



# Persönliche Freiheit

37 Anpassungen des IDG und Strategie Digitale Verwaltung

39 Einschränkungen der persönlichen Freiheit

# Anpassungen des IDG und Strategie Digitale Verwaltung

Im Jahr 2018 hat der Regierungsrat die Revision des Informations- und Datenschutzgesetzes (IDG) zuhanden des Kantonsrats verabschiedet. Er beschränkte sich dabei auf Anpassungen, die im Rahmen der Schengen-Assoziierung der Schweiz sowohl auf Bundes- wie auch auf Kantonsebene notwendig wurden. Auch 2018 hat der Regierungsrat die Strategie Digitale Verwaltung 2018–2023 beschlossen. Sie soll die Art und Weise der Datenbearbeitungen und die Zusammenarbeit der öffentlichen Organe grundlegend verändern. Erst in einem späteren Schritt sollen diesbezügliche Anpassungen des IDG erfolgen.

Der Regierungsrat hat sich bei der Revision des IDG auf die Wegleitung der Konferenz der Kantonsregierungen (KdK) gestützt, die den Kantonen als Grundlage für die Anpassung der Gesetzgebung an die EU-Richtlinie im Bereich Polizei und Justiz dient. Das Schengen-Assoziierungsabkommen der Schweiz mit der EU verpflichtet den Bund und die Kantone, die Richtlinie umzusetzen. Die EU evaluiert regelmässig die Zusammenarbeit im Rahmen des Schengen-Abkommens. Dabei wird auch die Umsetzung des Datenschutzes beurteilt [\[Seite 8\]](#). Der Datenschutzbeauftragte nahm im Rahmen der Vernehmlassung zum Gesetzesprojekt Stellung. Generell konnte der Datenschutzbeauftragte feststellen, dass die Anforderungen des KdK-Leitfadens gut aufgenommen und pragmatisch umgesetzt wurden. Seine Bemerkungen bezogen sich auf einige zu klärende Ergänzungen.

## Offene Punkte der Umsetzung

In der Weisung an den Kantonsrat vom 4. Juli 2018 (KR Nr. 5471) wurden allerdings materielle Änderungen vorgenommen, die nicht konform zu den Vorgaben der Richtlinie sind. In der Vorlage fehlt die verpflichtende Bestimmung, dass sich ein Bürger oder eine Bürgerin mit einer Beschwerde an den Datenschutzbeauftragten wenden kann, mit der sich dieser in einem förmlichen Verfahren zu befassen hat. Im Schengen-Datenschutzgesetz (SDSG) des Bundes wird diese Vorgabe gelöst, indem die Möglichkeit einer Anzeige beim Datenschutzbeauftragten mit folgender Verpflichtung festgeschrieben ist: «Hat die betroffene Person Anzeige erstattet, so informiert der Beauftragte sie über die gestützt darauf unternommenen Schritte und das Ergebnis einer allfälligen Untersuchung.» Dieses Recht muss auch der Zürcher Bevölkerung gewährt werden.

Weiter wird die Hürde für die Ausübung der Aufsicht des Datenschutzbeauftragten erhöht: Eine Verfügung zur Anpassung der Datenbearbeitungen soll nur bei einer «erheblichen» Verletzung von Bestimmungen über den Datenschutz möglich sein. «Erheblich» ist aber ein unbestimmter Rechtsbegriff und es ist nicht sinnvoll, wenn im Vorfeld einer Verfügung darüber gestritten wird, was «erheblich» ist. Das Gebot der Verhältnismässigkeit gilt in jedem Fall. Bei einer nicht erheblichen Verletzung von Bestimmungen wäre eine Verfügung des Datenschutzbeauftragten entsprechend unverhältnismässig.

Gestrichen wurde zudem die Möglichkeit, dass der Datenschutzbeauftragte vorsorgliche Massnahmen erlassen kann. Die gestrichene Formulierung lautete: «Die oder der Beauftragte kann vorsorgliche Massnahmen verfügen, um einen bestehenden Zustand aufrechtzuerhalten, gefährdete schutzwürdige Interessen zu schützen oder Beweismittel zu sichern.»

Dies sind drei wichtige Bestimmungen, um die Freiheitsrechte der Bürgerinnen und Bürger angesichts der umfassenden Digitalisierung zu schützen und bei Datenschutzproblemen effizient und effektiv eingreifen zu können. Der Datenschutzbeauftragte wurde von der zuständigen Kommission (StGK) zu einer Anhörung eingeladen, in der er diese Punkte konkretisieren konnte. Ende 2018 war die Gesetzesrevision noch bei der Kommission anhängig.

