dsb
datenschutzbeauftragte
des kantons zürich

Seite 3
Gefahren im analogen Homeoffice

Seite 3
Kein Pranger für Corona-Infizierte

Seite 4
Den verlorenen USB-Stick melden



# Teil der Lösung in der Krise

Beobachten wir die Diskussionen in der Corona-Pandemie aus der Perspektive des Datenschutzes und der Informationssicherheit, dann kommen wir zu zwei Erkenntnissen: Die Pandemie bewirkte einen Digitalisierungsschub und der Umgang mit diesem war sehr unterschiedlich. Einige sind sich der Gefahren der Digitalisierung ohne Datenschutz weiterhin nicht bewusst – und es interessiert sie auch nicht. Sie machen einfach irgendetwas. Aber es gibt auch die anderen. Sie sehen die Gefahren und arbeiten an Lösungen, um diese einzudämmen.

Die Datenschutzbeauftragte handelte in der Krise pragmatisch. Öffentliche Organe sowie die Einwohnerinnen und Einwohner brauchten schnelle Lösungen in der Krise. Die Datenschutzbeauftragte reagierte mit einer Produkteliste für die digitale Zusammenarbeit.

Aussergewöhnliche Zeiten verlangen eben nach aussergewöhnlichen Massnahmen. Das berechtigt jedoch noch lange nicht dazu, Datenschutz und Informationssicherheit zu vernachlässigen. Jede Bearbeitung von Personendaten ist ein Eingriff in das Grundrecht auf Datenschutz. Ob ein solcher Eingriff in die Privatsphäre zulässig ist, wird immer nach dem gleichen Schema überprüft – auch oder gerade während Krisen. In einer Pandemie kann die Überprüfung aber zu einem anderen Ergebnis führen als sonst.

Das Epidemiengesetz und die darauf basierenden Bestimmungen bilden die gesetzliche Grundlage für sehr weitgehende Bearbeitungen von heiklen Personendaten beispielsweise zur Rückverfolgung von Infektionen. Die Datenbearbeitungen müssen jedoch auch noch geeignet und erforderlich sein, um ein Ziel zu erreichen. Sie sollen nämlich helfen, die Ausbreitung des Virus zu bekämpfen. Sonst sind sie nicht verhältnismässig. Eine gesetzliche Grundlage reicht nicht aus.

Datenschutz ist ein Grundrecht. Bei Datenbearbeitungen müssen also bestimmte rechtliche 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 beantworten die Frage: Wie möchten wir als Gesellschaft zusammenleben?

**Grusswort**
Der Tätigkeitsbericht 2020 ist der 26. der Behörde, aber der 1. in meiner Amtszeit. Er steht im Zeichen des Schutzes der Grundrechte in Krisenzeiten.

Die Massnahmen zur Pandemiebekämpfung führten zu grossen Mengen an Personendaten, die erhoben, weitergegeben und ausgewertet wurden. Gleichzeitig gab es einen Digitalisierungsschub.

Die Aufsicht im Datenschutz ist eine der Voraussetzungen für die Grundrechte in der freien und demokratischen Gesellschaft. Sie finden den Tätigkeitsbericht 2020 unter: www.datenschutz.ch/tb2020

**Dr. iur. Dominika Blonski**
**Datenschutzbeauftragte**
**des Kantons Zürich**

# Gradmesser der Freiheit

Das Datenschutzgesetz im Kanton Zürich besteht ein Vierteljahrhundert. Solange war auch Bruno Baeriswyl Datenschutzbeauftragter. In einer Jubiläumsveranstaltung blickte er in die Vergangenheit, aber auch in die Zukunft. Viel ist geschehen seit dem vierseitigen Antragsformular für einen Internetanschluss, das er Mitte der 1990er Jahre ausfüllen musste. «Die Technologien sind dieselben auf der ganzen Welt, unabhängig vom politischen oder gesellschaftlichen System», sagte Baeriswyl. Totalitäre Staaten sähen in ihnen eine Möglichkeit zur Überwachung und der 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.

Der Datenschutz und die Rechtssicherheit seien wichtige Trümpfe des Wirtschaftsstandorts Zürich, betonte Regierungspräsidentin Carmen Walker Späh. Kantonsratspräsident Dieter Kläy sah vor allem auch, wie die Digitalisierung zunehmend unser Verhalten verändere. Darauf seien Antworten zu finden. Die Zürcher Hochschule der Künste illustrierte die Suche nach Antworten. Rektor Thomas D. Meier stellte Projekte von Studierenden in Kunst und Design vor, die Fragen zur Privatsphäre in der digitalisierten Gesellschaft bearbeiten. Der Schutz der Privatsphäre sei herausfordernd und neu zu denken in einer Zeit, in der alle zu jeder Zeit miteinander vernetzt sind, meinte Professor Felix Stalder. In den Zwischenspielen der audiovisuellen Künstlerin Melody Chua zeigte sich, wie die Technologie Wahrnehmung und Ausdrucksmöglichkeiten vermischt und verstärkt.

