dsb
datenschutzbeauftragte
des kantons zürich

Tätigkeitsbericht 2020

«Auch in der Krise muss der Staat dem Vertrauen der Bevölkerung in den Umgang mit ihren Personendaten gerecht werden.»

Datenschutz-beauftragte des Kantons Zürich

Vorwort

Die Beauftragte berichtet dem Wahlorgan periodisch über Umfang und Schwerpunkte der Tätigkeiten, über wichtige Feststellungen und Beurteilungen sowie über die Wirkung des Gesetzes. Der Bericht wird veröffentlicht (§ 39 IDG). Der vorliegende Tätigkeitsbericht deckt den Zeitraum vom 1. Januar 2020 bis und mit 31. Dezember 2020 ab und ist im Internet unter www.datenschutz.ch publiziert.

Der Tätigkeitsbericht 2020 ist der 26. der Behörde, aber der 1. in meiner Amtszeit. Er zeigt, wie die Grundrechte auch in Krisensituationen, wie wir sie aktuell mit der Corona-Pandemie erleben, ihre Funktion haben und Wirkung erzielen. Das Grundrecht auf Privatsphäre und informationelle Selbstbestimmung war im vergangenen Jahr ein zentrales Thema. Im Rahmen der Massnahmen zur Pandemiebekämpfung wurden grosse Mengen an Personendaten erhoben, weitergegeben und ausgewertet. Gleichzeitig entwickelte sich der Trend der Digitalisierung in diesem Umfeld rasch weiter. Die Beratung und die Aufsicht im Datenschutz sind die Voraussetzung, damit die Grundrechte in unserer demokratischen und freien Gesellschaft gewährleistet bleiben.

Dr. iur. Dominika Blonski
Datenschutzbeauftragte des Kantons Zürich

Inhaltsverzeichnis

6
Übersicht

7 Teil der Lösung in der Krise
10 Entwicklungsschwerpunkte

12
Homeoffice, aber sicher!

13 Regeln für das Homeoffice
14 Komplexe Fragen zur digitalen Zusammenarbeit
16 Prorektor-Wahl per Videokonferenz
17 Corona-Pandemie und Privatsphäre – als Video

31
Überlegen in der Digitalisierung

32 Impulsprogramm Datenschutz
34 Go-live der neuen Kantonswebsite
35 Informationsrichtlinien für die Verwaltung
36 Elektronische Kommunikation in der Justiz
37 Mitwirkungspflicht im Asylverfahren
38 Mehr Informationssicherheit in den Gemeinden
39 Zurückblicken und vorausschauen

41
Wirksame neue Instrumente

42 Datenschutz-Folgenabschätzung wird Pflicht
43 Datenschutzvorfälle müssen gemeldet werden

18
Fernunterricht, der bildet

19 Fragen zum digitalen Unterricht
21 Datenschutz online lernen

22
In der Krise ist nicht alles anders

23 Auch in der Krise nicht alles offenlegen
25 Datenschutz im Datenüberfluss
27 Mit Doodle zum Gottensdienst anmelden
28 Gemeindeversammlung im Fernsehen
29 Universalschlüssel zu den Bibliotheken
30 Rayonverbot mit Electronic Monitoring

46
Impressum

47
Kontakt

Übersicht

7 Teil der Lösung in der Krise
10 Entwicklungsschwerpunkte

Teil der Lösung in der Krise

Die Corona-Pandemie hat unseren Alltag in zahlreichen Lebensbereichen wesentlich verändert. Das zeigte sich auch bei den Tätigkeiten der Datenschutzbeauftragten im Jahr 2020. Zwar hat die Digitalisierung ihre Arbeit schon in den letzten Jahren geprägt. Doch in der Krise benötigten die öffentlichen Organe sowie die Einwohnerinnen und Einwohner schnelle Lösungen. Die Datenschutzbeauftragte unterstützte sie pragmatisch.

«Wir hören dich nicht – du bist noch stummgeschaltet.» Diese Aussage fällt in jeder Videokonferenz. Sie macht uns darauf aufmerksam, dass wir das Mikrofon anstellen sollen, wenn wir sprechen möchten. 2020 mussten wir viele neue Gewohnheiten lernen. Videokonferenzen finden meist im heimischen, provisorisch eingerichteten Büro – im Homeoffice – statt. Auch der Schulunterricht der Kinder wurde teilweise in ein virtuelles Umfeld verlegt. Die Trennung zwischen Freizeit und Arbeit, privat und beruflich, schwand.

Die Datenschutzbeauftragte wurde mit Fragen von öffentlichen Organen, aber auch von Einwohnerinnen und Einwohnern überhäuft. Sie sorgten sich um den Datenschutz im Homeoffice, im Fernunterricht, beim Contact Tracing, bei der Meldepflicht bei der Rückkehr aus Risikoländern, bei der Abfrage von Sommerferien-Reisedestinationen bei Schulkindern oder in Bezug auf Impfdaten. Die Datenschutzbeauftragte unterstützte unkompliziert und praxisbezogen bei der Umsetzung der Massnahmen. Sie veröffentlichte eine Produkteliste und Regeln fürs Homeoffice und zeigte die datenschutzrechtlichen Vorgaben auf.

Die Beobachtungen und Diskussionen in der Corona-Pandemie führen aus der Perspektive des Datenschutzes und der Informationssicherheit zu zwei Erkenntnissen: Die Pandemie bewirkte einen Digitalisierungsschub und der Umgang mit diesem war sehr unterschiedlich. In manchen Bereichen besteht weiterhin weder das Bewusstsein noch das Interesse für die Gefahren einer Digitalisierung, die nicht datenschutzkonform umgesetzt wird. Es wird einfach etwas gemacht. Aber es gibt auch andere Bereiche, die die Gefahren erkennen und versuchen, sie einzudämmen.

Ganz unabhängig davon, wie herausfordernd die Umstände sein mögen, bleiben die öffentlichen Organe verantwortlich für die Personendaten der Einwohnerinnen und Einwohner. Sie dürfen diese nur bearbeiten, wenn dies im Gesetz vorgesehen ist, und sie müssen sie schützen, indem sie die organisatorisch-technischen Vorgaben einhalten. Auch wenn aussergewöhnliche Zeiten nach aussergewöhnlichen Massnahmen verlangen, dürfen datenschutzrechtliche und sicherheitstechnische Aspekte nicht vernachlässigt werden. Zudem tragen die Mitarbeitenden öffentlicher Organe die Verantwortung dafür, wie sie ihre Arbeit im ungewohnten Umfeld organisieren.

Die Medien berichteten ausgiebig über die Datenbearbeitungen im Zusammenhang mit der Corona-Pandemie. Die Reaktionen der Bevölkerung haben gezeigt, dass sie sich sehr für ihr Grundrecht auf Datenschutz interessiert und seine Einhaltung bei den öffentlichen Organen auch einfordert. Die öffentlichen Organe sind in der Ausnahmesituation mehr denn je in der Pflicht, diese Erwartungen zu erfüllen und dem Vertrauen der Einwohnerinnen und Einwohner in den Umgang mit den Personendaten gerecht zu werden.

Ist in der Krise wirklich alles anders?
Beim Datenschutz handelt es sich um ein Grundrecht. Jede Bearbeitung von Personendaten ist ein Eingriff in dieses Grundrecht. Grundrechte können eingeschränkt werden, wenn bestimmte Voraussetzungen erfüllt sind. Ob eine Datenbearbeitung und damit ein Eingriff in das Grundrecht auf Privatsphäre zulässig ist, wird immer nach dem gleichen Schema überprüft – auch oder gerade während Krisen. In einer Krise kann die Überprüfung aber zu einem anderen Ergebnis führen als sonst. Dies zeigt die Corona-Pandemie sehr anschaulich. Auch Datenbearbeitungen, die in Zusammenhang mit der Pandemie erfolgen, brauchen eine rechtliche Grundlage und es muss ein öffentliches Interesse vorhanden sein. Die Eindämmung einer Infektionskrankheit liegt im öffentlichen Interesse, weil sie die Infrastruktur des Gesundheitswesens gefährlich stark beansprucht. Aufgrund des Epidemiengesetzes wurden Bestimmungen erlassen, die Datenbearbeitungen erlauben beispielsweise zur Rückverfolgung von Infektionen. Somit besteht eine gesetzliche Grundlage. Die Datenbearbeitung muss allerdings auch noch geeignet und erforderlich sein, um das Ziel erreichen zu können, nämlich die Ausbreitung des Virus zu bekämpfen. Sonst ist sie nicht verhältnismässig. Wäre die Angabe der Kontaktdaten freiwillig, könnten nicht alle betroffenen Personen eruiert werden. Die Datenbearbeitung wäre nicht geeignet, um das Ziel zu erreichen. Nicht erforderlich für die Rückverfolgung möglicher Infektionen wäre beispielsweise die Erfassung von Berufsangaben oder des Fingerabdrucks. Die rechtliche Grundlage und das öffentliche Interesse für die so flächendeckende Erfassung der Kontaktdaten bestehen allerdings nur während der Pandemie. In anderen Umständen wäre diese Massnahme nicht verhältnismässig. Das Gleiche gilt für alle anderen Grundrechte, die während der Pandemie eingeschränkt wurden, beispielsweise die Wirtschaftsfreiheit, als gewisse Betriebe während bestimmter Zeiten nicht öffnen durften, oder die Versammlungsfreiheit.

Neue Instrumente, neue Datenschutzbeauftragte und eine grössere Datenschutzbehörde
Das Jahr 2020 bringt für den Datenschutz im Kanton Zürich einige Neuerungen. Das revidierte Gesetz über die Information und den Datenschutz (IDG) sieht neue Instrumente für Datenbearbeiter und die Datenschutzbeauftragte vor.

Die Datenschutz-Folgenabschätzung soll helfen, bei neuen Datenbearbeitungen im Voraus die Risiken für die Privatsphäre einzuschätzen und zu minimieren. Die unterstützenden Dokumente wurden in die Projektmethode Hermes integriert, die bei allen Digitalisierungsprojekten der kantonalen Verwaltung eingesetzt werden muss. Die Datenschutz-Folgenabschätzung unterstützt die Entscheidungsfindung, ob ein Projekt oder eine geplante Datenbearbeitung der Datenschutzbeauftragten zur Vorabkontrolle vorgelegt werden muss. Schon bisher mussten öffentliche Organe dafür eine Risikoeinschätzung durchführen. Neu ist nur die ausdrückliche gesetzliche Pflicht, ein entsprechendes Dokument zu erstellen.

Seit Inkrafttreten des revidierten Gesetzes sind öffentliche Organe verpflichtet, Datenschutzvorfälle an die Datenschutzbeauftragte zu melden. Meldepflichtig ist beispielsweise, wenn sich ein Hacker Zugriff auf Daten verschafft oder auch wenn ein Mitarbeiter oder eine Mitarbeiterin einen USB-Stick mit Personendaten verloren hat.

Neu kann die Datenschutzbeauftragte eine Verfügung aussprechen, wenn sich ein Organ nicht an ihre Empfehlung hält. Sie kann beispielsweise den Abbruch einer Datenbearbeitung oder die Löschung von Daten verfügen. Dies stärkt die Datenschutzrechte der Einwohnerinnen und Einwohner.

Mit der Selbstdeklaration hat die Datenschutzbeauftragte ein neues Instrument entwickelt, mit dem Gemeinden die Einhaltung der datenschutzrechtlichen und sicherheitstechnischen Vorgaben einschätzen und verbessern können. Die Unterlagen der Datenschutzbeauftragten unterstützen dabei, eine Übersicht der bestehenden IT-Infrastruktur zu bekommen, die Risiken zu beurteilen und Verbesserungsmassnahmen zu ergreifen. Gemeinden können mit diesem neuen Datenschutzreview ihre immer komplexer werdenden IT-Infrastrukturen professionell dokumentieren. Dank dem Datenschutzreview mit Selbstdeklaration kann die Datenschutzbeauftragte die Reichweite ihrer Kontrollen stark erweitern.

Am 1. Mai 2020 trat Dominika Blonski als neue Datenschutzbeauftragte ihr Amt an. Sie war im Dezember 2019 vom Kantonsrat als Nachfolgerin von Bruno Baeriswyl gewählt worden, der altershalber zurücktrat.

Der Kantonsrat hat im Dezember 2019 das Budget der Datenschutzbeauftragten um drei Arbeitsstellen erhöht. Die drei Stellen wurden im Verlauf des Jahres besetzt. Mit diesen zusätzlichen Ressourcen möchte die Datenschutzbeauftragte insbesondere die Aufsicht über die Datenbearbeitungen stärken.

In welcher Gesellschaft wollen wir leben?

Die Öffentlichkeit diskutierte im letzten Jahr mehr denn je über Datenschutz. Oft zeigt sich, dass wenig bekannt ist über die Grundsätze des Datenschutzes. Was ist Datenschutz eigentlich? Wie funktioniert Datenschutz?

Datenschutz ist ein Grundrecht. Daraus leiten sich juristische Bedingungen ab. Bei Datenbearbeitungen müssen also bestimmte Vorgaben eingehalten werden. Viel bedeutender und stark unterschätzt ist jedoch die gesellschaftliche Dimension. Denn Grundrechte schützen die Werte einer Gemeinschaft, wie das Recht auf Leben, das Diskriminierungsverbot oder das Recht auf eine freie Meinungsbildung. Sie legen die Basis für die Beantwortung der Frage «Wie möchten wir als Gesellschaft zusammenleben?».