### **Digitalisierung ohne Datenschutz?**

Der Datenschutzbeauftragte hatte die Gelegenheit, vor der Verabschiedung der Strategie Digitale Verwaltung 2018–2023 Stellung zu beziehen. Die Digitalisierung der Verwaltungsabläufe beinhaltet unzählige Interaktionen mit internen und externen Personen und Organisationen. Dies führt zu einem exponentiellen Anwachsen der Datenmenge bei der Verwaltung, da jede digitale Interaktion Datenspuren hinterlässt. So wird zwangsläufig festgehalten, wer wann mit wem und wie oft welche Informationen und Daten ausgetauscht hat. Die zahlreichen Schnittstellen, die sich aus der Interaktion mit der Verwaltung ergeben, beispielsweise bei der Nutzung des Smartphones, führen aber immer auch dazu, dass private Datenbearbeiter über diese Interaktionen Daten erhalten (Hard- und Softwarehersteller, Telekomanbieter etc.).

Die Aufbewahrung, Bearbeitung oder Auswertung von Datenspuren ermöglicht die Erstellung von Profilen der betroffenen Personen. Dies ist oft Teil der Geschäftsmodelle im Privatbereich. Es kann nicht davon ausgegangen werden, dass die betroffenen Personen, die sich im Privatbereich ständig mit der Auswertung ihrer Verhaltensspuren konfrontiert sehen, die Auswertung solcher Daten auch von der staatlichen Verwaltung akzeptieren. Im Gegenteil: Der Staat hat ihre Grundrechte zu wahren. Die Verwaltung muss deshalb dafür sorgen, dass diesen Auswertungen nicht Vorschub geleistet wird, und muss ausschliessen, dass die Überwachung von Mitarbeitenden oder die Erstellung von Verhaltensprofilen von Bürgerinnen und Bürger ermöglicht wird. Deshalb sollen für die Interaktion datenschutzfreundliche Produkte gewählt werden. Der richtige und sichere Umgang mit den Daten ist kritisch für die Akzeptanz und das Vertrauen der betroffenen Personen. Wie diesen Herausforderungen der Digitalisierung begegnet wird, bleibt mit der vorliegenden Strategie weitgehend offen. Dafür bräuchte es eine Politik der Datenvermeidung und der Datensparsamkeit als Teil der Strategie der Digitalisierung. Der Datenschutzbeauftragte schlug deshalb vor, dass das Leitbild mit einem übergeordneten Zweck ergänzt wird, der mit der Digitalisierung im Kanton Zürich erreicht werden soll. Darin müsste zum Ausdruck kommen, dass die Digitalisierung zur Stärkung des Rechtsstaats und seiner Institutionen, der föderalen Demokratie und der Grundrechte beitragen soll. Zudem wurde der Datenschutzbeauftragte in der Organisationsstruktur zur Umsetzung der Digitalisierung der Verwaltung in keiner Art und Weise eingebunden. Dies erachtet der Datenschutzbeauftragte als einen schwerwiegenden Mangel, da die Fragen des Schutzes und der Sicherheit der Daten bei der Digitalisierung eine zentrale Rolle spielen müssen.

### **Pragmatische Zusammenarbeit**

Die Anmerkungen des Datenschutzbeauftragten wurden nicht in die Strategie aufgenommen. Der Datenschutzbeauftragte versuchte deshalb, die Zusammenarbeit mit den direkt involvierten Stellen zu intensivieren. Bis Ende 2018 ist es gelungen, in verschiedenen Bereichen eine Zusammenarbeit auf einer pragmatischen Grundlage zu etablieren. Auch bei den betroffenen öffentlichen Organen stand die Erkenntnis im Vordergrund, dass ohne eine angemessene Berücksichtigung der Anliegen des Datenschutzes digitale Lösungen in der Bevölkerung kaum akzeptiert werden ([Seite 7](#)).

# Einschränkungen der persönlichen Freiheit

Der Datenschutzbeauftragte nahm Stellung zu verschiedenen Gesetzes- und Verordnungsvorlagen, in denen Fragen zur Einschränkung oder Gefährdung der persönlichen Freiheit zentral waren.

## **Totalrevision des Sozialhilfegesetzes**

Der Datenschutzbeauftragte beurteilte in seiner Stellungnahme die Regelungen der Datenbearbeitungen im Entwurf des totalrevidierten Sozialhilfegesetzes als gelungen. Er begrüßte, dass die Bestimmungen zum Informationsaustausch bestehen bleiben (Schweigepflicht, Informationsaustausch, Amtshilfe). Das revidierte Gesetz erfüllt damit die Voraussetzungen für Grundrechtseinschränkungen sowie die Anforderungen an Rechtsgrundlagen für Datenbekanntgaben.

Der Gesetzesentwurf beinhaltet eine Regelung, die bei einem Wechsel des Unterstützungswohnsitzes als Rechtsgrundlage dienen soll für die sofortige Übergabe des vollständigen Sozialhilfedossiers an das neu zuständige Sozialhilfeorgan. Der Datenschutzbeauftragte forderte die Streichung dieser Regelung und zeigte die Rechtslage auf. Als öffentliches Organ unterliegt die Sozialhilfebehörde einer Dokumentations- und Aufbewahrungspflicht. Deshalb darf sie die Unterlagen nicht an ein anderes Organ übergeben. Die Übergabe des vollständigen Sozialhilfedossiers wäre zudem unverhältnismässig. Der verhältnismässige Informationsfluss ist bereits mit den bestehenden rechtlichen Bestimmungen gewährleistet.

