Daten zu welchem Zweck erhoben werden.

Kategorie 4: Vorabkontrolle und Datenschutz-Folgenabschätzungen

Zivilstandsamt Winterthur

Die Datenaufsicht ist zur Vorkonsultation samt Datenschutz-Folgenabschätzung betreffend digitales Tooling ersucht worden. Das Zivilstandsamt wünschte eine cloudbasierte Reservierungs- und Buchungssoftware einzuführen, die von Unternehmen, Organisationen und Einzelpersonen genutzt werden kann, um online Buchungen und Reservierungen zu verwalten. Im konkreten Fall sollte das Tool Brautpaaren zur Verfügung gestellt werden, damit sie künftig ihren Wunsch-Trautermin selbständig online reservieren können. Die Vorabkontrolle durch die Datenaufsicht ist von der Prüfung hinsichtlich Informationssicherheit zu unterscheiden, wobei momentan auf beiden Seiten die sogenannte «Illegalität» des Cloud Acts[10] festzustellen sei. Die Auswirkung auf die Nutzerinnen und Nutzer wäre, dass Daten, die in der Cloud gespeichert sind, durch die US-Strafverfolgungsbehörden gezielt abgerufen oder durchsucht werden «könnten». Besonders und hoch sensibel am Cloud Act ist, dass es den Cloud-Anbietern ausdrücklich untersagt ist, ihre Nutzerinnen und Nutzer zu informieren, sollte es zu einer Abfrage durch die Behörden kommen. Das Recht auf Benachrichtigung ist allerdings als «informationelle Selbstbestimmung» in der Schweiz fest verankert. So oder so wird gegen den potenziellen Zugriff durch auswärtige Behörden einzig eine starke Verschlüsselung[11] wirken. Dadurch mag der Inhalt eines Cloud-Speichers zwar immer noch zugänglich, sprich «einsehbar» sein, aber die Dateien enthalten nur Krypto-Zeichenketten – eine Auswertung der Dateien ist dadurch nicht mehr möglich. Daher empfiehlt die Datenschutzbeauftragte zwingend den Einsatz einer Ende-zu-Ende-Verschlüsselung. Zusätzlich ist es sinnvoll, ausschliesslich europäische bzw. Schweizer Cloud-Speicheranbieter in der Verwaltungsinfrastruktur zu implementieren.

Website Stadtwerk Winterthur

Die Datenaufsicht wurde ersucht, die Notwendigkeit einer Vorabkontrolle für das Projekt «Neue Website Stadtwerk Winterthur» auf deren Vereinbarkeit mit den Anforderungen an den Datenschutz und die Informationssicherheit zu prüfen. Drei der grössten Datenschutzrisiken in Web-Applikationen 2022 sind Schwachstellen in den (i) Anwendungen, (ii) Datenlecks auf Seiten der Betreiber und (iii) unzureichende Reaktionen auf Datenpannen. Es war daher zwingend notwendig genau zu wissen, was auf der Homepage und auch dahinter (auf dem Webserver, im CMS, sogar im verwendeten Thema, sowie in allen genutzten Plug-Ins, samt Bibliotheken) passiert. Wenn diese Informationen vollständig und korrekt vorliegen, können inhaltlich korrekte Datenschutzhinweise erstellt werden. Für die Datenschutz-Compliance einer Website stellen Webtracking-Dienste oder sog. Plugins ebenfalls eine Herausforderung dar und datenschutzrechtlicher Sicht problematisch. Durch die Einbindung können nämlich die Betreiber der Social-Media-Netzwerke über eine direkte Verbindung zu den Seitenbesuchern Daten, sprich Profile (Link) erheben. Auch wenn die Rechtslage bezüglich der Einbindung dieser Plugins nicht eindeutig geklärt ist, warnt die Datenschutzbeauftragte ausdrücklich davon, dass sie rechtlich bedenklich bleiben. Hier sind einige Aspekte, die mitunter geprüft wurden: Informationspflichten, Einwilligungsmanagement, Technische Massnahmen, Rechte der betroffenen Personen, Auftragsverarbeitung, Datenschutzerklärung.

Edulog

Die Datenaufsicht wurde aufgesucht, um eine Vorkonsultation bezüglich Edulog zu prüfen. Die Datenschutzbeauftragte hat eine Vorabkontrolle und Datenschutz-Folgenabschätzung begleitet. Obwohl Edulog darauf ausgelegt ist, den Zugang zu Online-Diensten zu vereinfachen und zu sichern, können immer noch Informationssicherheitsrisiken (technischer Datenschutz) auftreten. Die Datenschutzbeauftragte beriet vor allem zur systematischen Verwendung der AHV-Nummer (nachfolgend AHVN). Die Aufnahme der AHVN birgt gewisse Risiken, die primär in der Möglichkeit der Verknüpfung verschiedener Datenbestände besteht. Mit Blick auf die Zielsetzungen der Revision des AHV-Gesetzes (AHVG) soll die AHVN systematisch verwendet werden, um kostenintensive Verwaltungsfehler zu verhindern, mehr Effizienz dank automatisiertem Datenaustausch zwischen den Behörden zu ermöglichen und Verwechslungen zu vermeiden[12]. Es wurde vorgeschlagen, dass zwar die AHVN wie vorgesehen als Teil einer E-ID geführt werden darf, dass aber im Gesetz – zum Beispiel in Art.

[10] Der Cloud Act (Clarifying Lawful Overseas Use of Data Act) ist ein US-amerikanisches Gesetz, das 2018 verabschiedet wurde und Auswirkungen auf die Verwaltung von Daten durch Cloud-Dienstleister hat. Das Gesetz ermöglicht den US-Behörden den Zugriff auf Daten von US-amerikanischen Unternehmen, die auf Servern ausserhalb der USA gespeichert sind, wenn diese Daten für Ermittlungen im Rahmen von Strafverfahren benötigt werden.