Die Freiheitsrechte sind wichtige Pfeiler der liberalen Gesellschaft. Zu diesen gehört das Grundrecht auf Privatsphäre und auf persönliche Freiheit, die auch das Grundrecht auf Datenschutz beinhalten. In einer Gemeinschaft ohne dieses Grundrecht sind die Menschen manipulierbar. Sie können ihre Freiheiten nicht ausleben, die für das Funktionieren des demokratischen Rechtsstaats nötig sind. Individuen können nur selbstbestimmt leben, wenn sie auch darüber bestimmen können, welche persönlichen Informationen bekannt sind und welche eben geheim gehalten werden. Dies beeinflusst die freie Entfaltung der Persönlichkeit und verändert das Verhalten der Personen.

Grundrechte gelten aber nicht schrankenlos. Sie können unter bestimmten Voraussetzungen eingeschränkt werden, ohne dabei verletzt zu werden. Dafür braucht es eine rechtliche Regelung, ein öffentliches Interesse daran und das Ganze muss verhältnismässig sein. Und je nach Situation ist eine weitergehende Einschränkung zulässig oder eben nicht.

Unermüdlich für die Freiheitsrechte

Nach gut 25 Jahren als Datenschutzbeauftragter des Kantons Zürich ist Bruno Baeriswyl Ende April 2020 in Pension gegangen. Er nahm seine Arbeit 1994 auf, also bevor das erste Datenschutzgesetz des Kantons am 1. Januar 1995 in Kraft trat. Das Schlagwort Digitalisierung bestand damals noch nicht. Die Entwicklung, die damit gemeint ist, war jedoch schon in vollem Gang. Die elektronischen Datenbearbeitungen nahmen schon in den 1990er-Jahren schnell zu. Die Ansprüche an die Behörde wuchsen ständig. Der Beitritt der Schweiz zum Schengen-Abkommen führte zu einem weiteren Ausbau der Aufgaben. Zunächst war der Datenschutzbeauftragte der Justizdirektion angegliedert. Doch die Aufsichtsfunktion der Behörde verlangte nach vollständiger Unabhängigkeit. Bruno Baeriswyl setzte sich bis zum letzten Arbeitstag unermüdlich für den Datenschutz und die Persönlichkeitsrechte auch in der digitalisierten Gesellschaft ein. Dafür war und ist er immer noch weit über die Kantonsgrenzen bekannt. An der Jubiläumsveranstaltung zu 25 Jahren Datenschutzgesetzgebung im Kanton Zürich sagte er: «Auf der ganzen Welt werden dieselben Technologien entwickelt und eingesetzt, unabhängig vom politischen und gesellschaftlichen System. Totalitäre Staaten sehen in ihnen eine Möglichkeit zur Überwachung und zur Manipulation der Bevölkerung. In demokratischen und liberalen Gesellschaften steht das Grundrecht auf persönliche Freiheit im Vordergrund. Der Gesetzgeber steht in der Pflicht, die notwendigen Rahmenbedingungen zu schaffen.»

Die Bedeutung seines Engagements hätte nicht besser illustriert werden können als durch die Ereignisse der letzten Arbeitstage. Mit dem Lockdown stellten sich plötzlich sehr akut genau die Fragen nach den Risiken der Digitalisierung, die Baeriswyl 25 Jahre lang zur Diskussion stellte. Die Stellen, die sich diesen Anforderungen schon früher angenommen hatten, konnten mit den neuen Umständen im Jahr 2020 besser umgehen als andere. Bei seiner Verabschiedung im Kantonsrat drückte er seine Zuversicht aus: «Wenn ich sehe, dass der Kantonsrat auch in Krisenzeiten seine Rolle wahrnimmt, dann bin ich überzeugt, dass die Freiheitsrechte bei Ihnen in guten Händen sind.»

Entwicklungs-schwerpunkte

Der Konsolidierte Entwicklungs- und Finanzplan (KEF) der Datenschutzbeauftragten enthält vier Leistungsindikatoren und zwei Wirkungsindikatoren. Für das Jahr 2020 zeigen sie eine Verlagerung der Tätigkeiten, die sich aus der besonderen Situation aufgrund der Corona-Pandemie ergeben hat.

Mit der Verbreitung des Homeoffice und des Homeschooling seit dem ersten Quartal 2020 nahm der Einsatz von Produkten zum virtuellen Zusammenarbeiten oder zum virtuellen Unterrichten stark zu. Dadurch stiegen die Anfragen bei der Datenschutzbeauftragten zu diesen Themen an. Dieser Trend blieb das ganze Jahr hindurch bestehen. Kontinuierlich stellten sich datenschutzrechtliche Fragen im Zusammenhang mit der Bekämpfung des Coronavirus. Entsprechend zeigt der Leistungsindikator Beratungen eine deutliche Entwicklung. Die Datenschutzbeauftragte führte 2020 etwa ein Drittel mehr Beratungen durch als 2019.

Auch die Entwicklung des zweiten Leistungsindikators Kontrollen zeigt die besondere Situation im Berichtsjahr auf. Kontrollen laufen in drei Phasen ab. Zunächst fordert die Datenschutzbeauftragte öffentliche Organe auf, Unterlagen einzureichen, und prüft sie. In einem zweiten Schritt besucht sie die öffentlichen Organe vor Ort, um Interviews durchzuführen und einen Augenschein zu nehmen. Abschliessend verfasst sie einen Bericht gestützt auf die Erkenntnisse aus den beiden ersten Schritten. Die Massnahmen zur Eindämmung der Pandemie verhinderten die Kontrollen vor Ort. Die öffentlichen Organe waren auch im Verlauf des Jahres nicht für virtuell durchgeführte Kontrollen eingerichtet. Dies führte zu einer Verminderung der Anzahl der durchgeführten Kontrollen.

Stabil blieben hingegen die weiteren beiden Leistungsindikatoren Aus- und Weiterbildungen sowie Vernehmlassungen. Bei beiden bewegt sich der Indikator im Durchschnitt: Die Aus- und Weiterbildungsaktivität wie auch die Stellungnahmen im Rahmen von Vernehmlassungen konnten im geplanten Umfang ausgeführt werden.

Der Einfluss der Pandemie zeigt sich auch bei den Wirkungsindikatoren. Die Anzahl Besucherinnen und Besucher auf der Website verdoppelte sich beinahe. Das zeigt einerseits, dass die Informationen auf der Website in der Auswahl und der Qualität dem Bedürfnis der Nutzerinnen und Nutzer entsprechen. Andererseits illustriert die starke Besucherzunahme das steigende Informationsbedürfnis der Mitarbeitenden der öffentlichen Organe, aber auch der Bevölkerung. Die Website ist kontinuierlich weiterzuentwickeln, um diesen Anliegen gerecht zu werden. Am zweiten Wirkungsindikator Massnahmenumsetzung kann abgelesen werden, dass die Nachkontrollen konstant ihre Wirkung zeigen. Mit den Nachkontrollen kontrolliert die Datenschutzbeauftragte die Umsetzung der Massnahmen, die in Kontrollberichten festgehalten werden.

		KEF	2019	2020
Beratungen	Dieser Leistungsindikator im KEF misst die Anzahl der Beratungen von öffentlichen Organen und Privatpersonen in Fragen des Datenschutzes und der Informationssicherheit.	650	657	856
Kontrollen	Dieser Leistungsindikator im KEF misst die Anzahl der Kontrollen (Datenschutzreviews) der Anwendung der rechtlichen, technischen und organisatorischen Vorschriften in öffentlichen Organen.	60	30	10
Aus- und Weiterbildungen	Dieser Leistungsindikator im KEF misst die durchgeführten Weiterbildungsangebote für öffentliche Organe (Seminare, Kurse, Workshops und Referate).	20	27	27
Vernehmlassungen	Dieser Leistungsindikator im KEF gibt Auskunft über die Anzahl der Vernehmlassungsantworten, Stellungnahmen und Mitberichte.	18	25	13
Massnahmenumsetzung	Dieser Wirkungsindikator im KEF misst die prozentuale Umsetzung der Massnahmen, die nach Datenschutzreviews zur Behebung von Mängeln vorgeschlagen wurden.	80 %	66 %	52 %
Website-Besuche	Dieser Wirkungsindikator im KEF gibt Auskunft über die Nutzung der Informationsangebote.	45 000	47 618	79 705

Homeoffice, aber sicher!

13 Regeln für das Homeoffice

14 Komplexe Fragen zur digitalen Zusammenarbeit

16 Prorektor-Wahl per Videokonferenz

17 Corona-Pandemie und Privatsphäre – als Video

Regeln für das Homeoffice

Datenschutzfreundliche Anwendungen gewährleisten noch kein sicheres Homeoffice. Vielmehr sind einfache, aber wirkungsvolle Regeln für die Einrichtung und das Verhalten bei der Arbeit zu Hause zu beachten. Die Datenschutzbeauftragte publizierte einen Leitfaden, der kurz und bündig die wesentlichen Punkte zusammenfasst.

Die öffentliche Diskussion drehte sich um technische Voraussetzungen für die Zusammenarbeit auf Distanz. Diese waren grundlegend für das Funktionieren der Verwaltung und anderer Institutionen im ersten Jahr der Corona-Pandemie. Doch blieben die Risiken kaum beachtet, die damit verbunden waren, dass plötzlich Personendaten und heikle Geschäftsdaten nicht mehr im gesicherten Umfeld des Büros, sondern im Wohnzimmer bearbeitet wurden. Der private Computer diente zum Beispiel nicht mehr nur dem Gamen, sondern es wurden darauf beispielsweise die Personendaten von Sozialhilfeempfängerinnen und Sozialhilfeempfängern bearbeitet. Da die Schulen geschlossen waren, hielten sich auch Kinder in der Nähe des behelfsmässig eingerichteten Arbeitsplatzes am Esstisch auf und hörten bei der Videokonferenz mit.

Die Herausforderung fängt also mit dem richtigen Arbeitsplatz innerhalb der eigenen vier Wände an. Wo kann ungehindert am Bildschirm gearbeitet werden, ohne dass Dritte Einblick in die Informationen bekommen? Wie kann ungestört und ohne Zuhörende aus dem Familienumfeld telefoniert werden? Auch im digitalen Zeitalter bestehen analoge Probleme: Wie können Papiere verwahrt und ungehindert bearbeitet werden, ohne Informationen offenzulegen? Was kann in der Altpapiersammlung entsorgt werden? Diese wenigen Fragen zeigen, was alles zu beachten ist.

Einfache Massnahmen können ein gutes Mindestmass an Sicherheit gewährleisten. Jedoch muss das Bewusstsein für die Risiken vorhanden sein. Der Schwatz bei der Kaffeemaschine im Büro ist weit weniger verfänglich, als ein Gespräch mit dem Partner oder der Partnerin beim Teekochen in der privaten Wohnung. Das Homeoffice verlangt nach kleinen Verhaltensanpassungen aller Mitarbeitenden, die zur täglichen Routine werden müssen.

Die Datenschutzbeauftragte beleuchtet im Leitfaden 8 Regeln für das Homeoffice auch die technischen Aspekte, die den Datenschutz im Homeoffice gewährleisten. Wenn mit privaten Geräten gearbeitet wird oder Geräte im Einsatz sind, die nicht zentral über die Informatikabteilung gewartet werden, ist die Eigenverantwortung besonders wichtig. Auch im klassischen Büroumfeld gelingen Angriffe auf die Informationssicherheit meist über die Mitarbeitenden – Stichwort Social Engineering. Wenn in privaten Räumlichkeiten gearbeitet wird, nimmt dieses Risiko stark zu. Im Homeoffice bestehen zusätzliche Ablenkungsfaktoren. Ein Mausklick, der zu schnell oder zu viel gemacht wird, kann zu grösserem Schaden führen, auch weil sich private und geschäftliche Informationen auf dem benutzten Gerät vermischen. Bei der Arbeit zu Hause sind deshalb Routinen strikt einzuhalten, E-Mails von unbekannten Absendern besonders zu prüfen sowie System- und Softwareaktualisierungen regelmässig zu installieren.

8 Regeln für das Homeoffice auf
www.datenschutz.ch

Komplexe Fragen zur digitalen Zusammenarbeit

Aussergewöhnliche Zeiten verlangen nach aussergewöhnlichen Massnahmen. Dennoch dürfen sicherheitsrelevante Aspekte nicht vernachlässigt werden. Die neue Situation im Homeoffice verunsicherte die Mitarbeitenden öffentlicher Organe. Die Datenschutzbeauftragte publizierte deshalb zu Beginn des ersten Lockdowns eine Produkteliste für die digitale Zusammenarbeit.

Öffentliche Organe tragen eine besondere Verantwortung für die Personendaten der Einwohnerinnen und Einwohner. Datenschutz funktioniert präventiv. Wenn Personendaten in die falschen Hände geraten sind, kann die Kontrolle darüber nicht mehr zurückerlangt werden.

Soforthilfe geleistet

Homeoffice und Homeschooling kamen plötzlich. Das weitere Funktionieren der Verwaltung und des Schulbetriebs war nur dank digitaler Produkte möglich. Schnelles Handeln war auch für die Datenschutzbeauftragte angesagt. Sie prüfte die am meisten angefragten Produkte zur digitalen Zusammenarbeit summarisch und veröffentlichte innert wenigen Tagen eine Produkteliste auf ihrer Website. In- und ausländische Datenschutzstellen, aber auch Bildungsdirektionen und Bildungsministerien verwiesen während des Lockdowns auf die Zürcher Datenschutzwebsite.

Die Entscheidung für ein bestimmtes Produkt liegt beim öffentlichen Organ. Es bleibt für die Personendaten verantwortlich und darf auch unter Druck die Sicherheit der Personendaten nicht vernachlässigen. Nicht jedes Produkt ist für jeden Zweck geeignet. Das öffentliche Organ muss in jedem einzelnen Fall überlegen, zu welchem Zweck ein digitales Produkt genutzt werden soll. Für die Auswahl eines Produkts spielt die Art der bearbeiteten Personendaten ebenso eine Rolle wie die Geschäftsbedingungen des Anbieters. Das öffentliche Organ muss wissen, welches Recht angewendet wird, welcher Gerichtsstand gilt, ob ein Kontrollrecht verankert ist, wo die Daten bearbeitet und welche Cookies eingesetzt werden. Die Möglichkeiten der Datenverschlüsselung sind von zentraler Bedeutung. Die Anforderungen stehen im Leitfaden der Datenschutzbeauftragten Bearbeiten im Auftrag konkretisiert. In einer umfassenden Analyse sind die Risiken im Einzelfall abzuwägen mit Blick auf die vom Gesetz geforderten Massnahmen und von den Anbietern erfüllten Anforderungen.