Weiter nahm er Stellung zur neuen Bestimmung zur Observation. Er stellte fest, dass eine Observation einen schweren Eingriff in das Grundrecht auf Privatsphäre darstelle. Deshalb begrüßte er den Erlass einer formell-gesetzlichen Regelung für den Einsatz von Sozialdetektivinnen und Sozialdetektiven wie auch die Umsetzung der Rahmenbedingungen einer Observation gemäss dem Urteil des Europäischen Gerichtshof für Menschenrechte vom 18. Oktober 2016 zum Fall Vukota-Bojic gegen die Schweiz. Er wies darauf hin, dass auch für Hausbesuche im Sozialhilfebereich eine ausdrückliche Rechtsgrundlage zu schaffen ist, falls diese Massnahme weiterhin eingesetzt werden soll. Mit Hausbesuchen werde zusätzlich das Grundrecht auf Schutz der Wohnung tangiert.

## **Änderung der Verordnung über den allgemeinen Teil des Sozialversicherungsrechts**

Der Datenschutzbeauftragte begrüsst in seiner Stellungnahme zur Änderung der Verordnung über den allgemeinen Teil des Sozialversicherungsrechts, dass für Observationen eine Bewilligungspflicht vorgesehen ist und die fachlichen und persönlichen Anforderungen an die Personen definiert werden, die im Auftrag von Versicherungsträgern Observationen durchführen dürfen. Weiter begrüsst er, dass das Verfahren zur Einsichtnahme in das vollständige Observationsmaterial geregelt wird. Zu den Bestimmungen zu Aktenführung und Aktenaufbewahrung hielt er fest, dass diese nicht auf die Versicherungsträger zu beschränken sind. Auch für die beauftragten Spezialistinnen und Spezialisten sei zu regeln, wie sie die Akten zu führen sowie das Observationsmaterial aufzubewahren haben und die Einhaltung des Datenschutzes und der Datensicherheit gewährleisten müssen. Observationsmaterial, das nicht auf unrechtmässigen Leistungsbezug schliessen lässt, sei nach Erlass der Verfügung zu vernichten. Zudem müssten die von Versicherungsträgern mit Observationen beauftragten Personen das Observationsmaterial nach Beendigung des Auftrags dem Versicherungsträger übergeben.

## **Systematische Verwendung der AHV-Nummer**

Der Datenschutzbeauftragte nahm Stellung zur Änderung des Bundesgesetzes über die Alters- und Hinterlassenenversicherung (AHV) zur systematischen Verwendung der AHV-Nummer durch Bundesbehörden. Er stellte fest, dass die Vorlage die Risiken für die Persönlichkeitsrechte der Bürgerinnen und Bürger erhöht. Im Rahmen der Digitalisierungsvorhaben der Verwaltung müsse für die Verwendung der AHV-Nummer eine klare Ausgangslage geschaffen werden, welche die rechtlichen, organisatorischen und technischen Aspekte gleichermaßen berücksichtige. Der Datenschutzbeauftragte kritisierte, dass das Sicherheitskonzept für Personenidentifikatoren der Kommission für Rechtsfragen des Nationalrates nicht abgewartet wurde. Im Konzept, das aufgrund des Postulats 17.3968 in Auftrag gegeben worden war, soll definiert werden, wie bei der Verwendung der AHV-Nummer den Risiken für den Datenschutz und die Sicherheit begegnet werden kann. Das Vorziehen der Gesetzesänderung führe zur unbefriedigenden Situation, dass die Kantone eigenständig Risikoanalysen durchführen und prüfen müssten, ob die AHV-Nummer oder ein bereichsspezifischer Identifikator einzusetzen ist. Für die Schaffung eines einheitlichen eidgenössischen Personenidentifikators fehle zudem die verfassungsrechtliche Grundlage. Deshalb sei klarer auszuführen, dass die systematische Verwendung der AHV-Nummer nicht die Schaffung eines einheitlichen eidgenössischen Personenidentifikators bedeute. Aus datenschutzrechtlicher Sicht ist die Verwendung verschiedener, sektorieller Personenidentifikatoren zu bevorzugen, da die rechtlichen und technischen Risiken eines universellen Identifikators zu hoch sind.

Der Datenschutzbeauftragte stellte infrage, ob überhaupt ein genügender Regulierungsbedarf besteht. Einerseits werde die systematische Verwendung der AHV-Nummer angestrebt, um die korrekte Verknüpfbarkeit von Datenbanken zu erhöhen. Andererseits sei dem Bericht zur Vorlage zu entnehmen, dass die Zuverlässigkeit der Verknüpfbarkeit auch ohne Verwendung der AHV-Nummer bei 99,98 Prozent liege. Dem finanziellen und administrativen Aufwand stehe kein entsprechender Nutzen gegenüber.