## Religionszugehörigkeit braucht Schutz

Für die Terminplanung eignet sich Doodle meistens. Wenn Gläubige sich für den Kirchenbesuch anmelden sollen, wird es heikel. Bei Informationen über religiöse Aktivitäten besteht ein grosses Diskriminierungsrisiko. Sie müssen deshalb besonders geschützt werden. Eine telefonische Anmeldung wäre am sichersten. Die Ressourcen im Frühjahr 2020 waren aber überall knapp und digitale Lösungen konnten einen Ausweg bieten. Allerdings dürfen die Kontaktdaten der Kirchgängerinnen und Kirchgänger nicht für alle sichtbar sein. Eine Anmeldung mit Pseudonymen schützt am besten. Die Kontaktdaten können auf einem anderen Weg erfasst werden.

## Personendaten unter allen Ämtern teilen?

Geben wir es zu: Es nervt, wenn wir immer wieder die gleichen Registrationsdaten angeben müssen. Die Digitalisierung sollte unser Leben vereinfachen und Wiederholungen verhindern. Das Once-Only-Prinzip wäre die Lösung. Die Daten einmal angeben und das Amt, das sie braucht, bekommt Zugriff darauf. Doch eine vollständige Umsetzung dieses Prinzips würde das Grundrecht auf Privatsphäre gefährden. Eine Regelung in einem kantonalen Gesetz reicht nicht aus.

Der Staat darf Personendaten nur für den Zweck benutzen, für den er sie erhoben hat. Das ist eine der Grundlagen des Grundrechts auf Privatsphäre. Personendaten dürfen nicht zweckentfremdet werden und die Einwohnerinnen und Einwohner müssen darauf vertrauen können. Datenmanagement ist ein Kernstück der Digitalisierungsstrategie. Eine Baustelle, an der weitergearbeitet werden muss. Die Datenschutzbeauftragte wacht und arbeitet lösungsorientiert mit.

# Gefahren im analogen Homeoffice

Arbeit zu Hause ist die neue Normalität. Da braucht es sichere Videokonferenztools, Remote Access und Coworking-Plattformen. Ein Digitalisierungsschub hat die Schweiz überrollt. Der private Laptop, auf dem sonst nur gegamet und gestreamt wurde, bearbeitet jetzt Sozialhilfedaten. Die Kinder platzen in die Videokonferenz. Der Schwatz beim Teekochen in der heimischen Küche mit der Mitbewohnerin oder dem Mitbewohner ist heimtückischer als der Klatsch bei der Kaffeemaschine im Büro. Hipp sind die analogen Gefahren des Homeoffice nicht. Doch nun die gute Nachricht: Die wichtigsten 8 Regeln für das sichere Homeoffice sind auf www.datenschutz.ch zusammengefasst. So schützen wir uns mit einfachen Routinen bei der Arbeit im privaten Umfeld.

## Kein Pranger für Corona-Infizierte

Das Smartphone klingelt. Ein Contact Tracer meldet sich. Der Anruf könnte eine Covid-19-Erkrankung ankündigen, auf jeden Fall sind zehn Tage Hausarrest sehr wahrscheinlich. Panik bricht aus. Klar hören die Contact Tracer die Frage häufig: Wer ist die Person mit dem positiven Corona-Test? Vielleicht fand der Kontakt in einem Restaurant statt. Schnell wüsste das halbe Dorf von offizieller Stelle von der möglichen Erkrankung einer Person, wenn der Kontakt in jedem Fall bekanntgegeben würde. Gesundheitsdaten sind auch und gerade in Krisenzeiten besonders schützenswert. Wenn die positiv getestete Person damit einverstanden ist, darf ihr Name genannt werden. Oder wenn es nicht anders geht. Falls die angerufene Person gegen die Quarantäne rechtlich vorgehen möchte, ist es vielleicht notwendig, Namen zu nennen.

## Sichere Informationssicherheit

Ziemlich zu Beginn der Digitalisierungsoffensive will der Kanton die Informationssicherheit festlegen. Die Systeme werden vernetzter. Informationen fliessen immer schneller. Die Vorgaben für die Identitätskontrolle, die Verschlüsselung und Systemüberwachung sollen einheitlich sein. Richtlinien für die Informationssicherheit sollen auch die Schutzniveaus für alle Daten definieren. Informationssicherheit ist der technische Teil des Datenschutzes. Doch der rechtliche Teil spielt hier ebenfalls eine Rolle. Die Daten können unterschiedlich geschützt werden, je nachdem ob sie öffentlich, intern, vertraulich oder geheim eingestuft werden. Das leuchtet ein, ist aber nicht genug. Manche Personendaten sind nicht geheim. Trotzdem brauchen sie ein hohes Schutzniveau. Darum ist die Zusammenarbeit der Datenschutzbeauftragten in den Projekten der Digitalisierungsprojekte so wichtig.