Risikoanalyse vor dem Einsatz
Datenschutzkonforme oder zumindest datenschutzfreundliche Messengers und Videokonferenzsysteme auszuwählen, ist schwierig. Die Plattformen verfügen über unterschiedliche Funktionen von der reinen Kommunikation über das Teilen von Dokumenten bis zum Speichern des Gesprächsinhalts. Aber allen Produkten ist gemeinsam, dass sie die Anforderungen einer Auslagerung respektive einer Auftragsdatenbearbeitung erfüllen müssen. Beim Anbieter einer Kommunikationsplattform fallen zudem viele Randdaten wie Name, IP-Adresse oder Dauer des Gesprächs an. Diese werden in einer Cloud gespeichert und in vielen Fällen bis zum Löschen des Kontos aufbewahrt.

Die Datenschutzbeauftragte prüfte Messengers und Videokonferenzsysteme anhand der Dokumente, welche die Anbieter zur Verfügung stellten. Sie veröffentlichte ein Merkblatt Messengers und Videokonferenzsysteme mit einer Beurteilung nach den wichtigsten Kriterien.

Vor dem Einsatz eines Produkts muss das öffentliche Organ entscheiden, welches Produkt für die jeweilige Kommunikation geeignet ist. Für sensitive Bereiche wie die Strafverfolgung oder im Spitalbereich können gewisse Produkte ungeeignet sein. Der konkrete Sachverhalt ist auch hier zu berücksichtigen. Ein Produkt kann in einem Spital vielleicht intern zum Austausch im administrativen Bereich genutzt werden, ist aber ungeeignet für die Nutzung in Bereichen, in denen auch Patientendaten übermittelt werden. Das Merkblatt Messengers und Videokonferenzsysteme unterstützt bei dieser Risikoabwägung mit Fragen und Tipps:

- Zu welchem Zweck soll die Software eingesetzt werden?
- Welche Arten von Informationen sollen ausgetauscht werden?
- In welchem Bereich soll die Software eingesetzt werden?
- Welches Recht ist anwendbar und welcher Gerichtsstand gilt?
- Wo werden die Randdaten gespeichert: im EU-Raum, in der Schweiz oder in anderen Ländern?
- Gibt es eine Verschlüsselung?
- Gibt es eine Zwei-Faktor-Authentifizierung?

Nach der Auswahl einer Anwendung muss entschieden werden, welche weiteren Massnahmen je nach Nutzung umgesetzt werden sollen. So kann das Speichern von Dokumenten und Gesprächsinhalten gesperrt oder das Attention Tracking deaktiviert werden.

Microsoft 365 in der Verwaltung
Organe der Verwaltung möchten Microsoft 365 datenschutzkonform nutzen. Sie drängen auf eine Antwort der Datenschutzbeauftragten. Die Konferenz der schweizerischen Datenschutzbeauftragten privatim unterstützte die Schweizerische Informatikkonferenz (SIK) bei Verhandlungen mit Microsoft. Daraus entstand der SIK-Rahmenvertrag, in dem für Datenschutzbelange die Anwendung von schweizerischem Recht und ein schweizerischer Gerichtsstand verankert sind. Trotzdem muss auch bei dieser Auslagerung eine Risikoabwägung vorgenommen werden. Es gilt zu beurteilen, mit welchen Produkten des Microsoft-365-Pakets welche Personendaten ausgelagert werden sollen. Neben dem Ort der Speicherung sind die Zugriffsberechtigungen und die Art der Verschlüsselung zu berücksichtigen. Zusätzlich sind ausländische Gesetze wie der CLOUD Act zu beachten. In diesem Zusammenhang sind Personendaten unter speziellen Geheimnispflichten wie dem Berufs- oder Steuergeheimnis im Rahmen der Risikoanalyse besonders zu berücksichtigen.

Schrems II oder der ungenügende Schutz durch das Privacy Shield
Im letzten Sommer stufte der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte die USA als Land mit nicht angemessenem Datenschutzniveau ein. Er reagierte damit auf ein Urteil des Europäischen Gerichtshofs, in dem der Datenschutz durch das Privacy-Shield-Abkommen als ungenügend eingeschätzt wird (Schrems II). Auch die Standardvertragsklauseln sind allein nicht ausreichend für einen Transfer von Personendaten in Länder ohne angemessenen Datenschutz. Deshalb müssen neue Wege gesucht werden, um die Personendaten angemessen zu schützen. Verschiedene Stellen erarbeiten Lösungsansätze. Auf europäischer Ebene werden die Standardvertragsklauseln revidiert.

Nutzen öffentliche Organe Cloud-Dienste, die einen Transfer von Personendaten in die USA beinhalten, müssen sie mit einer Kombination von rechtlichen und organisatorisch-technischen Massnahmen einen angemessenen Schutz sicherstellen. Eine hybride Cloud, bei der ein Teil der Personendaten lokal gespeichert wird, oder zusätzliche vertragliche Absicherungen vermindern beispielsweise das Risiko. Weitere Möglichkeiten sind etwa Verschlüsselung der Personendaten, wenn der Schlüssel beim öffentlichen Organ liegt, oder die Pseudonymisierung der Personendaten.

Die Datenschutzbeauftragte informiert auf ihrer Website www.datenschutz.ch über die Entwicklungen in diesem Bereich.

Prorektor-Wahl per Videokonferenz

Informationen in Bewerbungsdossiers stellen Persönlichkeitsprofile und somit besondere Personendaten dar. Sie bedürfen eines besonderen Schutzes bei der Bearbeitung. Die Datenschutzbeauftragte beantwortete die Frage, ob die Wahl des Prorektors einer Berufsschule als Videokonferenz durchgeführt werden darf.

In der Praxis werden dem Gesamtkonvent alle Bewerbungsunterlagen vorgestellt. Die Datenschutzbeauftragte hat dies als unverhältnismässig beurteilt. Zwar wird bei den Bewerbenden eine Einwilligung eingeholt. Diese kommt jedoch nicht freiwillig zustande, da sie für die Teilnahme am Bewerbungsverfahren vorausgesetzt wird. Bei der digitalen Durchführung des Verfahrens bestehen zusätzliche Risiken für die Persönlichkeitsrechte, da die Bewerbungsunterlagen hier einfacher weiterverbreitet werden können. Die Verhältnismässigkeit, aber auch die Informationssicherheit sind deshalb noch stärker zu berücksichtigen. Die Aufnahmefunktion des Videokonferenztools ist zu deaktivieren und den Teilnehmenden ist die Aufnahme mit Hinweis auf die Strafbarkeit zu untersagen. Die Wahl selber ist entweder brieflich oder mit verschlüsselten E-Mails durchzuführen, damit das Wahlgeheimnis gewährleistet ist.

Corona-Pandemie und Privatsphäre – als Video

Die Öffentlichkeit diskutierte im letzten Jahr ausgiebig über Privatsphäre und Datenschutz. Oft zeigte sich, dass die Grundsätze dieser Grundrechte wenig bekannt sind. Dies trifft nicht zu auf die Teilnehmenden des Datenschutz-Video-Wettbewerbs. Ihre Beiträge beschäftigen sich mit der Frage, wie viel Persönliches wir in Zeiten von Corona freiwillig und unfreiwillig preisgeben.

Die Zugangsweisen der jungen Videomaker und Youtuber sowie die Aspekte, die sie in ihren Videos behandeln, könnten nicht unterschiedlicher sein. Beim erstplatzierten Beitrag handelt es sich um eine kleine Tragikomödie. Sehr prägnant illustriert der Kurzfilm die Tücken des Homeoffice: In einem Videocall offenbart ein geschätzter Mitarbeiter Einblicke in sein Privatleben, die seinen Chef quasi gegen den eigenen Willen dazu bringen, ihn zu entlassen. Die weiteren ausgezeichneten Videos befassen sich mit der allgemeinen Unsicherheit in der bedrohlichen Krisensituation. Der zweitplatzierte Beitrag nutzt dafür eine witzige Animation, während das drittplatzierte Video auf schnelle und direkte Tiktok-Ästhetik setzt. Wie viele persönliche Informationen muss ich zur Eindämmung der Virusverbreitung bekanntgeben? Und bin ich sicher, dass meine Solidarität nicht missbraucht wird?

Fernunterricht, der bildet

19 Fragen zum digitalen Unterricht
21 Datenschutz online lernen

Fragen zum digitalen Unterricht

Plötzlich mussten Schulen den Bildungsauftrag im Fernunterricht erfüllen. Die Datenschutzbeauftragte sah sich mit einer grossen Anzahl Anfragen konfrontiert. Sie prüfte Plattformen und Anwendungen und sensibilisierte die Schulen und Lehrpersonen für die datenschutzrechtlichen Fallen.

Dringliche Anfrage im Kantonsrat
Nach dem ersten Corona-Lockdown reichten Kantonsrätinnen und Kantonsräte verschiedener Parteien eine dringliche Anfrage ein zum Einsatz von Videokonferenz- und Meeting-Tools in Volksschulen. Darin nahmen sie Bezug auf den Produktekatalog für digitale Zusammenarbeit in der Corona-Krise, den die Datenschutzbeauftragte auf ihrer Website veröffentlicht hatte. Die Bildungsdirektion ersuchte die Datenschutzbeauftragte um einen Mitbericht.

Die Datenschutzbeauftragte bekräftigte, dass jedem Einsatz von digitalen Produkten eine Risikoanalyse vorausgehen muss. Der Produktekatalog diente während der Krise zur Unterstützung bei dieser Risikoanalyse. Die Datenschutzbeauftragte hatte die Produkte des Katalogs summarisch geprüft. Dabei fokussierte sie auf Eigenschaften, die einen datenschutzkonformen Einsatz ausschliessen würden. Falls solche nicht gefunden wurden, stufte sie aufgrund der Krisensituation die Nutzung für vorläufig zulässig ein. Die Datenschutzbeauftragte fasste im Mitbericht die technischen und rechtlichen Hauptkriterien zusammen, die für den Entscheid über den Einsatz von digitalen Produkten massgebend sind, etwa die Sensitivität der Personendaten, die darüber gespeichert oder geteilt werden, der Standort der Datenspeicherung oder die Verschlüsselung der Personendaten.

Lernplattformen datenschutzfreundlich einsetzen
Lernplattformen ermöglichen eine zeit- und ortsunabhängige Vermittlung von Wissen und sind im Fernunterricht unentbehrlich. Auf einfache und schnelle Weise können Lehrpersonen mit den Schülerinnen und Schülern kommunizieren, ihnen Aufgaben zuteilen und Prüfungen durchführen. Dabei werden viele Personendaten der Lernenden aufgezeichnet, die zur Erfüllung des Bildungsauftrag der Schule nicht notwendig sind. Darunter fallen Zeitpunkt und benötigte Zeit für das Erledigen einer Aufgabe. Daraus können Persönlichkeitsprofile erstellt werden. Die Schule darf diese Personendaten nicht auswerten.

Beim Einsatz einer Lernsoftware bearbeiten die Produkteanbieter Personendaten. Die Schule bleibt allerdings für die Personendaten verantwortlich. Die eingesetzten Produkte müssen deshalb sorgfältig ausgewählt werden. Die Schule muss einen Vertrag abschliessen, der die notwendigen Bestimmungen für den Schutz der Personendaten enthält. Da in der Regel Personendaten der Lernenden betroffen sind, müssen schweizerisches Recht anwendbar und ein schweizerischer Gerichtsstand verankert sein. Zudem sind geeignete Schutzmassnahmen zu bestimmen und vertraglich festzuhalten. Am besten erstellt die Schule ein Konzept mit den wichtigsten Punkten. Dazu gehören die Kategorisierung der Personendaten nach deren Sensitivität und die

Bestimmung technischer Massnahmen wie Verschlüsselung. Die Aufbewahrungsfristen müssen festgelegt werden, wie auch eine allfällige Protokollierung der Zugriffe, das Vorgehen zur Authentifizierung und die Anforderungen an Passwörter oder E-Mail-Adressen. Ein Rollen- und Berechtigungskonzept gewährleistet die Transparenz darüber, wer zu welchen Zwecken Zugriff auf die Personendaten hat. Das öffentliche Organ hat das Produkt so zu konfigurieren, dass nicht notwendige (Rand-)Daten gar nicht erhoben werden, falls dies möglich ist.

Die Schulen müssen die Lernenden und bei jüngeren Kindern auch ihre Eltern informieren über die Art, den Umfang, den Zweck und die Bearbeitung respektive die Nutzung der Personendaten.

Tracker in Lernplattformen
Zu Beginn der Corona-Krise vergrösserte sich das Angebot an Lernplattformen und digitalen Produkten für den Fernunterricht schnell. Die Datenschutzbeauftragte machte darauf aufmerksam, dass bei einem unkontrollierten Einsatz digitaler Produkte Persönlichkeitsprofile entstehen können. Sie rät deshalb zur anonymisierten oder pseudonymisierten Nutzung. Die Eltern und die Schülerinnen und Schüler sind über mögliche Auswertungen zu informieren. Die Schulen müssen sich in jedem Fall überlegen, zu welchem Zweck digitale Produkte genutzt werden sollen.