[11] Eine starke Verschlüsselung zeichnet sich dadurch aus, dass es sehr schwierig ist, die verschlüsselten Daten ohne Kenntnis des richtigen Entschlüsselungsschlüssels zu lesen oder zu verändern. Die Stärke einer Verschlüsselung hängt auch davon ab, wie gut der Algorithmus und die Schlüssel geschützt sind, um Angriffe zu verhindern.

[12] Botschaft zur Änderung des Bundesgesetzes über die Alters- und Hinterlassenen Versicherung I Systematische Verwendung der AHV-Nummer durch Behörden; BBl 2019 7359, 7376.

16 VE-BGEID – ausdrücklich festgehalten wird, dass sie mit Hilfe von technischen Massnahmen nur jenen Verifikatoren zugänglich gemacht werden darf, für die grundsätzlich die rechtlichen Grundlagen für die systematische Verwendung gemäss AHVG gegeben sind und private Verifikatoren somit keinen Zugang haben. Damit soll der ungehinderten Verbreitung an private Verifikatoren, welche die E-ID verwenden, vorgebeugt werden. Sollte eine technische Massnahme nicht möglich sein, ist man der Ansicht, dass die AHVN nicht in der E-ID geführt werden sollte. Die Arbeit an konforme Lösungen sind diesbezüglich noch im Gange.

Schoolfox
Auch diesbezüglich wurde die Datenschutzbeauftragte für eine Vorabkontrolle konsultiert. Schoolfox ist eine Plattform, die entwickelt wurde, um die Kommunikation zwischen Schulen und Eltern weiter zu vereinfachen. Die Kommunikation kann Namen, E-Mail-Adressen, Anwesenheitsdaten, Noten und Leistungsberichte, die für den Schulbetrieb relevant sind, beinhalten. Die Datenaufsicht führte enge Vorabklärungen in der Form einer DSFA durch, bot Beratung auf Vertragsebene samt AGBs an, prüfte die Datenflussmatrix, die technischen als auch die organisatorischen Massnahmen und sprach Empfehlungen aus. Auf Schoolfox sollen nur die nötigsten bzw. zweckgebundene Daten geteilt werden. Die Sicherheit von Schoolfox ist ein elementarer Aspekt, da die Plattform sensible Informationen des Schulalltags enthält. Eine der Empfehlungen ist, dass die Zwei-Faktor-Authentifizierung zwingend sichergestellt wird. Durch die Einführung dieser zusätzlichen Sicherheitsebene wird das Risiko von Accounts, die wegen schwacher und/oder gestohlener Passwörter kompromittiert werden, minimiert. Bis dahin sollen weder Geburtsdatum noch das Attribut Nationalität erfasst werden. Diese Daten sind für die Nutzung von Schoolfox nicht zwingend erforderlich. Dadurch sind ein Datenverzicht bzw. eine Dateneinschränkung zeitlich zumutbar. Die Stadt hat sich für ein Produkt entschieden, das Profiling – die automatisierte Verarbeitung personenbezogener Daten – vermeidet. Insgesamt kann man beruhigt sagen, dass Schoolfox eine sichere Plattform ist.

Kategorie 5: Beurteilung von Erlassen und Vorhaben (§ 34 lit. f IDG) IDG-Totalrevision
Mit Beschluss Nr. 203/2022 vom 4. März 2020 verabschiedete der Regierungsrat des Kantons Zürich das Konzept der Totalrevision des IDG. Am 8. Juni 2022 ermächtigte der Regierungsrat die Direktion der Justiz und des Innern, eine Vernehmlassung zum Entwurf für eine Totalrevision des IDG durchzuführen. Die Datenschutzbeauftragte der Stadt Winterthur erhielt die Gelegenheit, zum Entwurf für die Totalrevision der IDG-Stellung zu nehmen. Sie begrüsst, dass mit dem vorliegenden Entwurf das Öffentlichkeitsprinzip gestärkt werden soll. Mit der Schaffung einer Aufsicht erhielten neben der kantonalen Verwaltung auch die Gemeinden sowie die Bürgerinnen und Bürger eine zentrale Anlaufstelle für Datenschutz und Öffentlichkeitsprinzip, was die Wahrnehmung ihrer Rechte transparent gestaltet.

Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)
Die Datenaufsicht der Stadt Winterthur begrüsst die neue Initiative zur Einführung eines elektronischen Identitätsnachweises (E-ID) auf der Basis einer staatlich betriebenen Infrastruktur und den Grundsätzen des Schutzes der Privatsphäre durch Technik (Privacy by Design), der Datensparsamkeit und der dezentralen Datenspeicherung. Zu den wichtigsten Bestimmungen aus datenschutzrechtlicher Sicht zählt mitunter die Verwendung der AHV-Nummer (Art. 2 Abs. 3 Bst. a VE-BGEID). In den Erläuterungen wird nicht ersichtlich, weswegen die AHV-Nummer enthalten sein muss. Der Zweck des Gesetzes in Art. 1 Abs. 2 Bst. a VE-BGEID, die sichere Identifizierung mittels E-ID unter Privaten und mit Behörden zu gewährleisten, könnte auch ohne die AHV-Nummer erreicht werden.

Workshop zur Erarbeitung der Nationale Cyberstrategie (NCS)
Die Datenschutzbeauftragte nahm am NCS-Workshop teil. Die Cybersicherheit hat auf allen Ebenen an Bedeutung gewonnen. Sie ist ein Schlüsselelement der Sicherheitspolitik, unabdingbare Voraussetzung und Chance für den Wirtschafts- und Forschungsstandort sowie ein zentraler Faktor der digitalen Verwaltungspolitik. Eine erfolgreiche Cybersicherheitsstrategie erfordert das Verständnis der neuesten Bedrohungen, Risikobewertungen, angemessene Schutzmassnahmen sowie die Schulung und Sensibilisierung der Nutzerinnen und Nutzer. Der Steuerungsausschuss des Nationalen Zentrums für Cybersicherheit (National Cyber Security Centre NCSC[13]) hat die Verantwortlichkeiten zur Erarbeitung der neuaufgelegten Strategie festgelegt. Im Jahr 2022 hat sich das NCSC zusammen mit Vertreterinnen und Vertretern der Kantone, der Hochschulen und der Wirtschaft der Erarbeitung der Neuauflage gewidmet.