## Neue Website des Kantons

Der Kanton lancierte eine neue Website und hat damit Grosses vor. Doch auch bei Websites gilt: Öffentliche Institutionen dürfen nur Personendaten bearbeiten, wenn es nötig ist, um ihre gesetzliche Aufgabe zu erfüllen. Informieren mit einer Website gehört zu den Aufgaben. Aus technischen Gründen werden dabei Personendaten bearbeitet. Das ist erlaubt. Tracking der Nutzerinnen und Nutzer gehört nicht zu den Aufgaben des Kantons und ist deshalb nicht erlaubt. Bei Websites werden immer auch externe Dienste eingebunden, etwa Videos, die auf Youtube publiziert sind, die aktuellen Tweets oder Navigationshilfen von Google. Ohne die ausdrückliche Einwilligung der Nutzerinnen und Nutzer dürfen dabei keine Informationen an diese Firmen weitergegeben werden. Die Zwei-Klick-Lösung sollte Mindeststandard sein. Der Kanton hat sie nicht überall eingebaut.

Wie Websites sicher und mit Datenschutz funktionieren, beschreibt die Datenschutzbeauftragte auf www.datenschutz.ch.

# Sichere Plattformen unkompliziert nutzen

Die ausserordentliche Situation erforderte praktische, unkomplizierte Hilfe. Die Online-Produkteliste der Datenschutzbeauftragten fasste zusammen, welche Tools zur digitalen Zusammenarbeit eingesetzt werden können. Denn der Betrieb im verordneten Homeoffice sollte nahtlos weitergehen. Das wollten alle Mitarbeitenden im öffentlichen Dienst. Aber wirklich darauf vorbereitet waren die Wenigsten. Die Arbeit mit vielen neuen Zusammenarbeitstools machte unsicher. Darum schaute die Datenschutzbeauftragte viele Videokonferenzsysteme, Lern- oder Datenaustauschplattformen an. Nicht alle Produkte auf der Online-Liste waren datenschutzkonform, aber sie ermöglichten das Funktionieren der Verwaltung, der Gemeinden und der Schulen. Und sie waren für die Krisensituation gut genug. Doch die Institutionen müssen immer wieder neu überlegen, welche App oder Plattform eingesetzt wird. Was für eine virtuelle Kaffeepause geeignet ist, muss noch lange nicht für ein Bewerbungsgespräch passend sein, genau wie in der analogen Welt: In einem Fall bleiben die Türen offen, im anderen sind sie zu.

Datenschutzstellen und Bildungsdirektionen aus dem In- und Ausland verwiesen auf die Zürcher Produkteliste. Während des ersten Lockdowns besuchten ähnlich viele Personen die Website wie sonst in einem ganzen Jahr.

**Sicherheit mit QR-Codes**
Der QR-Code, dieses Quadrat mit unregelmässigen Punkten, überwindet den Medienbruch von Print zu Digital.

**Zwei Sicherheitshinweise:**

**1. Eine sichere Scan-App benutzen**
iOS: Kamera-App zum Scannen verwenden (ab Systemversion 11)
Android: QR-Scanner der Secuso Research Group installieren

**2. Angezeigte Webadresse kontrollieren**

Datenschutzbeauftragte des Kantons Zürich
Postfach, 8090 Zürich, +41 43 259 39 99
datenschutz@dsb.zh.ch, datenschutz.ch, twitter: @dsb_zh

## Den verlorenen USB-Stick melden

Ging das Mail mit den Patientendaten an die falsche Person, dann sind die Persönlichkeitsrechte der Patientin verletzt. Ist der USB-Stick weg, ist die Kontrolle über die gespeicherten Personendaten verloren. Datenschutz funktioniert als Prävention. Erste Erfahrungen mit der Meldepflicht für Datenschutzvorfälle zeigen jedoch: Auch nach dem Datenverlust ist Handeln sinnvoll. So kann das Fachwissen der Datenschutzbeauftragten bei der Eindämmung des Schadens helfen. Mit Massnahmen werden ähnliche Vorfälle zukünftig vermieden. Mit der Arbeit an einem konkreten Fehler wächst das Bewusstsein für andere Schwachpunkte.

Die Zeit wird zeigen, welche Probleme immer wieder auftauchen. Daraus ergeben sich Massnahmen, die flächendeckend umgesetzt Risiken in allen Institutionen beheben.


**Download**
Hier können Sie den Tätigkeitsbericht 2020 herunterladen.