Schulen mussten sehr schnell vom Präsenzunterricht auf Fernunterricht umstellen. Die Registrierung der Schülerinnen und Schüler für die Lernplattformen erfolgte ohne Information der Eltern. Oft wurde nicht abgeklärt, was der Einsatz eines Produktes längerfristig bedeuten kann. Personendaten, die einmal in einer ungeeigneten Datenbank gespeichert wurden, werden sehr wahrscheinlich nie wieder gelöscht. Die Datenschutzbeauftragte wies darauf hin, dass das öffentliche Organ die Verantwortung für die Personendaten trägt. Es hat vor der Wahl eines Produkts die Risiken der Nutzung abzuklären.

Aufmerksame, sensibilisierte Eltern informierten die Datenschutzbeauftragte über problematische Tracker in Lernplattformen für Grundschülerinnen und -schüler. Verschiedene Plattformen erstellten mit Cookies oder Tracking-Tools personenbezogene Auswertungen. Die Datenschutzbeauftragte unterstützte die Eltern und die verantwortlichen Anbieter von Produkten, die verbreitet im Einsatz waren. In einem Fall waren die Dienste Google Tag Manager und Google Analytics eingesetzt worden, bei denen personenbezogene Daten an das Unternehmen Google übermittelt werden. Bei der Evaluation von Alternativen sind rechtliche sowie organisatorisch-technische Fragen zu berücksichtigen. Die Datenschutzbeauftragte zeigte auf, dass die lokal gehostete Open-Source-Anwendung Matomo zur Erstellung von Nutzungsstatistiken genutzt werden kann.

Die Beratung der Datenschutzbeauftragten bewirkte den Ersatz der Tools, die unzulässigerweise Personendaten übermitteln, durch datenschutzkonforme Lösungen. Diese Erfahrungen zeigen, dass datenschutzkonforme Lösungen möglich sind, auch wenn eine unvorhergesehene Krisensituation keinen Zeitverlust erlaubt. Voraussetzung dafür sind aufmerksame und sensibilisierte Nutzerinnen und Nutzer, die auf Produkteanbieter treffen, die datenschutzkonforme Produkte anbieten wollen. So können Schulen und Lernende pädagogisch wertvolle Produkte datenschutzkonform in Anspruch nehmen und ein Fernunterricht, der bildet, kann aufgegleist werden.

Kamerazwang in Vorlesungen
Der Einsatz von Videokonferenzsystemen führte zu einer besonders grossen Nachfrage nach Unterstützung. Hier stellten sich Fragen zur Auswahl spezifischer datenschutzfreundlicher Produkte als auch zur konkreten Anwendung, da die Lösungen verschiedene Funktionen zur Verfügung stellen. Zentral ist die Frage, zu welchem Zweck ein Videokonferenzsystem eingesetzt werden soll.

Eine Hochschule verordnete ihren Studierenden einen Kamerazwang bei Online-Vorlesungen. Weiter forderte sie, dass Profilbilder hochgeladen würden. Auch Hochschulen dürfen nur die Daten erheben und bearbeiten, die für ihre Aufgabenerfüllung erforderlich sind. Die Datenschutzbeauftragte hat festgehalten, dass eine Pflicht, die Kamera bei Videokonferenzsystemen einzuschalten, unter gewissen Umständen gerechtfertigt sein kann, beispielsweise in Fällen von Pflichtvorlesungen oder in der damaligen Lockdown-Situation bei online stattfindenden Prüfungen. Die Datenschutzbeauftragte sah jedoch keinen Grund, weshalb Studierende Profilbilder auf ihr Konto beispielsweise bei Zoom laden müssten. Sie beurteilte diese Forderung der Hochschule als unverhältnismässig. Die Datenschutzbeauftragte riet den Betroffenen, mit der Schule in den Dialog zu treten.

Datenschutz online lernen

Die Ausbildungsaktivitäten der Datenschutzbeauftragten fanden üblicherweise im Präsenzunterricht statt. Das Online-Lernprogramm zum Datenschutz war bis 2020 die Ausnahme. Während der Corona-Krise war einiges anders. Zum Erliegen kamen die Ausbildungsaktivitäten aber nicht – im Gegenteil.

Verschiebungen und Absagen geplanter Angebote kamen nur selten vor. Der Zertifikatskurs CAS Datenschutzverantwortliche entstand aus der Zusammenarbeit der Datenschutzbeauftragten mit der Zürcher Hochschule für Angewandte Wissenschaften (ZHAW). Er konnte 2020 planmässig zwei Mal mit hoher Teilnehmerzahl durchgeführt werden. Organisatoren und Teilnehmende bewerteten die Beiträge der Datenschutzbeauftragten als sehr gut. Auch am CAS im Kindes- und Erwachsenenschutzrecht war die Datenschutzbeauftragte wieder aktiv und erfolgreich beteiligt.

Der Input der Datenschutzbeauftragten beim CAS Digital Leadership in Education der Pädagogischen Hochschule Zürich (PHZH) stiess auf besonderes Interesse. Die Corona-Krise machte die Digitalisierung im Schulbereich zu einem brennenden Thema. Der Datenschutzteil im CAS-Programm entwickelte sich zu einer angeregten Diskussionsrunde. Weiter arbeitete die Datenschutzbeauftragte mit dem kantonalen Personalamt bei einem Ausbildungsangebot für die Lernenden in der Verwaltung zusammen. Zudem führte sie mit der Universität Zürich und dem Universitätsspital Zürich eine Datenschutzlektion für Forschende in der Humanmedizin durch. Zu den umfangreichen Angeboten kamen kürzere Auftritte und Referate an verschiedenen Veranstaltungen. Hier lassen sich Wissensvermittlung, Sensibilisierung und Öffentlichkeitsarbeit erfolgreich und nachhaltig kombinieren.

Die Datenschutzbeauftragte war 2020 mit denselben Herausforderungen konfrontiert wie alle Akteurinnen und Akteure im Aus- und Weiterbildungsbereich. Bei Präsenzveranstaltungen galten teilweise strenge Schutzmassnahmen. Andere Angebote erfolgten komplett digital. So bot sich die Gelegenheit, unterschiedliche digitale Kommunikationstechnologien und -formen einem Praxistest zu unterziehen. Von dieser Erfahrung konnte die Datenschutzbeauftragte in ihrer Beratungstätigkeit im Bildungsbereich stark profitieren. Diese Erkenntnisse helfen, die Beratungstätigkeit noch praxisnäher zu gestalten.

In der Krise ist nicht alles anders

23 Auch in der Krise nicht alles offenlegen
25 Datenschutz im Datenüberfluss
27 Mit Doodle zum Gottesdienst anmelden
28 Gemeindeversammlung im Fernsehen
29 Universalschlüssel zu den Bibliotheken
30 Rayonverbot mit Electronic Monitoring

Auch in der Krise nicht alles offenlegen

Gerade in der Krise sind Einwohnerinnen und Einwohner auf den Schutz ihrer Grundrechte angewiesen. Grundrechte wie der Datenschutz dürfen nur eingeschränkt werden, wenn eine rechtliche Grundlage dies erlaubt und die Einschränkung geeignet und erforderlich ist, einen angestrebten Zweck zu erreichen.

Ein Vater wandte sich kurz vor den Sommerferien an die Datenschutzbeauftragte. Die Primarschule seines Kindes verlangte in einem Elternbrief die Offenlegung aller Reisepläne der Eltern und der Kinder in Länder, für die zum damaligen Zeitpunkt Quarantänebestimmungen galten.

Abklärungen der Datenschutzbeauftragten ergaben, dass die Schule eine Vorlage mit Textbausteinen des Volksschulamtes (VSA) missverstanden hatte. Die Offenlegung von Reiseplänen vor den Sommerferien ist weder erforderlich noch geeignet, um Ansteckungen mit dem Coronavirus zu verhindern. Die Eltern sind somit nicht dazu verpflichtet.

Auf Nachfrage der Datenschutzbeauftragten bestätigte das VSA, dass lediglich nach den Ferien eine Informationspflicht der Eltern gelte, wenn ein Kind infolge Quarantäne den Unterricht nicht besuchen kann. Die Vorlage des VSA enthielt keinen Hinweis auf eine Pflicht zur Information über Reisepläne. Das VSA hatte mit dem Elternbrief vor den Sommerferien beabsichtigt, die Eltern und Schülerinnen und Schüler an die Quarantänebestimmungen zu erinnern und den Hinweis anzubringen, dass kein Anspruch auf Fernunterricht bestehe.

Die Datenschutzbeauftragte half der Schule noch vor den Sommerferien, die Probleme mit dem Elternbrief zu bereinigen, und riet, die Eltern sofort aufzuklären. Sie wies die Schule auf die Pflicht hin, bisher erhaltene Daten über Ferienpläne und Destinationen zu löschen.

Einheitliche Regelung statt Chaos

Die Quarantäneregelungen hatten Konsequenzen für den Schulbetrieb nach den Ferien. Die Datenschutzbeauftragte informierte, dass das aktive Abfragen von Reisedestinationen auch nach den Ferien nicht Aufgabe der Schule und Lehrpersonen sei. Die Schulen bekamen von verschiedenen Seiten andere Ratschläge. Sie stellten sich die Frage, wie sie nach den Schulferien mit der Situation umgehen sollten. Die Schulen haben eine Fürsorgepflicht und müssen gewisse Massnahmen zur Prävention übertragbarer Krankheiten treffen. Das VSA wollte mit einem Leitungszirkular für Klarheit sorgen.

Das VSA erinnerte im Leitungszirkular daran, dass die Eltern für die Einhaltung der Quarantäne selbst verantwortlich sind und darüber bereits vor den Sommerferien informiert worden waren. Es hielt nochmals fest, dass die Schulen keine eigenen Nachforschungen zur Abklärung oder Überprüfung der Quarantänepflicht tätigen. Die Schule oder das Lehrpersonal sollten jedoch die betroffenen Eltern nochmals über ihre Verantwortlichkeit informieren, wenn sie vermuteten, dass sich eine Schülerin oder ein Schüler in Quarantäne befinden sollte. Wussten sie von der Quarantänepflicht einer Schülerin oder eines Schülers, sollte sie

respektive er nach Hause geschickt sowie die Eltern und der kantonale Schulärztliche Dienst informiert werden. Der Schulärztliche Dienst würde das weitere Vorgehen mit dem Kantonsärztlichen Dienst koordinieren. Die Quarantäne sollte wie Abwesenheit wegen Krankheit behandelt werden.

Die Datenschutzbeauftragte beurteilte die Regelungen des VSA als datenschutzkonform.

Fragen zum Gesundheitszustand vor Prüfungen

Eine Hochschule kontaktierte die Datenschutzbeauftragte in ihren Vorbereitungen auf die Prüfungen, die nach dem Lockdown wieder vor Ort stattfinden sollten. Den Prüfungskandidatinnen und -kandidaten sollte schriftlich mitgeteilt werden, dass sie nur an den Prüfungen teilnehmen dürfen, wenn sie sich absolut gesund fühlen. Zusätzlich erarbeitete die Schule einen Fragebogen zum Gesundheitszustand der Kandidatinnen und Kandidaten.

Personendaten dürfen bearbeitet werden, wenn dies zur Erfüllung der gesetzlich umschriebenen Aufgaben geeignet und erforderlich ist. Die Bearbeitung besonderer Personendaten wie Gesundheitsdaten muss in einem formellen Gesetz geregelt sein.

Die Datenschutzbeauftragte hielt fest, dass für den Fragebogen zum Gesundheitszustand verschiedene Bestimmungen als rechtliche Grundlage herbeigezogen werden können. Der Einsatz des Fragebogens muss jedoch auch durch ein öffentliches Interesse gerechtfertigt und verhältnismässig sein.

Die Hochschule wollte mit dem Fragebogen Personen davon abhalten, trotz Krankheit oder Symptomen an den Prüfungen zu erscheinen. Die Datenschutzbeauftragte befand, dass das Abfragen von Krankheitserscheinungen oder Unwohlbefinden für diesen Zweck nicht geeignet sei. Die Befragten könnten den Fragebogen trotz Krankheit mit «gesund» oder «keine Symptome» ausfüllen. Die Datenschutzbeauftragte schlug vor, die Punkte des Fragebogens als Hinweis in die vorbereitete Covid-Richtlinie für Prüfungen aufzunehmen. Alle Prüfungskandidatinnen und -kandidaten seien darüber aufzuklären, dass sie bei Vorliegen von Symptomen nicht an einer Prüfung erscheinen dürfen. Zu Dokumentationszwecken und um die Hürde für die Umgehung zu erhöhen, könnte verlangt werden, die Kenntnisnahme der Regeln mit der Unterschrift zu bestätigen. Dadurch wird dieselbe Wirkung erzielt wie durch den Fragebogen, ohne dass Gesundheitsdaten gespeichert werden.

Fluggastdaten zur Kontrolle der Meldepflicht

In der Sommerferienzeit waren die Fluggesellschaften verpflichtet, die Kontaktdaten von Flugpassagieren aufzunehmen und dem Bundesamt für Gesundheit (BAG) abzuliefern. Das BAG sollte die Daten danach an die Kantone übermitteln, damit diese die Meldepflicht für Reisende aus Risikoländern kontrollieren konnten. Der Kanton Zürich sah in diesem Vorgehen eine Gefahr von zeitlichen Verzögerungen. Er setzte die Kantonspolizei ein, um die Kontaktdaten direkt bei den Fluggesellschaften abzuholen und der Gesundheitsdirektion auszuhändigen.

Die Datenschutzbeauftragte erfuhr von diesem Vorgehen zunächst aus den Medien. Nachträglich entstand ein konstruktiver Austausch mit der Sicherheitsdirektion. Sie konsultierte die Datenschutzbeauftragte zu den Bemühungen des Kantons, das bereits praktizierte Vorgehen mit dem BAG schriftlich zu regeln. Der Kanton Zürich übernahm die digitale Erfassung der Kontaktkarten der Fluggesellschaften auch für andere Kantone. Die Datenschutzbeauftragte erhielt die Gelegenheit, das Vorgehen bei der Erfassung der Kontaktdaten vor Ort zu überprüfen. Gestützt auf ihre Beobachtungen regte sie Anpassungen der Bearbeitungsprozesse an.