Kategorie 6: Meldung von Datenschutzverletzungen
Datenschutzverletzung Impfzentrum
Die Datenaufsicht wurde im Zusammenhang mit einer potenziellen Belästigung, resultierend aus einer Datenschutzverletzung in einem Impfzentrum, aufgesucht. Eine angestellte Person hat sich dem System bedient, um an vertrauliche Daten einer Kundin heranzukommen. Die Datenschutzbeauftragte wurde um Rat bezüglich Anzeige, Kündigung, Imageschaden und möglich Schritte gebeten. Der Sachverhalt liess sich wie folgt einordnen: Gelangt man zur Ansicht, dass hier die Betroffene widerrechtlich in ihrer Persönlichkeit verletzt worden sei, kann sie mit einer Zivilklage dagegen vorgehen. In diesem Zusammenhang ist eine Anzeige bei der Polizei von Vorteil. Für eine Verletzung der Privatsphäre kann man sich an den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) wenden. Dieser berät Bürgerinnen und Bürger, Unternehmen und

[13] Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken

private Organisationen. Er beaufsichtigt die Datenbearbeitungen ebendieser. Beanstandungen bearbeitet das EDÖB unter Berücksichtigung der Schwere der Persönlichkeitsverletzung und der Anzahl betroffener Personen. Anderseits kann der Beauftragte dann einschreiten, wenn die Inhaber von Datensammlungen die Grundsätze des Datenschutzes nicht einhalten. Bei Einzelfällen obliegt es der betroffenen Person, zivilrechtlich gegen die Persönlichkeitsverletzung vorzugehen (Kontaktformular EDÖB: hier.)

Einsatz von Drohnen durch die Polizei – Drohnenabsturz

Die Baupolizei in der Luzerner Gemeinde Horw wollte zum Beispiel mittels Drohnen feststellen, ob illegale Bauten erstellt worden sind. [14] Durch unbemannte Luftfahrtsysteme im Sinne des Luftverkehrsgesetzes kann man einen erheblichen Mobilitätsgewinn erzielen und wäre in der Lage, biometrische Daten zu erheben. Bei der Datenaufsicht ist mit Verzögerung eine Meldung einer potenziellen Datenschutzverletzung durch einen Drohnenverlust eingetroffen. Die Datenschutzbeauftragte hat die Datenschutzverletzung mit vollumfänglicher Unterstützung der Verantwortlichen geprüft und rechtlich als kritisch, aber nicht akut eingeordnet. Das Problem des Einsatzes einer Drohne ist, dass es sich dabei nicht einfach um eine Weiterentwicklung der Videoüberwachung mittels Kamera handelt, sondern «einen intimeren Blick auf das Geschehen erlaube, ohne dass notwendigerweise ersichtlich ist, von wo die Aufnahme gemacht wird». Das ist datenschutzrechtlich leicht anders zu gewichten. Wir begegnen hier einer echten Herausforderung, denn es ist nicht immer eindeutig, schnell und klar kommuniziert, wer von wem und von wo aus mit einer Drohne filmt. Nicht nur die informationelle Selbstbestimmung ist damit auf die Probe gestellt, sondern auch die Versammlungsfreiheit. Darum empfiehlt die Datenschutzbeauftragte, Drohnenaufnahmen auf «mit hoher Wahrscheinlichkeit strafrechtlich relevantes Verhalten» zu konzentrieren und lückenlos zu dokumentieren. Bei hochaufgelösten Aufnahmen einer Kundgebung von oben können aber Personendaten erhoben werden, die keinen strafrechtlichen Zusammenhang haben. Als Sofortmassnahme muss eine Drohne bei Verlust aus der Ferne gesperrt werden können, um sicherzustellen, dass kein Datenzugang durch Dritte möglich ist. Einige Risiken, die geprüft worden sind und zu einer entsprechenden Anpassung des Meldeprozesses geführt haben: Verlust von Daten, Missbrauch von Daten, Verlust von Hardware, Ausnutzung von Schwachstellen, Beeinträchtigung des Ansehens, Technologie-Schwachstellen und Rechte der Betroffenen. Der Verlust der Drohne könnte auch das Ansehen der Polizei, ja sogar der Verwaltung insgesamt beeinträchtigen, wenn der Eindruck entsteht, dass die Lage nicht beherrscht wird und Technologien nicht sicher verwaltet und geschützt werden. Die Datenaufsicht hat diesbezüglich eng beraten. Anpassungen wurden datenschutzkonform vorgenommen.

Kategorie 7: Überwachung der Anwendung der Vorschriften über den Datenschutz (§ 34 lit. c IDG)

reCaptcha-Sicherheitsverfahren

Der Datenaufsichtspüfung ging eine Bürgermeldung voraus, die den Einsatz von Google reCaptcha und einen Datenverlust bemängelte. Die Datenschutzbeauftragte startete umgehend eine Sicherheitsüberprüfung. Zusammen mit IDW-Verantwortlichen wurden mehrere Lösungen ausgelotet. reCaptcha ist ein Sicherheitstool, das von Google entwickelt wurde, um automatisierte Bot-Angriffe auf Websites zu verhindern. Dabei wird überprüft, ob die Nutzerin oder der Nutzer ein Mensch oder ein Bot ist, indem verschiedene Kriterien wie Klickverhalten, IP-Adresse oder Bewegungsmuster ausgewertet werden. In Bezug auf den Datenschutz gibt es bei der Verwendung von reCaptcha einige Aspekte zu beachten. Denn Google nutzt die Datenauswertung, um das Sicherheitssystem von reCaptcha zu verbessern und Angriffe besser erkennen zu können. Zum anderen ist es möglich, dass bei der Verwendung von reCaptcha auch personenbezogene Daten von Nutzerinnen und Nutzern erfasst werden. Die Datenschutzbeauftragte prüfte zusammen mit der IDW alternative Sicherheitstools, die weniger personenbezogene Daten erfassen und verarbeiten. Die jetzige Lösung ist datenschutzfreundlicher, sprich datenschutzkonform.

Videoüberwachung mittels KI

Die Datenschutzbeauftragte beriet zum Einsatz von KI-Modulen, die innerhalb einer aktiven Videoüberwachungsmassnahme eingesetzt werden sollten, um das Logistikumfeld einer Baustelle intelligenter zu steuern. Systeme der algorithmischen Entscheidungsfindung bergen Risiken, die mit dem Einsatz ebendieser einhergehen und so eine rechtliche Regulierung[15] in den Vordergrund rücken. Die Idee, KI-Systeme a priori einer Risikokategorie zuzuordnen, ist insofern problematisch, als dadurch die Faktoren Zweck und Kontext der Anwendung eines Systems nicht im Einzelfall berücksichtigt werden können. Um die Praktikabilität eines KI-Ansatzes zu gewährleisten, hat die Datenschutzbeauftragte mittels Datenschutz-Folgenabschätzung etwaige Risiken geprüft. In einem ersten Schritt führte man eine Triage durch, die es erlaubte, Risikosignale zu erkennen, die sich vor Ort mittels Videoüberwachung und KI ergeben würden. Je mehr Risikosignale bezüglich des Einsatzes des noch unreifen KI-Systems erkannt wurden, desto umfassender wurden die Transparenzpflichten, denen die entsprechenden Akteure unterworfen worden wären. Der Auftraggeber entschied sich letztendlich gegen den Einsatz eines KI-Models, weil es noch nicht einsatzreif war. Stattdessen wurde ein einfacher Sensormechanismus gewählt.

Ordnungsbusse und Einsichtnahme in Blitzerfotos

Die Datenaufsicht wurde kontaktiert, um die Sachlage bezüglich Zugangsgewährung zum Beweisfoto einzuordnen und einen richtungsweisenden Zugangsprozess zu initiieren. In Winterthur wird in Zukunft eine Einsichtnahme bzw.

[14] Siehe Urteil: hier.

[15] Am 21. April 2021 hat die Europäische Kommission ihren Entwurf für eine Verordnung zur Künstlichen Intelligenz vorgelegt, bei dem es sich um die weltweit erste rechtlich bindende horizontale Regulierung von KI-Systemen handeln würde. Sie hat damit sowohl politisch ein Zeichen gesendet als auch substanziell einen Standard gesetzt. Der KI-Verordnungsentwurf wird derzeit im Europäischen Parlament und im Rat der EU behandelt.

Aushändigung des Fotos möglich sein. Die Veröffentlichung von Blitzerfotos/Beweisfotos ist nicht einheitlich geregelt und kann je nach Kanton und Gemeinde unterschiedlich gehandhabt werden. Auch wenn datenschutzrechtliche Vorschriften in vielen Bereichen der Datenverarbeitung Grenzen setzen – das IDG schützt nicht vor den Folgen eines Blitzerfotos, denn es lässt Ausnahmen zu und öffnet die Privacy-Schranken. Im Allgemeinen gelten folgende Bestimmungen:

- **Verwendung durch Behörden:** Blitzerfotos können von den zuständigen Behörden zur Verfolgung von Verkehrsverstössen bzw. Ordnungswidrigkeiten jederzeit verwendet werden.
- **Verwendung durch Dritte:** Die Veröffentlichung von Blitzerfotos durch Dritte, zum Beispiel durch Medien oder auf Social-Media-Plattformen, ist in der Regel nicht erlaubt. Hierbei handelt es sich um eine Verletzung der Persönlichkeitsrechte der betroffenen Personen.
- **Auskunftspflicht der Behörden:** Auf Anfrage können die zuständigen Behörden Auskunft über den Verlauf des Verfahrens geben und gegebenenfalls Blitzerfotos zur Verfügung stellen bzw. diese beschreiben.
- **Datenschutzmanagement:** Personenbezogene Daten dürfen lediglich zum Zwecke der Verfolgung der Ordnungswidrigkeit genutzt werden und müssen nach Beendigung des Bussgeldverfahrens nachweislich gelöscht werden.
- **Einschränkungen:** Es ist wichtig zu beachten, dass der Zugang zu Blitzerfotos auch mit gewissen Einschränkungen verbunden sein kann. So ist es zum Beispiel möglich, dass ein Blitzerfoto nur für eine begrenzte Zeit zur Verfügung steht oder dass es nur bestimmten Personen zugänglich ist.

Microsoft 365

Microsoft sammelt Daten von Nutzerinnen und Nutzern seiner Produkte und Dienste. Diese Daten können persönliche Informationen wie Name, E-Mail-Adresse, Standort, Suchanfragen und Nutzungsverhalten enthalten. Es gibt Bedenken, dass Microsoft die gesammelten Daten nicht nur für einen homogenen Zweck verwendet, sondern auch für andere Zwecke wie Werbung und Marktforschung. Microsoft hat jedoch in den letzten Jahren grosse Anstrengungen unternommen, um diese Datenschutzprobleme zu beheben.

Aufzeichnung und Abhören von Telefondaten und Funkverkehr

Die Datenaufsicht hat auf Anraten den Prozess der Dienstanweisung «Aufzeichnung und Abhören von Telefondaten und Funkverkehr» der Stadtpolizei überprüft. Zur Optimierung der Prozesse wurden Empfehlungen eingepflegt. Festzuhalten sei, dass das Abhören von Telefongesprächen grundsätzlich verboten ist (Art. 179bis StGB). Die systematische Erstellung von Kommunikationsprofilen anhand etwaiger Randdaten ist ebenfalls unzulässig. Hingegen dürfen Randdaten zur Kontrolle von Weisungen betreffend den Telefonverkehr und für Abklärungen bei Verdacht auf «schwerwiegende Pflichtverletzungen» verwertet werden. Mitunter empfahl die Datenaufsicht: Der Zeitpunkt des Einbezugs der Mitarbeiterin oder des Mitarbeiters soll so früh wie möglich erfolgen, soweit dies im Einklang mit operativ-strategischen Entscheidungen steht. Alle Mitarbeitenden sind über mögliche Kontrollen/Stichproben vorgängig zu informieren. Generelle Hinweise in den Allgemeinen Anstellungsbedingungen würden nebst einer Anpassung der Dienstanweisung genügen. Die Datenschutzbeauftragte empfahl dringend kommunikativ begleitete Schulungen und Ernstfallproben, die mindestens einmal jährlich durchgeführt werden.