Datenschutz im Datenüberfluss

Die Gesundheitsdirektion musste beim Contact Tracing grosse Mengen Personendaten bearbeiten. Dabei handelte es sich um Gesundheitsdaten und somit besondere Personendaten. Dies verlangte besondere Aufmerksamkeit beim Datenschutz. Die betroffenen Personen mussten sich auch in Krisenzeiten auf den Schutz ihrer Privatsphäre verlassen können. Die Gesundheitsdirektion arbeitete eng mit der Datenschutzbeauftragten zusammen.

Kontrolle über Contact-Tracing-Daten behalten
Mitte Juli 2020 wurde die Gesundheitsdirektion beauftragt, die Kapazitäten des Contact Tracings auszubauen, um die Nachverfolgung von mindestens 100 Neuinfektionen pro Tag gewährleisten zu können. Sie vergab einen Teil des Contact Tracings an eine private Firma, um den Kantonsärztlichen Dienst zu entlasten. Die Gesundheitsdirektion wandte sich an die Datenschutzbeauftragte, um die Einhaltung der datenschutzrechtlichen Vorgaben bei diesem Outsourcing zu überprüfen. Die Datenschutzbeauftragte gab rasch konkrete Anregungen zur Erstellung eines Informationssicherheitskonzeptes sowie zu den datenschutzrechtlichen Bestimmungen. Somit konnte sichergestellt werden, dass die Gesundheitsdirektion die Verantwortung und die Kontrolle über die Contact-Tracing-Daten und ihre Sicherheit behält.

Sicherer Umgang mit Daten quarantänepflichtiger Personen
Aufgrund von Vorschriften des Bundes müssen sich Personen bei der Einreise aus einem Risikoland bei der Gesundheitsdirektion melden und in Quarantäne gehen. Die Gesundheitsdirektion wollte diese Meldepflicht für die Einreisenden so einfach wie möglich gestalten. Dafür musste sie im Sommer 2020 innert weniger Tagen ein mehrsprachiges Online-Formular bereitstellen. Die Datenschutzbeauftragte beriet die Gesundheitsdirektion, wie sie die Informationssicherheit bei der Bearbeitung der Daten von quarantänepflichtigen Personen einhalten kann, beispielsweise durch die Verwendung verschlüsselter E-Mails und Excel-Dokumente sowie dem Einsatz von sicheren Webtransfers.

Covid-19-Schutzkonzepte und der Schutz der Personendaten
Eine Kantonsratsanfrage befasste sich mit dem Schutz von Personendaten im Rahmen von Covid-19-Schutzkonzepten. Für die Antwort lud die Gesundheitsdirektion die Datenschutzbeauftragte zum Mitbericht ein. Die Datenschutzbeauftragte wies darauf hin, dass die Datenbearbeitung durch private Betriebe wie Restaurants unter die Aufsicht des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) fallen. Die Datenschutzbeauftragte ist für die Aufsicht über die Datenbearbeitungen der öffentlichen Organe im Kanton Zürich zuständig. Bei Anfragen im Zusammenhang mit der datenschutzrechtlichen Umsetzung der Schutzkonzepte durch öffentliche Organe hat sie diese beraten.

Bedenken bei Angabe von Kundenkontakten
Die Datenschutzbeauftragte erhielt eine Anfrage einer gemeinnützigen Institution, die junge Erwachsene zur Berufsintegration berät. Die jungen Erwachsenen werden von der IV und vom RAV vermittelt. Die Institution wollte wissen, wie sie mit der Aufforderung zur Weitergabe der Kontaktangaben umgehen solle. Die Personendaten geben Auskunft über die aktuelle soziale oder gesundheitliche Situation der Personen. Sie sind deshalb als sensitiv einzustufen. Die Datenschutzbeauftragte erklärte, dass die Bekanntgabe der

→

Personendaten an den Kantonsärztlichen Dienst durch das Epidemiengesetz gerechtfertigt sei. Sie riet der Institution, die jungen Erwachsenen darauf aufmerksam zu machen, dass sie ihre Daten dem Kantonsärztlichen Dienst auf Aufforderung bekanntgeben muss.

Corona-Infizierte haben ein Recht auf Datenschutz

Beim Contact Tracing werden Personen angerufen und mit der Information konfrontiert, dass einer ihrer Kontakte mit Corona infiziert ist. Das weckt Ängste und führt zu einschneidenden Einschränkungen durch die Quarantänepflicht. Häufig wird den Contact Tracern die Frage gestellt, wer die Kontaktperson mit dem positiven Testresultat sei. Die Gesundheitsdirektion bat die Datenschutzbeauftragte um eine Stellungnahme, ob die Identität der infizierten Person – Indexfall genannt – bekanntgegeben werden dürfe.

Diese Information ist wichtig für Personen, die sich gegen eine Quarantäneanordnung zur Wehr setzen möchten. Sie erhalten eine begründete Verfügung, gegen die sie auf dem Rechtsweg vorgehen können. Es ist kaum möglich, eine Begründung zu formulieren, ohne die Identität des Indexfalls bekanntzugeben. Für die erkrankte Person ist es jedoch ein zusätzlicher einschneidender Eingriff in ihre Persönlichkeitsrechte, wenn ihre Infektion allen Kontaktpersonen bekanntgegeben wird. Bei einem Infektionsfall in einem Restaurant würde so möglicherweise eine sehr persönliche Information einer erheblichen Zahl von Personen bekanntgegeben.

Die Datenschutzbeauftragte betonte, dass die Bekanntgabe der Identität der infizierten Person nur zulässig ist, wenn sie für den Zweck des Contact Tracings notwendig ist. Nach Gesprächen mit der Gesundheitsdirektion regte sie ein schrittweises Vorgehen an. Zunächst ist der Indexperson vorzuschlagen, Kontaktpersonen selbst zu informieren. Als weitere Möglichkeit kann sie gefragt werden, ob sie der Bekanntgabe ihrer Identität zustimme. Wenn die Indexperson beides ablehnt, ist eine Quarantäneanordnung ohne Personenbezug zu begründen. Die infizierte Person ist nur eindeutig zu identifizieren, wenn die Begründungspflicht dies verlangt, etwa wenn eine Kontaktperson den Rechtsweg beschreiten möchte.

Keine Weitergabe von Contact-Tracing-Daten für Strafuntersuchung

Ein Restaurantbesitzer fragte die Datenschutzbeauftragte an, ob er verpflichtet ist, Kontaktdaten seiner Gäste an die Kantonspolizei herauszugeben. Die Ermittlung betraf ein schwerwiegendes Gewaltdelikt in unmittelbarer Nähe seines Restaurants.

Die Kontaktdaten sind zweckgebunden für das Contact Tracing erhoben worden. Bei einer Strafuntersuchung können auch Informationen genutzt werden, die in einem anderen Zusammenhang gesammelt wurden. Dafür gelten allerdings Einschränkungen. Eine umfassende Beweisausforschung ist nicht erlaubt. Gezielte Ermittlungen bei einem konkreten Tatverdacht sind erlaubt. Der Restaurantbesitzer muss also nur die Kontaktdaten mit einem nahen Bezug zur Straftat herausgeben, beispielsweise der männlichen Gäste, die zu einem bestimmten Zeitpunkt das Restaurant verliessen, falls diese Kriterien für die Ermittlungen relevant sind.

Anonyme Auswertung von Contact-Tracing-Daten

In den Anfangszeiten der Pandemie mangelte es an epidemiologischen Daten. Die Zusammenarbeit zwischen der Gesundheitsdirektion und dem Statistischem Amt sollte diese Situation verbessern. Dafür wurden grosse Mengen von Personendaten mit Gesundheitsbezug bearbeitet. Auf Anregung der Gesundheitsdirektion unterstützte die Datenschutzbeauftragte die Beteiligten bei der Ausarbeitung einer Zusammenarbeitsvereinbarung. Sie stellte dabei sicher, dass die Verantwortlichkeit für die Privatsphäre der betroffenen Personen angemessen geregelt wurde.

Mit Doodle zum Gottesdienst anmelden

Nach dem Lockdown im Frühling 2020 wurde auch ein Schutzkonzept für den Kirchenbesuch entwickelt. So war die Anzahl der teilnehmenden Personen begrenzt und ihre Kontaktdaten mussten registriert werden. Eine Kirchgemeinde wollte die Registrierung über das Online-Terminplanungstool Doodle lösen. Ein Journalist wandte sich an die Datenschutzbeauftragte und wies darauf hin, dass die Kontaktdaten öffentlich einsehbar waren.

Angaben zu religiösen Aktivitäten sind besondere Personendaten. Die Datenschutzbeauftragte erklärte, dass eine telefonische Anmeldung den Schutz der Privatsphäre am besten gewährleisten würde. Wenn die personellen Ressourcen dafür in der aktuellen Krise fehlten, könnten auch Kirchgemeinden auf digitale Kanäle ausweichen. Bei der Wahl des Produkts sind die wichtigsten Anforderungen zu berücksichtigen, vor allem der Speicherort der Daten. Werbefinanzierte Gratisangebote sind für solche Zwecke ungeeignet.

Bei der Nutzung des Produkts steht die Privatsphäre der Kirchgängerinnen und Kirchgänger im Vordergrund. Eingebaute Schutzmassnahmen wie die anonymisierte Darstellung erhöhen die Vertraulichkeit. Allerdings kann die Kirche deren Zuverlässigkeit nicht vollständig abklären.

Deshalb sind weitere Massnahmen zu treffen. Besonders geeignet ist die Verwendung von Pseudonymen oder Initialen. Eine geschickte Kombination von Vorsichtsmassnahmen kann zu einer Lösung führen, die in der aktuellen besonderen Situation vertretbar ist.

Gemeinde-versammlung im Fernsehen

Gemeindeversammlungen sind im Kanton Zürich öffentlich. Jede Person kann als Gast teilnehmen, ohne ein besonderes Interesse anmelden zu müssen. Das Prinzip der Öffentlichkeit kennt jedoch Einschränkungen.

Dies illustriert der Fall eines Bürgers, der sich in einer Nachrichtensendung bei der Abstimmung an der Gemeindeversammlung wiedererkannte. Die Datenschutzbeauftragte hielt fest, dass Bild- und Tonaufnahmen an Gemeindeversammlungen nur erlaubt sind, wenn sie die Stimmberechtigten nicht beeinträchtigen.

Zulässig sind Gesamtaufnahmen, bei denen die einzelnen Stimmberechtigten nicht erkennbar sind. Die Versammlungsleitung hat die Teilnehmenden über die Aufnahmen zu informieren. Aufnahmen während Wahlen und Abstimmungen sind nicht zulässig. Der Schutz des Wahlgeheimnisses und der freien Meinungsbildung ist unter diesen Voraussetzungen gewährleistet.

Universalschlüssel zu den Bibliotheken

Die neue nationale Lösung Swisscovery soll den Zugang zu allen Bibliotheken der Schweiz ermöglichen. Jede Person kann mit einem einzigen Konto entsprechend ihrer Berechtigungen Bücher ausleihen. Swisscovery wird durch die Swiss Library Services Platform (SLSP) betrieben.

Die Universitäten Bern, Basel und Zürich meldeten Swisscovery bei den kantonalen Datenschutzbehörden zur Vorabkontrolle an. Die zuständigen Datenschutzbehörden dieser Kantone arbeiteten bei der Vorabkontrolle aufgrund der schweizweiten Bedeutung des Projekts zusammen. Bei kantonsübergreifenden Projekten fand schon früher ein Austausch zwischen verschiedenen Aufsichtsbehörden statt. Das vollständig koordinierte Vorgehen beim Swisscovery-Projekt war neu.

Die zentrale Herausforderung von Swisscovery lag in der Vielfalt der angeschlossenen Institutionen. Swisscovery muss sehr unterschiedlichen Bedürfnissen entgegenkommen, von grossen Institutionen wie der Universität Zürich und kleinen wie beispielsweise der Jesuitenbibliothek sowie Nutzenden unterschiedlicher Altersgruppen. Gleichzeitig müssen Institutionen aus dem privatwirtschaftlichen Bereich und aus allen Kantonen berücksichtigt werden. Die Datenschutzbehörden setzten sich in der Vorabkontrolle mit den vielen verschiedenen Rechtsgrundlagen auseinander, die zur Anwendung kommen. Die kantonalen Gesetze sehen die Teilnahme an Plattformen teilweise nicht ausdrücklich vor. Deshalb regten die Datenschutzbehörden für den Kanton Zürich an, eine konkrete Rechtsgrundlage zu schaffen. Weiter prüften sie die vertraglichen Grundlagen zwischen Institutionen und der SLSP und die technische Umsetzung der Plattform. Swisscovery kann ausschliesslich mit einer edu-ID genutzt werden. Die edu-ID wird durch die Stiftung Switch herausgegeben und wurde zur Identifizierung im schweizerischen Bildungssystem entwickelt. Die Datenschutzbehörden hinterfragten diese Anbindung kritisch. Sie regten Verbesserungen beim Registrierungsprozess der Nutzerinnen und Nutzer an. Sie sind transparent zu informieren, welcher Anbieter welche Personendaten bearbeitet.