IV. Schwerpunktthema: Microsoft 365

Microsoft 365 (nachfolgend M365) ist ein cloudbasiertes bei diesen Vertragsverhandlungen war, welche Dienste unbedenklich inkludiert werden können. Ein Beispiel sei erwähnt: «Customer Lockbox».

Customer Lockbox

Customer Lockbox ist eine Sicherheitsfunktion, die angeboten wird, um Kunden die Kontrolle darüber zu geben, wer auf ihre Daten zugreifen kann. Das Problem ist, dass die Verwendung von Customer Lockbox möglicherweise die Effizienz und Skalierbarkeit der Cloud-Dienste beeinträchtigt. Wenn ein Kunde eine Anfrage an den Anbieter eines Cloud-Dienstes sendet, um auf seine Daten zuzugreifen, muss der Anbieter diese Anfrage an den Kunden weiterleiten, um eine Genehmigung zu erhalten. Darüber hinaus kann Customer Lockbox die Sicherheit beeinträchtigen, wenn Kunden die Genehmigung für den Zugriff auf ihre Daten Personen erteilen, die nicht über die erforderliche Sicherheitsüberprüfung verfügen. Zusammenfassend lässt sich sagen, dass Customer Lockbox eine nützliche Funktion für Kunden sein kann. Es gibt aber auch potenzielle Herausforderungen, die bei der Implementierung berücksichtigt werden müssen, um sicherzustellen, dass Effizienz und Sicherheit des Cloud-Dienstes nicht beeinträchtigt werden.

Telemetriedaten Microsoft

Ein weiteres Problem besteht darin, dass Nutzerinnen und Nutzer möglicherweise nicht vollständig darüber informiert sind, welche Telemetriedaten Microsoft tatsächlich sammelt und wie sie weiterverwendet werden. Es ist wichtig zu beachten, dass Microsoft in der Regel nur «anonymisierte» Telemetriedaten sammelt, die keine persönlichen Informationen enthalten. Dennoch gibt es Bedenken, dass die Daten nicht ausreichend anonymisiert sind oder dass Microsoft bestimmte personenbezogene Informationen speichert, die nicht für Telemetriedaten verwendet werden sollten. Um diese Bedenken zu adressieren, hat Microsoft verschiedene Massnahmen ergriffen, um sicherzustellen, dass die Verwendung von Telemetriedaten den Datenschutzbestimmungen entspricht. Darüber hinaus hat Microsoft erklärt, dass es keine personenbezogenen Daten verkauft

oder weitergibt. Es ist wichtig zu beachten, dass ständig daran gearbeitet wird, die Einhaltung der Datenschutzbestimmungen für M365 zu verbessern und sicherzustellen, dass die Dienste den Anforderungen der Nutzerinnen und Nutzer sowie der Regulierungsbehörden entsprechen.

- **Datenhoheit:** Da öffentliche Einrichtungen oft sensible und vertrauliche Informationen verwalten, bestehen Bedenken bezüglich der Kontrolle über Daten, wenn sie in der Cloud gespeichert werden.
- **Datensicherheit:** M365 ist ein beliebtes Ziel für Hackerangriffe (Glossar: Malware). Bedenken bezüglich der Sicherheit der Daten sind vorhanden, wenn sie auf einer Plattform gespeichert werden, die möglicherweise gefährdet ist.
- **Abhängigkeit von einem Anbieter:** Wenn eine öffentliche Einrichtung sich für M365 entscheidet, ist sie von Microsoft als Anbieter abhängig. Dies kann zu Problemen führen, wenn die öffentliche Einrichtung beschliesst, den Anbieter zu wechseln.

V. Schwerpunktthema 2: Auditprogramm

Ausgangslage
Datenbearbeitungen[16] die aus Sicht des Datenschutzbeauftragten als Gegenstand eines Datenaudits im Jahr 2018 vorgeschlagen wurden, haben mittlerweile einen festen Platz im Tagesgeschäft und werden kontinuierlich beobachtet. Dazu gehören: Datenbearbeitung im Bereich Bildung/Pädagogik und Beratung bei der Nutzung von Microsoft Office 365 an den Schulen, Umsetzung Reglemente Videoüberwachungen.

Erstanalyse und Bewertung mittels Fragekatalog (Auslegeordnung gemäss §7 IDG)
Aus den erhobenen Informationen des zur Verfügung gestellten Fragenkatalogs wurden Bedrohungsanalysen mit potenziellen Schwachstellen und ihren Auswirkungen erstellt. Es erfolgte eine Bewertung der Qualität der Dokumentation im Hinblick auf formelle und materielle Inhalte und Vorgaben, vor allem betreffend Datensicherheit, die teils noch lückenhaft dokumentiert war. Folgende Segmente bezüglich WebGIS wurden datenschutzrechtlich innerhalb des Audits geprüft:

- Datenpopulationen, Datenflüsse, Schnittstellen
- Management und Organisation
- Konzepte und Dokumentationen
- Physikalische Sicherheit der Infrastruktur
- Awareness der Mitarbeitenden
- Rollen-/Rechtekonzept
- Serversystem und Netzwerk
- Websites und Webanwendungen, etc.

Informationsbeschaffung
Die angeführten Informationen wurden mittels Dokumentation, Workshops vor Ort und Unterlagenstudium gesammelt und in einer schriftlichen Zusammenstellung via Fragenkatalog strukturiert und erläutert. Dazu gehören unter anderem der Prozessablauf und der Systemaufbau, ein Soll-Ist-Vergleich mit Datenschutz-Standardvorgaben, die Erarbeitung von Referenzdokumenten und die Erhebung von technisch-organisatorischen Massnahmen. Bei der Informationsbeschaffung sind allerdings nicht alle Möglichkeiten ausgeschöpft worden (IDW-Partner / Vertragsmanagement Dritte).

- Authentifizierungen und Auftragsverarbeitung
- Meldeprozess von Datenschutzverletzungen
- Löschung- und Archivierungsprozesse
- Protokollierung: Integritätsverlust
- Business-Continuity-Prozess: Back-up-Konzept
- Kryptographie – Verschlüsselungstechnik
- Auswahl von Software (Security by Design / PEN-Testzyklen), etc.

Vertiefende Analyse (Audit-Assessment)
Auf der Grundlage der in der Erstanalyse festgestellten Schwachstellen und Bedrohungen erfolgten notwendige Detailanalysen des Betriebs Geodateninfrastruktur (GDIW), die auf einem risikobasierten Ansatz beruhen. Für besonders wichtige Inhalte wurde in Workshops mit dem Auftraggeber ein Massnahmenkatalog erstellt, wobei die Umsetzung ebendieser innerhalb Jahresfrist erneut zu prüfen sei (sog. Aktionsplan 2023).
Datenschutzmaturität/Scoring

[16] Die Auflistung sagt nichts über das Datenschutzniveau der betreffenden Stellen aus, sondern weist auf Datenbearbeitungen hin, die von der Natur der Sache her eine gewisse Kritikalität für die Persönlichkeit der Datensubjekte «ausstrahlt».

Die Umsetzung des Datenschutzes gilt als «Enabler» für ein besseres Verständnis der Anforderungen und des Schutzbedarfs. Mit der Durchführung des Audits konnte die Maturität in diesem Bereich massgeblich gesteigert werden. Erst nach Umsetzung des Aktionsplans ist ein Scoring möglich, weil auch die «Wahl» der Massnahmen und das «Wie» der Umsetzung in die Maturitätsbewertung einfliessen werden.

Abschlussbericht mit Empfehlungen -> Aktionsplan vom Fachbereich erwartet 2023

Aus den erfolgten Analysen sind Handlungsempfehlungen abgeleitet worden (sogenannte «red flags»). Ziel ist, dass für alle relevanten Risiken angemessene Massnahmen und Dokumentationen erarbeitet bzw. Nachweise erbracht werden.

VI. Interne Zusammenarbeit mit anderen Datenschutzbehörden und Verbänden schweizweit

Die Datenaufsicht ist Mitglied von Privatim, der Konferenz der schweizerischen Datenschutzbeauftragten. Die Arbeitsgruppen führten ihre Sitzungen während des ganzen Jahres durch, mit Schwerpunkt M365 und Prozessgestaltung für Meldungen von Datenschutzverletzungen. Nebst dem institutionalisierten Austausch arbeitete die Datenschutzbeauftragte auch themenbezogen mit anderen Datenschutzaufsichtsstellen zusammen. Diese Zusammenarbeit erlaubt es, rascher zu standardisierten Lösungen zu kommen und zudem eine gewisse Harmonisierung in Datenschutzfragen zu erzielen. Ein Austausch erfolgte im Berichtsjahr insbesondere im Zusammenhang mit der sogenannten eWohnsitzbescheinigung und Edulog.

VII. Interne Schulungen

Im Berichtsjahr 2022 nahm die Datenschutzbeauftragte an zwei internen Einführungsveranstaltungen für neue Kadermitglieder der Stadtverwaltung teil.

VIII. Ausblick 2023/2024

Datenaufsicht

Der im Rahmen des Jahresrückblicks erwähnte Trend, dass die Zahl der bei der Datenaufsichtsstelle eingehenden Anfragen stetig zunimmt, hält unvermindert an. Zum Zeitpunkt der Finalisierung dieses Tätigkeitsberichts hat die Datenschutzbeauftragte den Rückstand, der vor 2021 angefallen ist, bis auf wenige Dossiers parallel zu den eingehenden Geschäften 2021 und 2022 kontinuierlich abgearbeitet.

Datenrecht

Im Fokus der Überprüfungen werden weiterhin die Vertragswerke von Microsoft, konkret die Online Service Terms (OST) und der Auftragsverarbeitungsvertrag (DPA) stehen. Ein «Evergreen» im Jahr 2022 war und bleibt auch 2023 die sensitive Datenübermittlung in Drittländer. Hintergrund ist das Schrems II-Urteil von Juli 2020. In Italien gibt es strenge Auflagen für ChatGPT, in der EU eine Task Force. AlgorithmWatch fordert Massnahmen auch in der Schweiz. Die Entwicklungen im Datenschutz waren 2022 und bleiben rasant:

Artificial Intelligence Act

Der Artificial Intelligence Act (AI-Act) befindet sich noch im Entwurfsstadium: hier. Die Verordnung soll einen einheitlichen Rechtsrahmen für vertrauenswürdige KI-Systeme etablieren sowie einheitliche Regeln für deren Entwicklung, Vermarktung und Verwendung innerhalb der EU schaffen, die im Einklang mit ihren Werten und den Grundrechten sind.

Digital Services Act

Der Digital Services Act (DSA) zielt auf einen besseren Schutz der Verbraucher und ihrer Grundrechte im Internet. Der DSA ist am 16. November 2022 in Kraft getreten und wird am 17. Februar 2024 wirksam. Vor dem Hintergrund dieser Zielsetzung soll für die Haftung von Online-Plattformen wegen unrechtmässiger Inhalte (z.B. Hass) ein einheitlicher Rechtsrahmen geschaffen werden und für mehr Transparenz bei der Verwendung von Algorithmen gesorgt werden.