Die Vorabkontrolle konnte nach mehreren Nachlieferungen der Institutionen abgeschlossen werden. Die Datenschutzbeauftragten halten im Bericht fest, dass der datenschutzkonforme Betrieb der Plattform möglich ist. Allerdings sind Nachbesserungen nötig. Dabei geht es einerseits um einzelne Aspekte, wie dem Umgang mit Cookies und der Optimierung interner Prozesse. Andererseits stellte sich die Grundsatzfrage nach einer wirksamen Kontrolle der Plattform. Die teilnehmenden Bibliotheken müssen die Möglichkeit haben, Audits durchzuführen oder zu veranlassen. Die Erfahrung der Datenschutzbeauftragten zeigt, dass die Überwachung der Anbieter schwierig zu koordinieren ist, wenn bei Projekten zahlreiche Institutionen in verschiedenen Kantonen beteiligt sind. Im Vorabkontrollbericht werden die Universitäten Bern, Basel und Zürich aufgefordert, Koordinationsmöglichkeiten zu prüfen.

Zudem beriet die Datenschutzbeauftragte einzelne Institutionen zu konkreten Umsetzungsfragen. Im Vordergrund stand der Zugang zu den Bibliotheken für Nutzerinnen und Nutzer ohne eigene E-Mail-Adresse.

Die Datenschutzbeauftragte wird die Entwicklungen bei Swisscovery weiter verfolgen und überwachen.

Rayonverbot mit Electronic Monitoring

Electronic Monitoring (EM), auch als elektronische Fussfessel bekannt, wird im Straf- und Massnahmenvollzug sowie als strafprozessuale Ersatzmassnahme eingesetzt. Künftig wird EM auch im Zivilrecht als präventive Massnahme zum Schutz gewaltbetroffener Personen angewandt, also zur Überwachung eines Rayonverbots.

EM ist die räumliche und zeitliche Überwachung einer Person. Die betroffene Person trägt einen elektronischen Sender. Der Sender übermittelt die Standortdaten an den EM-Server. Zur Ortung der überwachten Person wird entweder die Radiofrequenz-Technologie oder das Global Positioning Service (GPS) verwendet. Die Datenübertragung vom Sender zu den Servern erfolgt über das Mobiltelefonnetz.

Bei der räumlichen und zeitlichen Überwachung von Personen wird eine grosse Menge an sensitiven Personendaten bearbeitet. Da sie beim EM in Zusammenhang mit einer administrativen oder strafrechtlichen Verfolgung oder Sanktion bearbeitet werden, handelt es sich zudem um besondere Personendaten. Ihre Erfassung und weitere Bearbeitung stellen besondere Anforderungen an den Datenschutz und die Informationssicherheit. Die Datenschutzbeauftragte begrüsst es, dass ihre Behörde in den vergangenen Jahren mehrmals in das Projekt einbezogen wurde. Im Jahr 2013 prüfte sie die Ausschreibungsunterlagen für die EM-Technik und die Überwachungszentrale. Bei der Überführung vom Pilot- in den Regelbetrieb im Jahr 2018 prüfte sie die Massnahmen zum Datenschutz und zur Informationssicherheit.

2020 stellte sie fest, dass die Anforderungen an Datenschutz und Informationssicherheit als zentrale Punkte beim Betrieb des EM bereits weitgehend berücksichtigt und umgesetzt wurden. Als problematisch erachtete sie, dass das System auch Überwachungsdaten erfasst und Meldungen absetzt, wenn dies zur Überwachung der Auflagen nicht erforderlich ist. Die Ortung findet auch statt, wenn die Person die Auflagen nicht verletzt. Sie verlangte, dass diese widerrechtlich bearbeiteten Informationen zeitnah gelöscht werden.

Am Betrieb des EM sind neben öffentlichen Organen auch private Unternehmen beteiligt. Wenn Private im Auftrag eines öffentlichen Organs handeln, gelten für sie in Bezug auf Geheimhaltung und Informationssicherheit die gleichen Pflichten. Die Datenschutzbeauftragte konnte die Verträge der beauftragten Privaten nicht prüfen. Sie wies aber darauf hin, dass die kantonalen Vorgaben zur Informationssicherheit auf die Privaten zu übertragen sind. In Zusammenarbeit mit dem öffentlichen Organ konnten zahlreiche weitere Aspekte geklärt werden.

In Zukunft wollen alle Kantone der Schweiz die gleiche EM-Technologie und eine gemeinsame Überwachungszentrale betreiben. Die Datenschutzbeauftragte beteiligt sich in einer Arbeitsgruppe der Konferenz der schweizerischen Datenschutzbeauftragten privatim zu diesem Thema. Sie unterstützt die Projektleitung in Datenschutzfragen.

Überlegen in der Digitalisierung

32 Impulsprogramm Datenschutz
34 Go-live der neuen Kantonswebsite
35 Informationsrichtlinien für die Verwaltung
36 Elektronische Kommunikation in der Justiz
37 Mitwirkungspflicht im Asylverfahren
38 Mehr Informationssicherheit in den Gemeinden
39 Zurückblicken und vorausschauen

Impulsprogramm Datenschutz

Die Datenschutzbeauftragte pflegt eine konstruktive Zusammenarbeit mit den Stellen, die für die Projekte des Impulsprogramms Digitale Verwaltung zuständig sind. Der regelmässige Austausch mit der Abteilung Digitale Verwaltung und E-Government der Staatskanzlei hat sich bewährt.

Die Datenschutzbeauftragte konnte ihren Einblick in das Impulsprogramm Digitale Verwaltung weiter vertiefen. In vielen Projekten berät sie die Verantwortlichen. Sie prüfte zahlreiche Rechtsgrundlagenanalysen sowie Informationssicherheits- und Datenschutzkonzepte, nahm an Sitzungen und Workshops teil und konnte den Anliegen des Datenschutzes und der Informationssicherheit Gehör verschaffen.

Expo: Datenschutz in der Hermes-Projektmethodik
Im März 2020 hätten an einer Expo Projekte aus dem Impulsprogramm präsentiert werden sollen. Auch die Datenschutzbeauftragte wäre an diesem Anlass vor Ort vertreten gewesen, um über ihren Beitrag zur Digitalisierung der Verwaltung zu informieren. Trotz Verschiebung in den November konnte die Veranstaltung nicht physisch stattfinden, sondern musste digital durchgeführt werden. Die Datenschutzbeauftragte informierte über die Bedeutung des Gesetzes über die Information und den Datenschutz für die Digitalisierung der Verwaltung sowie die Neuerungen nach der Revision. Sie wies darauf hin, dass die Anliegen des Datenschutzes in die Hermes-Projektmethodik integriert sind, die für die Projekte des Impulsprogramms vorgeschrieben ist.

Datenstrategie als Kernstück
Das Projekt Datenmanagement/Datenstrategie (IP 3.1) ist ein Kernstück des Impulsprogramms. Im Rahmen dieses Projekts wurden grundlegende Fragen zum Umgang mit Personendaten behandelt. Die Datenschutzbeauftragte hat dieses Projekt eng begleitet. Besonders intensiv diskutiert wurde das Once-Only-Prinzip, wonach Personendaten nur einmal erhoben und danach von verschiedenen Stellen weiterverwendet werden sollen. Eine vollständige Umsetzung dieses Prinzips würde das Grundrecht auf Privatsphäre gefährden. Die Aufhebung der Zweckbestimmung für erhobene Personendaten ist beispielsweise nicht verfassungskonform. Die Datenschutzbeauftragte konnte sich im Projekt davon überzeugen, dass die Verantwortlichen die Gefahren erkannt haben und berücksichtigen.

Die Definition eines Stammdatensets zur behördenübergreifenden Nutzung gehört zu den Umsetzungsprojekten im Bereich Datenmanagement/Datenstrategie. Über den Umfang dieses Sets gehen die Vorstellungen auseinander. Die Datenschutzbeauftragte wird darauf achten, dass dieses Set, das der ganzen Verwaltung offensteht, nicht umfassende Informationen über Einwohnerinnen und Einwohner enthält. Denn diese müssen darauf vertrauen können, dass ihre Daten nicht zweckentfremdet werden. Weiter wird eine Data Community geschaffen. Die Datenschutzbeauftragte freut sich darauf, in diesem Rahmen das Thema Datenmanagement im Kanton weiter zu begleiten.

Elektronisch einbürgern
Das Gemeindeamt fragte die Datenschutzbeauftragte an, das Projekt eEinbürgerung zu begleiten. Hier soll eine Plattform für Einbürgerungsgesuche zur Verfügung gestellt werden. Im Einbürgerungsverfahren müssen viele und besonders persönliche Informationen eingereicht werden. Die Einhaltung der rechtlichen Vorgaben ist dabei ebenso wichtig wie die Sicherstellung eines angemessenen technischen Schutzes. Die Datenschutzbeauftragte begleitet das Projekt.

Richtplan-Mitwirkungsprozess digitalisieren
Über die Hälfte der Stellungnahmen im Mitwirkungsprozess bei Revisionen des Richtplans wird noch per Post eingereicht und nicht über das elektronische Eingabeformular. Diese Eingaben werden eingescannt und manuell in eine Datenbank übertragen. Das Amt für Raumentwicklung möchte diesen Ablauf durch einen Prozess ohne Medienbrüche ersetzen. Die Datenschutzbeauftragte prüfte im Projekt eVernehmlassung die Konzepte aus rechtlicher und organisatorisch-technischer Sicht und beantwortete verschiedene Einzelfragen.

Online-Steuererklärung ohne Zwei-Faktor-Authentifizierung
Die Einreichung der Steuererklärung im Kanton Zürich hat sich wesentlich verändert. Sie kann für das Jahr 2020 zum ersten Mal durchgehend elektronisch und ohne Unterschrift auf Papier eingereicht werden. Steuerpflichtige haben damit die Möglichkeit, nur durch Eingabe der AHV-Nummer und eines Passworts auf Steuerdaten aus dem Vorjahr zuzugreifen. Die Datenschutzbeauftragte äusserte sich zu dieser Änderung kritisch. Sie hat darauf hingewiesen, dass der Zugriff auf diese Personendaten über eine Zwei-Faktor-Authentifizierung zu erfolgen hat, wie dies im Bereich von Finanzdaten anerkannter Standard ist. Diese Forderung wurde vom kantonalen Steueramt bisher nicht erfüllt. Die Gespräche mit dem Steueramt dauern an.

Künstliche Intelligenz in der Verwaltung
Die Professorin Nadja Braun Binder der Universität Basel verfasste im Rahmen des Projekts IP 6.4 eine Studie zum Einsatz Künstlicher Intelligenz in der Verwaltung. Dafür führte sie zusammen mit der gemeinnützigen Organisation Algorithmwatch Experten-Interviews durch, auch mit der Datenschutzbeauftragten. Im Vordergrund standen die ethischen und rechtlichen Fragen. Die Datenschutzbeauftragte brachte ein, dass bei einem geplanten Einsatz Künstlicher Intelligenz immer eine Vorabkontrolle durch ihre Behörde durchgeführt werden muss, weil es sich um eine neue Technologie handelt. Zudem wies sie darauf hin, dass die Transparenz gegenüber der Bevölkerung höchste Priorität habe. Die Einwohnerinnen und Einwohner müssten immer wissen, wann Künstliche Intelligenz wie eingesetzt werde und welche Aufgaben sie genau übernehme.

Einsatz der Blockchain-Technologie
Die Datenschutzbeauftragte war im Rahmen mehrerer Workshops an der Erarbeitung einer Blockchain-Studie beteiligt. Sie konnte einbringen, dass staatliches Handeln einer gesetzlichen Grundlage bedarf. Für den Einsatz von Blockchain-Lösungen in der kantonalen Verwaltung wäre eine neue gesetzliche Grundlage nötig. Die Datenschutzbeauftragte erklärte, dass dem kantonalen Gesetzgeber Grenzen gesetzt sind. Übergeordnetes Datenschutzrecht verlangt beispielsweise, dass falsche Einträge geändert werden können. Bei der Blockchain-Technologie sind zwar Korrekturen möglich. Der Hinweis auf den falschen Eintrag bleibt jedoch bestehen. Zudem muss staatliches Handeln immer eindeutig einer Akteurin oder einem Akteur zugeordnet werden können, damit er in einem Schadenfall zur Verantwortung gezogen werden kann. Dies ist bei Blockchains nicht immer gewährleistet, da Akteurinnen und Akteure mit Pseudonymen beteiligt sein können. Der Austausch mit der Staatskanzlei war sehr konstruktiv. Die Datenschutzbeauftragte wurde bei der Erstellung des Leitfadens Blockchain in der kantonalen Verwaltung einbezogen. Sie konnte bewirken, dass die bereits in der Blockchain-Studie aufgezeigten datenschutzrechtlichen Herausforderungen auch im Leitfaden übernommen wurden. Damit wird das Verständnis für die Einhaltung datenschutzrechtlicher Vorgaben beim Einsatz von Blockchain in der Verwaltung gestärkt.

Go-live der neuen Kantonswebsite

Am 8. Juli 2020 ging der neue Webauftritt des Kantons Zürich online. Die Datenschutzbeauftragte war in die Vorarbeiten doppelt involviert. Einerseits war die eigene Website Teil des Webauftritts des Kantons. Andererseits hat die Datenschutzbeauftragte die Projektverantwortlichen zu Datenschutzaspekten beraten.

Die Ausgangslage für Webauftritte öffentlicher Organe unterscheidet sich von solchen privater Organisationen. Private Organisationen haben gestützt auf die Einwilligung der Nutzenden sehr viele Möglichkeiten zur Bearbeitung von Personendaten. Öffentliche Organe müssen sich hingegen auf ihre gesetzlichen Aufgaben beschränken. Online informieren gehört zu den Aufgaben öffentlicher Organe, jedoch gehört personenbezogenes Tracking beispielsweise nicht dazu. Aus diesen Gründen ist der Auftritt des Kantons deutlich abzugrenzen gegenüber kommerziellen Angeboten. Die Datenschutzbeauftragte hatte die Projektverantwortlichen zu den datenschutzrechtlichen Vorgaben beraten. Sie hatte angeregt, externe Inhalte etwa von Google, Youtube oder Facebook mit einer Zwei-Klick-Lösung einzubinden. Bei dieser Lösung werden Besucherinnen und Besucher darauf hingewiesen, dass sie die Website verlassen oder Personendaten weitergegeben werden. Diese Anregung wurde nur teilweise umgesetzt.