IX. Impulse

Ethischer Datenschutz

Datenschutz ist im Spannungsfeld der informationellen Selbstbestimmung kein Selbstzweck, sondern Teil der staatlichen Aufgabenerfüllung. Ethischer Datenschutz betrifft viel mehr als nur KI gesteuerte Systeme. Digitale Räume, eben Bereiche der Inneren Sicherheit, der Bildung, eigentlich jeder Bereich unseres Lebens braucht ein entsprechendes ethisches Gleichgewicht. Dieser Verantwortung sind sich viele Menschen bewusst, die in der Verwaltung arbeiten. Diese Haltung sollten wir auch weiterhin beibehalten – insbesondere im Hinblick auf die bevorstehenden Erweiterungen des Öffentlichkeitsprinzips.

Dankeschön

Wir können unsere Arbeiten nur mit der Unterstützung vieler Menschen und Fachbereiche machen. Ich möchte mich bei allen bedanken, die ein waches Auge haben für Entwicklungen des Datenschutzes und sich für Datenschutzbelange einsetzen, bei allen Mitarbeiterinnen und Mitarbeitern der Verwaltung und Privaten, die sich vertrauensvoll mit Fragestellungen an mich gewandt haben. Zuletzt einen Dank sei noch an die Leitungen des Parlamentsdienstes, der Ombudsstelle und der Finanzkontrolle sowie der IDW für hervorragende Zusammenarbeit, gerichtet.

X. Antrag

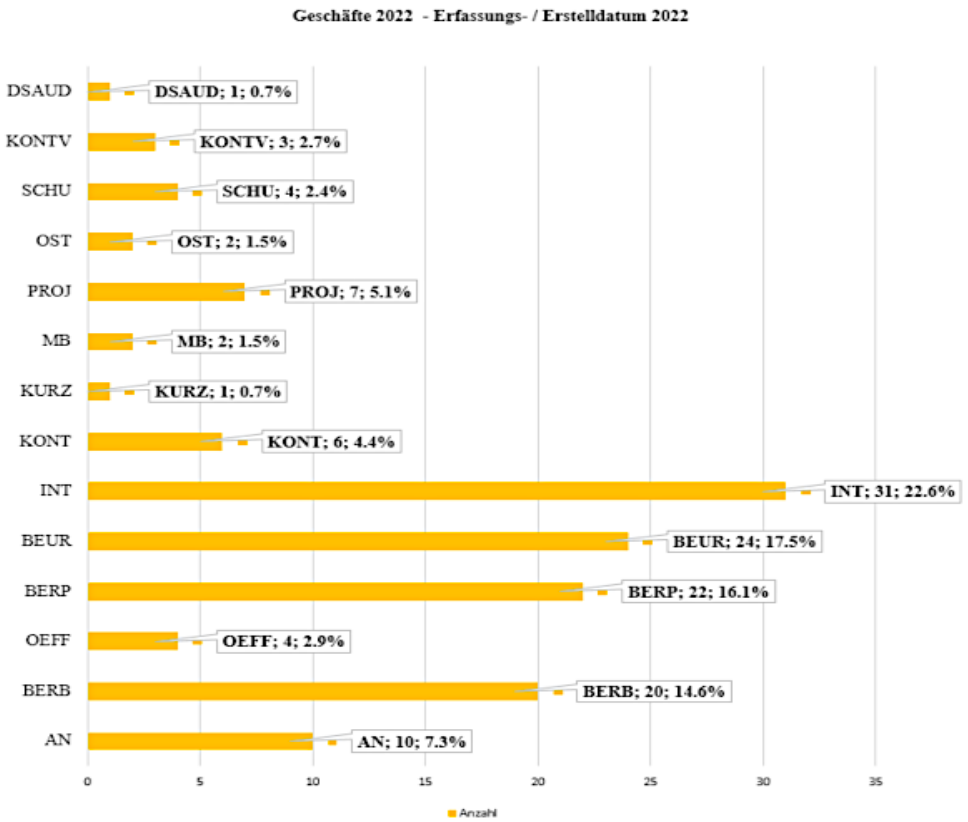
Ich beantrage, Herr Präsident, sehr geehrte Damen und Herren, auf den Bericht der Datenaufsicht der Stadt Winterthur über das Jahr 2022 einzutreten.

Anhang A: Statistische Auswertungen

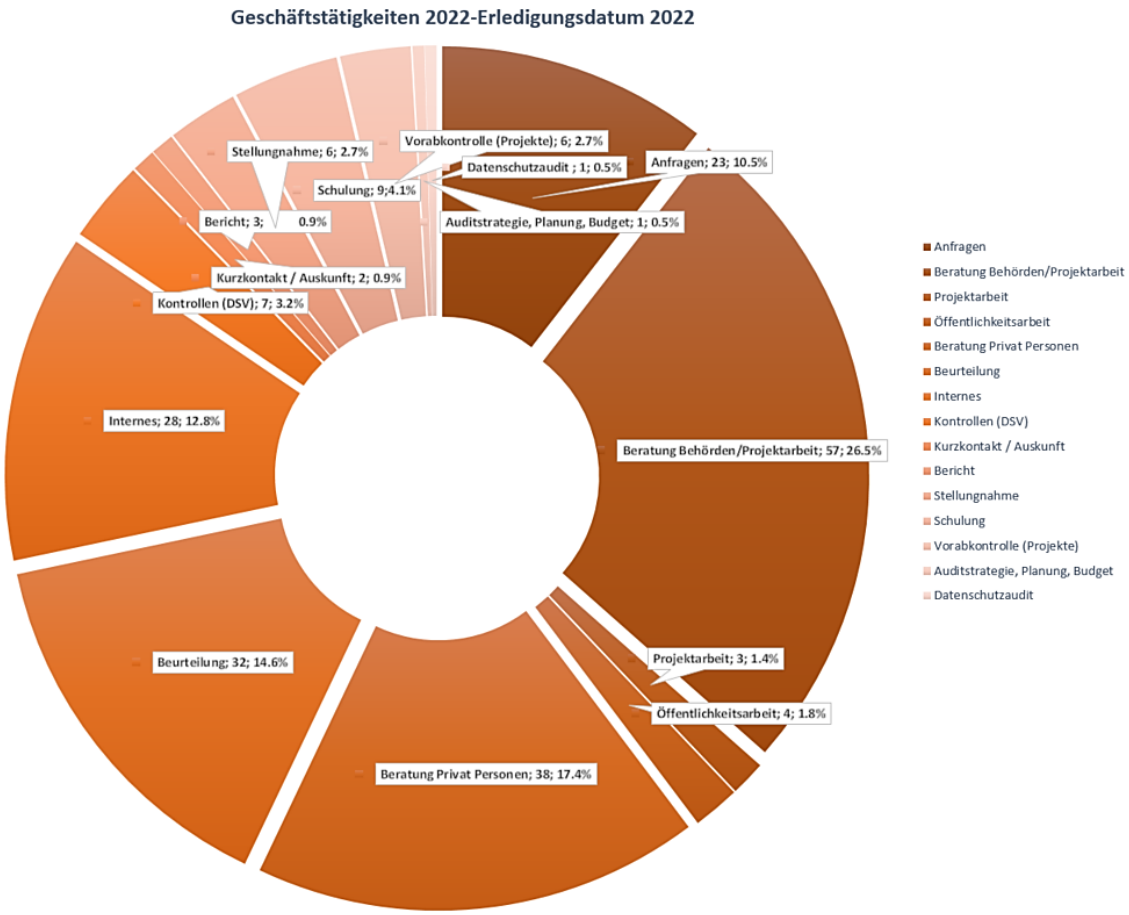
Tabelle: Bearbeitungsstand per 31. Dezember 2022; Quelle: Geschäftskontroll-Datenbank Stadt Winterthur.