Die Datenschutzbeauftragte stellt auf der Website www.datenschutz.ch unter Datenschutz in öffentlichen Organen mehrere Merkblätter zur Erstellung einer datenschutzkonformen und sicheren Website zur Verfügung.

Informations-richtlinien für die Verwaltung

Die Datenschutzbeauftragte wurde vom Amt für Informatik (AFI) in die Ausarbeitung der Besonderen Informationssicherheitsrichtlinien (BISR) für die kantonale Verwaltung einbezogen.

Der Regierungsrat erliess 2019 die Allgemeine Informationssicherheitsrichtlinie (AISR). Sie dient der Umsetzung der gesetzlichen Vorgaben zur Informationssicherheit und gilt für die ganze kantonale Verwaltung. In der AISR ist eine Liste von 27 Themen enthalten, zu denen eine weiterführende Regelung zu erlassen ist. Es handelt sich dabei um Themen wie Identitäts- und Zugriffskontrolle, Verschlüsselungstechniken, Protokollierung und Überwachung. Die BISR konkretisieren die Anforderungen der AISR. Der Auftrag zur Ausarbeitung eines Entwurfs der Regelungen für die Mehrzahl der Themen ging an das AFI. Alle Entwürfe wurden in der Fachgruppe IKT-Sicherheit (FAGIS) besprochen und vom Gremium Steuerung Digitale Verwaltung und IKT (SDI) verabschiedet.

Die Datenschutzbeauftragte beteiligte sich an den Diskussionen in der FAGIS und konnte sich zu allen BISR-Entwürfen äussern. Besonders intensiv wurde der Entwurf zum Thema Datenklassifikation und -handhabung diskutiert. Die Datenschutzbeauftragte konnte aufzeigen, dass zur Klassifizierung von Informationen zwei verschiedene Raster angewendet werden müssen. Informationen sind gemäss BISR-Regelung als «öffentlich», «intern», «vertraulich» oder «geheim» zu klassifizieren. Dabei stehen Geheimhaltungsinteressen des Kantons im Vordergrund. Die Privatsphäre der Betroffenen ist ein davon unabhängiges Thema. Auch dort gibt es verschiedene Schutzniveaus. Manche Personendaten brauchen einen hohen Schutz, obwohl sie nicht als «geheim» klassifiziert sind. Die Datenschutzbeauftragte schätzt den Einbezug. Ihre Anregungen wurden in den BISR-Entwürfen mehrheitlich berücksichtigt.

Der Faktor Mensch in der Informationssicherheit
Das AFI präsentierte der Datenschutzbeauftragten ein Projekt zur Verbesserung der Sicherheitskultur in der kantonalen Verwaltung. Informationssicherheit ist der Kern des technischen Datenschutzes. Ohne Berücksichtigung des Faktors Mensch kann Informationssicherheit nicht verwirklicht werden. Die Awareness-Strategie des AFI berücksichtigt diese Zusammenhänge. Das AFI plant zahlreiche strukturierte Aktivitäten zur Sensibilisierung und zur Schulung von Mitarbeitenden des Kantons. Die Datenschutzbeauftragte begrüsst diese Initiative.

Elektronische Kommunikation in der Justiz

Das Bundesgesetz über die Plattform für die elektronische Kommunikation in der Justiz (BEKJ) soll die rechtlichen Voraussetzungen definieren für eine zentrale Plattform, über die Behörden, Gerichte, Anwaltschaft, Parteien und weitere Verfahrensbeteiligte Dokumente zustellen und empfangen können. Der Bund und die Kantone betreiben die Plattform gemeinsam. Dafür gründen sie eine Körperschaft, die zuständig ist für den Aufbau, den Betrieb, die Weiterentwicklung und die Sicherheit der Plattform.

Das BEKJ regelt neben der grundlegenden Organisation der Körperschaft auch die notwendigen Funktionalitäten der Plattform, um den Austausch von Dokumenten und die elektronische Akteneinsicht zu ermöglichen. Dazu gehört die Festlegung der Anforderungen an die Authentifizierung der Benutzerinnen und Benutzer.

Die Plattform ist abhängig vom Vertrauen aller Nutzerinnen und Nutzer. Dafür ist neben den gesetzlichen Grundlagen vor allem die Informationssicherheit von Bedeutung. Zumindest in familienrechtlichen, strafrechtlichen und sozialversicherungsrechtlichen Verfahren werden besondere Personendaten bearbeitet, was zusätzliche Anforderungen an die Informationssicherheit stellt. Die Gewährleistung der Informationssicherheit kann jedoch aufgrund des Vorentwurfs des Bundesgesetzes nicht beurteilt werden.

Die Datenschutzbeauftragte betonte in ihrer Stellungnahme, dass bei einem Projekt dieser Grösse und Brisanz die enge Zusammenarbeit mit den Datenschutzbehörden des Bundes und der Kantone notwendig ist. Bei einer Kooperation von Bund und Kantonen muss geklärt werden, ob das Datenschutzrecht des Bundes oder das Datenschutzrecht der Kantone auf die Plattform und den Datenaustausch anwendbar ist. Die Datenschutzbeauftragte wies darauf hin, dass der Gesetzesvorentwurf diese Frage ungenügend regelt.

Das Sicherheitsniveau für die Authentifizierung der Benutzerinnen und Benutzer soll sich gemäss Vorentwurf nach den Standards des Bundesgesetzes über die elektronischen Identifizierungsdienste (E-ID-Gesetz) richten. Nachdem dieses in der Volksabstimmung im März 2021 verworfen wurde, müssen für die Authentifizierung andere Sicherheitsstandards gesetzt oder herangezogen werden. Die Datenschutzbeauftragte verfolgt diese Entwicklung in Zusammenarbeit mit anderen Datenschutzbehörden weiter.

Mitwirkungspflicht im Asylverfahren

Die Datenschutzbeauftragte nahm Stellung zum Vorentwurf zur Änderung des Asylgesetzes. Mit dieser Änderung soll die Mitwirkungspflicht der asylsuchenden Personen bei der Klärung ihrer Identität auf die Überprüfung von mobilen Datenträgern ausgeweitet werden.

Asylsuchende Personen sind verpflichtet, bei der Feststellung des Sachverhalts mitzuwirken. Sie müssen gegenüber den Behörden ihre Identität offenlegen, Reisepapiere und Identitätsausweise abgeben, den Grund für das Asylgesuch nennen und allfällige Beweismittel einreichen. Mit der Änderung des Asylgesetzes sollen asylsuchende Personen auch verpflichtet werden, ihre mobilen Datenträger den Behörden zur Prüfung auszuhändigen, wenn ihre Identität, die Nationalität oder der Reiseweg nicht auf andere Weise festgestellt werden können.

Die Pflicht zur vorübergehenden Aushändigung elektronischer Datenträger stellt einen schweren Eingriff in die Privatsphäre dar. Für Eingriffe in die Grundrechte muss gemäss Bundesverfassung eine gesetzliche Grundlage bestehen, sie müssen im öffentlichen Interesse liegen und sie müssen verhältnismässig sein. Ein Grundrechtseingriff ist verhältnismässig, wenn er geeignet und erforderlich ist, um das angestrebte Ziel zu erreichen. Die Datenschutzbeauftragte stellte fest, dass keine verlässlichen Angaben bestehen, ob die Auswertungen elektronischer Datenträger für die Identitätsfeststellung geeignet sind. Deshalb konnte sie die Vorlage nicht vorbehaltlos als verhältnismässig beurteilen. Sie verlangte, dass die Überprüfung der Wirksamkeit der Auswertungen verbindlich im Gesetz vorgeschrieben wird.

Bei der Speicherung und Auswertung der elektronischen Datenträger werden in jedem Fall Personendaten von Drittpersonen bearbeitet, die auf den Datenträgern vorhanden sind. Für diese Datenbearbeitung fehlte im Entwurf eine gesetzliche Grundlage. Die Datenschutzbeauftragte zeigte diesen Mangel auf und verlangte eine Ergänzung der Vorlage.

Bei den Daten auf Mobiltelefonen oder Tablets kann es sich um sehr persönliche Informationen handeln. Öffentliche Organe, die solche Personendaten speichern, müssen dafür sorgen, dass sie sicher aufbewahrt werden. Die Regelung im Vorentwurf genügte den datenschutzrechtlichen Anforderungen nicht. Die Datenschutzbeauftragte verlangte die Schaffung einer einheitlichen und verbindlichen Regelung.

Mehr Informations-sicherheit in den Gemeinden

Die Gemeinden erweitern ihre Online-Angebote für die Bevölkerung und müssen technisch aufrüsten. Die IT-Infrastrukturen werden immer komplexer. Die Digitalisierung führt zu zusätzlichem Druck auf die Ressourcen der Gemeinden. Gemeinden jeder Grösse stehen vor der grossen Herausforderung, die Anforderungen an den Datenschutz und die Informationssicherheit sowie die gesetzlichen Vorgaben zu erfüllen.

Mit der Durchführung von Datenschutzreviews nimmt die Datenschutzbeauftragte ihre Aufsichtsfunktion über die Datenbearbeitung in Gemeinden wahr. Eine solche Kontrolle ist für alle Beteiligten zeitintensiv. Bei 162 Gemeinden im Kanton Zürich kann deshalb die Qualität der Informationssicherheit nicht in genügend kurzem Abstand kontrolliert werden. Die Datenschutzbeauftragte hat deshalb ein neues Konzept zur Überprüfung des Datenschutzes und der Informationssicherheit in Gemeinden entwickelt: den Datenschutzreview mit Selbstdeklaration.

Der Datenschutzreview mit Selbstdeklaration wird durch die Gemeinde selbst umgesetzt. Mit Unterstützung und Hilfestellungen der Datenschutzbeauftragten können die Gemeinden ihre IT-Infrastruktur in den Bereichen Datenschutz und Informationssicherheit selbst beurteilen und verbessern. Die Datenschutzbeauftragte hat dazu benutzerfreundliche und praxisnahe Vorlagen entwickelt. Sie ermöglicht damit auch Gemeinden mit beschränkten Ressourcen eine professionelle Informationssicherheits-Dokumentation.

Die Selbstdeklaration beginnt mit einem Begrüssungsschreiben der Datenschutzbeauftragten. In einer Kick-off Sitzung werden der Gemeinde das Vorgehen beschrieben und erste Fragen rund um die Selbstdeklaration beantwortet. Danach erhält sie die Vorlagen. Die Gemeinde kann nun ihre eigenen Dokumente überprüfen, um festzustellen, wie weit die bestehende Dokumentation schon dem Standard entspricht und wo weitere Unterlagen erstellt werden müssen. Die Selbstdeklaration hilft den Gemeinden, den Zustand der eigenen Infrastruktur einzuschätzen und wenn nötig Massnahmen zu definieren und umzusetzen. Sobald die Gemeinde alle Dokumente erstellt hat, meldet sie sich bei der Datenschutzbeauftragten. Diese überprüft die Unterlagen stichprobenartig. Wenn die Prüfung erfolgreich ist, wird ein Attest ausgestellt.

Im Jahr 2021 finden Lancierungsveranstaltungen zur Selbstdeklaration statt. Die Gemeinden können sich bei der Datenschutzbeauftragten melden und in der Pilotphase mitwirken. In einem ersten Schritt sollen erste Erfahrungen mit dem neuen Ansatz des Datenschutzreviews gesammelt werden. In einem weiteren Schritt wird die Selbstdeklaration weiterentwickelt, damit sie auch in anderen öffentlichen Organen eingesetzt werden kann.

Zurückblicken und vorausschauen

Das Jahr 2020 bot sich an, die Brücke aus der Vergangenheit in die nahe Zukunft zu schlagen. Am 28. Januar, dem Datenschutztag, blickte der Datenschutzbeauftragte Bruno Baeriswyl zwar zurück auf 25 Jahre Datenschutzgesetzgebung – aber nicht nur.

Zusammen mit Referentinnen und Referenten aus Kultur, Rechtswissenschaften und Politik suchte auch er vor allem nach Lösungen, wie neue Technologien in Zukunft demokratisch und sozialverträglich gestaltet werden können. Regierungspräsidentin Carmen Walker Späh betonte die Bedeutung des Datenschutzes und der Rechtssicherheit als Standortvorteil. Kantonsratspräsident Dieter Kläy sah vor allem, wie die Digitalisierung zunehmend unser Verhalten verändere. Darauf seien Antworten zu finden.

Die Veranstaltung im Museum für Gestaltung wurde in Zusammenarbeit mit der Zürcher Hochschule der Künste (ZHdK) durchgeführt. Rektor Thomas D. Meier stellte einige Beispiele zum Umgang in Kunst und Design mit Fragen der Privatsphäre vor. Professor Felix Stalder diskutierte die Herausforderungen an den Schutz der Privatsphäre in einer Zeit, in der alle zu jeder Zeit miteinander vernetzt sind. Melody Chua umrahmte das Programm künstlerisch. Die audiovisuelle Künstlerin zeigte, wie stark sich durch die Technologie alle Bereiche der Wahrnehmung und der Ausdrucksmöglichkeiten miteinander vermischen und gegenseitig verstärken.

Die Völkerrechtsprofessorin Astrid Epiney der Universität Fribourg erläuterte das Menschenrecht auf Datenschutz und die absolute Vorbedingung, dass zusätzliche Datenbearbeitungen durch Verwaltung und Behörden immer durch detaillierte gesetzliche Regelungen gerechtfertigt sein müssen. Die demokratische Kontrolle dürfe nie aufgeweicht werden. Elisabeth Ehrensperger, Geschäftsführerin der Stiftung für Technologiefolgen-Abschätzung TA-Swiss, trat für die fundierte Abklärung der Folgen von neuen Technologien wie künstliche Intelligenz ein. Digitalisierung führe zu immer stärkerer Personalisierung. Dies schränke die Autonomie des einzelnen Menschen ein. Die heutige Entwicklung stelle die Errungenschaften der Aufklärung grundlegend infrage.

Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte Adrian Lobsiger, wie auch der Präsident der Konferenz der schweizerischen Datenschutzbeauftragten privatim, Beat Rudin, schilderten, wie die gesetzlichen Voraussetzungen aussehen müssten, um einen unbürokratischen Datenschutz zu gewährleisten, der die Privatsphäre der Einwohnerinnen und Einwohner wirksam schützt.

Bruno Baeriswyl, Datenschutzbeauftragter seit Inkrafttreten des entsprechenden Gesetzes im Kanton Zürich, betonte, dass auf der ganzen Welt dieselben Technologien entwickelt und eingesetzt werden, unabhängig vom politischen und gesellschaftlichen System. Totalitäre Staaten sähen in ihnen eine Möglichkeit zur Überwachung und zur Manipulation der Bevölkerung. In demokratischen und liberalen Gesellschaften stehe das Grundrecht auf persönliche Freiheit im Vordergrund, dem sich die Nutzung neuer Technologien unterzuordnen hat. Der Gesetzgeber stehe in der Pflicht, die notwendigen Rahmenbedingungen zu schaffen. Gesetze sollen sich daran orientieren, welche Wirkung in Bezug auf die Freiheitsrechte der Bürgerin und des Bürgers erreicht werden soll. Der Datenschutz sei ein Gradmesser für die Freiheit, die in einer Gesellschaft herrscht.

Die Gefahren der Zukunft sind schon sichtbar

Die Sicherheitsdispositive unserer Gesellschaft vertrauen zunehmend auf Künstliche Intel-

ligenz. Der automatischen Gesichtserkennung wird ein immenses Potenzial zugeschrieben etwa zur Bekämpfung von Kriminalität. Der Dokumentarfilm Coded Bias, der am Zurich Film Festival gezeigt wurde, bildete im ZFF Talk die Grundlage einer Diskussion über die Risiken der neuen Technologie. Im Film illustriert die afroamerikanische Protagonistin, wie Vorurteile und Diskriminierung durch algorithmenbasierte Entscheidungen verstärkt werden. Unter der Leitung der NZZ-Redaktorin Nicole Althaus diskutierten die Datenschutzbeauftragte Dominika Blonski, der ETH-Professor Dirk Helbing sowie Patrick Walder von Amnesty International. Dominika Blonski hob hervor, dass aufgrund von alten Daten etwas für die Zukunft kreiert werde. Es brauche eine gesellschaftliche Diskussion und darauf basierend gesetzliche Regelungen. Aktuell seien Algorithmen Blackboxes ohne Kontrolle. Patrick Walder wies darauf hin, dass bei Entscheidungen durch Algorithmen niemand die Verantwortung trage. Dirk Helbing warnte vor ständiger Identifizierung durch Gesichtserkennung etwa bei der Videoüberwachung. Dies könne nie verhältnismässig sein, weil wir ja nie alle kriminell werden, meinte er. Das Bewusstsein sei zwar inzwischen geschärft, die Menschenrechte aber immer noch in Gefahr.

Wirksame neue Instrumente

42 Datenschutz-Folgenabschätzung wird Pflicht
43 Datenschutzvorfälle müssen gemeldet werden

Datenschutz-Folgenabschätzung wird Pflicht

Seit Juni 2020 sind öffentliche Organe verpflichtet, eine Datenschutz-Folgenabschätzung (DSFA) zu erstellen. Bei neuen Datenbearbeitungen sollen im Voraus die Risiken für die Privatsphäre eingeschätzt und minimiert werden. Die Datenschutzbeauftragte hatte öffentliche Organe schon immer im Umgang mit Privatsphärerisiken unterstützt. Neu ist die ausdrückliche gesetzliche Pflicht, ein entsprechendes Dokument zu erstellen.

Die Datenschutzbeauftragte erstellte ein Formular und ein Merkblatt, das die datenbearbeitenden Stellen bei der Datenschutz-Folgenabschätzung unterstützt. Es hilft, alle wesentlichen Angaben zu sammeln und auszuwerten. Erste Erfahrungen zeigen, dass das Formular und das Merkblatt zweckmässig sind. Die Datenschutzbeauftragte erhielt von mehreren Organen vollständige und aussagekräftige Analysen.

Die DSFA dient auch dazu, die Pflicht zur Vorabkontrolle abzuklären. Wenn besondere Risiken erkennbar sind, muss das Projekt der Datenschutzbeauftragten zur Vorabkontrolle unterbreitet werden. Die DSFA macht die Beurteilung der Vorabkontrollpflicht sowohl für die Organe als auch für die Datenschutzbeauftragte transparenter. In Projekten ohne Vorabkontrollpflicht ist die DSFA ein internes Arbeitsinstrument. Die Datenschutzbeauftragte steht auch in solchen Fällen für einen Austausch zur Verfügung.

Die DSFA ist neu Teil der Projektmanagement-Methode Hermes. Die Datenschutzbeauftragte konnte in Zusammenarbeit mit dem Competence Center für Projektmanagement (CCPM) klären, in welcher Projektphase eine DSFA zu erstellen ist. Damit ist sichergestellt, dass bei Projekten in der kantonalen Verwaltung die Datenschutzrisiken rechtzeitig und korrekt adressiert werden.

Projektverantwortliche nehmen den Datenschutz manchmal nur als zusätzliche Hürden wahr, oft sogar als Hindernis. Die Datenschutzbeauftragte sieht es als ihre Aufgabe, Projektverantwortliche davon zu überzeugen, dass Datenschutz das Resultat ihrer Arbeit verbessern kann. Dafür müssen die Anforderungen des Datenschutzes rechtzeitig in die Projektentwicklung integriert werden. Die DSFA mag auf den ersten Blick als lästige Pflicht erscheinen. Auf den zweiten Blick bietet sie eine Chance, einen Mehrwert für ein Projekt zu schaffen.

Das Formular und das Merkblatt zur Datenschutz-Folgenabschätzung sind auf der Website der Datenschutzbeauftragten www.datenschutz.ch unter Datenschutz in öffentlichen Organen publiziert.

Datenschutz-vorfälle müssen gemeldet werden

Im Juni 2020 trat das revidierte Gesetz über die Information und den Datenschutz (IDG) in Kraft. Seitdem sind öffentliche Organe verpflichtet, Datenschutzvorfälle an die Datenschutzbeauftragte zu melden. Meldepflichtig ist beispielsweise, wenn sich eine Hackerin oder ein Hacker Zugriff auf Daten verschafft oder auch wenn ein Mitarbeiter oder eine Mitarbeiterin einen USB-Stick mit Personendaten verloren hat.

Die Datenschutzbeauftragte erstellte ein Formular, um Datenbearbeitenden die Meldung zu erleichtern. Dafür arbeitete sie zusammen mit Datenschutzaufsichtsbehörden anderer Kantone, in denen die Meldepflicht eingeführt wurde. Ebenfalls verfügbar ist ein Merkblatt, das die wichtigsten Fragen beantwortet, etwa welche Vorfälle meldepflichtig sind und wie bei der Meldung vorzugehen ist.

Die Bandbreite möglicher Reaktionen der Datenschutzbeauftragten reichen von blosser Kenntnisnahme bis zur umfangreichen Kontrolle vor Ort. Deshalb definierte die Datenschutzbeauftragte einen Bearbeitungsprozess. In einem ersten Schritt klärt sie den Sachverhalt mit der meldenden Stelle. Wenn ein Vorfall meldepflichtig ist, untersucht die Datenschutzbeauftragte ihn und definiert Massnahmen. Sie können einerseits zur Bewältigung des Geschehenen dienen. Andererseits sind Massnahmen zu treffen, um ähnliche Vorfälle in der Zukunft zu vermeiden. Das öffentliche Organ erhält die Massnahmen mit einer Umsetzungsfrist mitgeteilt. Die Datenschutzbeauftragte stellt mit dem internen Prozess eine wirksame Unterstützung des meldenden Organs sicher.

Kurz nach Inkrafttreten des revidierten IDG gingen die ersten Meldungen ein. Auch vor Inkrafttreten war die Datenschutzbeauftragte vereinzelt auf Missstände hingewiesen worden. Die Einführung der Pflicht liess die Anzahl der Meldungen schnell stark ansteigen. Es ist damit zu rechnen, dass sich dieser Trend fortsetzt. Das Wissen um die Meldepflicht muss sich bei den öffentlichen Organen weiterverbreiten. Dafür sorgt die Datenschutzbeauftragte auch in ihren Weiterbildungsaktivitäten.

Die Datenschutzbeauftragte behandelt die Vorfälle vertraulich und setzt bei der Bewältigung bewusst auf ein kooperatives Vorgehen. Die meldepflichtigen Organe schätzen die konstruktiven Anregungen.

Die Datenschutzbeauftragte musste auch entscheiden, wie sie mit meldepflichtigen Vorfällen umgeht, die sie aus anderen Quellen erfährt. In den Medien wurde beispielsweise über einen Cyberangriff in ihrem Zuständigkeitsbereich berichtet. In diesen Fällen nimmt die Datenschutzbeauftragte Kontakt mit dem betroffenen Organ auf und klärt, ob der Vorfall meldepflichtig ist.

Die bisher gemeldeten Vorfälle sind vielfältig. Eine Behörde sendete Belege an die falsche Person. Ein Spital sendete Patienteninforma-

tionen an die falsche Adressatin. Eine Behörde entsorgte Rechner ohne ausreichende Datenlöschung. Ein vor Jahren entwendetes Dokument wurde dem Absender von einem Unbekannten zugespielt.

Nach der Bearbeitung der ersten Meldungen ist klar, dass die Information der Betroffenen meist die zentrale Frage darstellt. Die Datenschutzbeauftragte kann von der meldenden Stelle verlangen, dass die Betroffenen über den Vorfall informiert werden. In welchen Fällen dies notwendig ist, will die Datenschutzbeauftragte mit einem standardisierten Entscheidungsprozess beurteilen.

Die ersten Erfahrungen zeigen, dass die gemeinsame Bearbeitung der Vorfälle durch die Datenschutzbeauftragte und das öffentliche Organ zu deutlichen Verbesserungen beim Schutz der Privatsphäre führen kann. Die konkrete Behandlung von Datenschutzvorfällen entwickelt präventive Wirkung.

Die gemeldeten Datenschutzvorfälle eignen sich als Anschauungsbeispiele in Weiterbildungen der Datenschutzbeauftragten. Nichts bleibt so gut im Gedächtnis haften wie die Praxisbeispiele dazu, was in der Vergangenheit schiefgegangen ist und wie die Lösung aussieht.

Das Formular und das Merkblatt für die Meldepflicht von Datenschutzvorfällen sind auf der Website der Datenschutzbeauftragten www.datenschutz.ch unter Datenschutz in öffentlichen Organen publiziert.

Verwaltungsmassnahmen zum Einsatz bereit
Das revidierte IDG ermöglicht der Datenschutzbeauftragten, Verwaltungsmassnahmen zu ergreifen. Wenn sich ein Organ nicht an eine Empfehlung der Datenschutzbeauftragten hält, kann sie eine Verfügung aussprechen. Sie kann beispielsweise den Abbruch einer Datenbearbeitung oder die Löschung von Daten verfügen. Diese Möglichkeit kam noch nicht zur Anwendung. Der konstruktive und kooperative Umgang zwischen der Datenschutzbeauftragten und den beaufsichtigten Organen hat sich bewährt. Die Datenschutzbeauftragte ist jedoch vorbereitet. Das neue und schärfste Aufsichtsinstrument steht zum Einsatz bereit.

Datenschutz-beauftragte des Kantons Zürich

Die Datenschutzbeauftragte (DSB) beaufsichtigt die Datenbearbeitungen der kantonalen Verwaltung, der Gemeinden und der übrigen Behörden und öffentlichen Einrichtungen im Kanton, um die Privatsphäre der Einwohnerinnen und Einwohner sicherzustellen.

Sie berät die öffentlichen Organe, beurteilt datenschutz-relevante Vorhaben (Vorabkontrollen) und nimmt Stellung zu Erlassen. Sie bietet Aus- und Weiterbildungen in den Bereichen Datenschutz und Informationssicherheit an.

Bei öffentlichen Organen überprüft sie mit Kontrollen (Datenschutzreviews), ob die Anforderungen des Datenschutzes in rechtlicher, organisatorischer und sicher-heitstechnischer Hinsicht eingehalten sind. Öffentliche Organe sind verpflichtet, Datenschutzvorfälle zu melden. Die Datenschutzbeauftragte kann die Umsetzung von Massnahmen verfügen.

Die Datenschutzbeauftragte berät Privatpersonen über ihre daten schutzrechtlichen Ansprüche und vermittelt in Konfliktfällen zwischen Privatpersonen und öffentlichen Organen. Sie informiert die Öffentlichkeit über die Anliegen des Datenschutzes und der Informationssicherheit.

Impressum

Herausgeberin
Datenschutzbeauftragte des Kantons Zürich, Postfach,
8090 Zürich

Korrektorat
Text Control, Dufourstrasse 107, 8008 Zürich

Layout
TKF Kommunikation & Design, t-k-f.ch

Der Tätigkeitsbericht 2020 ist elektronisch verfügbar
unter www.datenschutz.ch/tb2020.

ISSN 2571-5003

Kontakt

E-Mail
datenschutz@dsb.zh.ch

Adresse
Datenschutzbeauftragte des Kantons Zürich,
Postfach, 8090 Zürich

Telefon
+41 43 259 39 99

Internet
www.datenschutz.ch

Twitter
@dsb_zh

Youtube

Datenschutz mit Qualität