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
2022	137	123	14	220
Total	1028	857	613	1563

Übersicht Geschäfte Datenschutzbeauftragte 2022
Diagramm 1: Auflistung aller Geschäfte mit Erfassungsdatum 2022, die bis zum 31.12.2022 erledigt wurden.
Quelle: Geschäftskontroll-Datenbank Stadt Winterthur.



Übersicht Geschäfte Datenschutzbeauftragte
Diagramm 2: Auflistung aller Geschäfte mit Erledigungsdatum 2022, die bis zum 31.12.2022 erledigt wurden.
Quelle: Geschäftskontroll-Datenbank Stadt Winterthur.



Anhang B
Abkürzungsverzeichnis

DSG	Bundesgesetz über den Datenschutz, SR 235.1
E.	Erwägung
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
ICT	eng. Abkürzung für Information and Communication Technology
IDG	Informations- und Datenschutzgesetz Kanton Zürich, SR 170.4
IDV	Verordnung über die Information und den Datenschutz, SR 170.41
ISDS	Informationssicherheit und Datenschutz (Abkürzung HERMES-Projektmethode)
i.S.v.	im Sinne von
KI	Künstliche Intelligenz
Nr.	Nummer
privatim	Konferenz der schweizerischen Datenschutzbeauftragten
SR	Systematische Rechtssammlung (des Bundes)
vgl.	vergleiche
Ziff.	Ziffer

Glossar[17]

Anonymisierung
Der Vorgang, personenbezogene Daten so zu verändern, dass diese Daten der Person nicht mehr oder nur noch mit aussergewöhnlichem Aufwand zugeordnet werden können.

Authentifizierung
siehe Verifizierung

Biometrics
Biometrische Authentifizierungssysteme verwenden diese Merkmale, um eine Person zu identifizieren oder zu verifizieren, indem sie sie mit einem zuvor erstellten biometrischen Profil abgleichen.

Encryption
Chiffrierung, Verschlüsselung. Die Umwandlung von Daten in eine Form, genannt Chiffrat, die von Unbefugten nicht interpretiert werden kann.

Hacker
Subjekt, dessen Ziel es ist, ein tiefgreifendes Verständnis der internen Arbeitsweise eines technischen Systems zu haben. Hacker kreieren oder verändern Software und Hardware, inklusive programmierrelevante Elemente.

Identität
Eine Identität bezieht sich auf die Gesamtheit der Eigenschaften, Merkmale und Aspekte, die eine Person oder Entität einzigartig und unterscheidbar von anderen machen. Die Identität kann aus einer Kombination von Faktoren bestehen, einschliesslich aber nicht beschränkt auf das Geschlecht, die Ethnizität, die Nationalität, die Religion, die sexuelle Orientierung, die familiäre Herkunft, die soziale Klasse, die Bildung, die persönlichen Erfahrungen und Überzeugungen. Es muss unterschieden werden zwischen Identifizierung (eindeutiges Erkennen einer Person oder eines Objektes) und Verifizierung (Bestätigung der Authentizität einer behaupteten Identität).

Logging (Protokollieren)
Jede Aktivität in einem Computersystem, einer Anwendung oder in einem Netzwerk kann geloggt werden. Das bedeutet, dass ein Protokoll dieser Aktivitäten erstellt werden kann. Aus Sicht des Datenschutzes ist dies eine Massnahme, die unter gewissen Bedingungen (Art. 10 VDSG) sogar gefordert wird.

Malicious Software (Malware)
Dieser Begriff umfasst Software, die Schaden auf einem Computer anrichten kann. Malware ist ein Sammelbegriff für Computerviren und -würmer, trojanische Pferde und Spywares oder Adwares.

Passwort
Ein Passwort oder Kennwort ist ein Mittel zur Überprüfung der Identität, beispielsweise einer Benutzerin oder eines Benutzers innerhalb eines Systems.

Pseudonymisierung
Vorgang der Trennung der identifizierenden von den restlichen Personendaten. Die Zuordnung der beiden Datenbereiche erfolgt durch ein Pseudonym, das sowohl bei den identifizierenden als auch bei den restlichen Daten vorhanden sein muss. Somit ist eine Zusammenführung der beiden Datenteile durch Berechtigte wieder möglich (Depseudonymisierung/Reidentifizierung).

Verifizierung
Die Beglaubigung der Echtheit von etwas oder jemandem. In privaten oder öffentlichen Computer-Netzwerken, wie beispielsweise dem Internet, erfolgt die Verifizierung normalerweise über Passwörter, die eine Anmeldung erst möglich machen.

****

[17] EDÖB