



Digital zusammenarbeiten

- 47 Digital zusammenarbeiten
- 49 Neue datenschutzrechtliche Leitplanken
- 51 Datenschutzerklärungen, Banner, Pop-ups und andere Scheinlösungen
- 52 Nationales System zur Abfrage von Adressen
- 53 Online-Publikation von Einbürgerungsdaten

Digital zusammenarbeiten

Der Datenschutzbeauftragte konnte die Zusammenarbeit im Bereich der Digitalisierungsprojekte weiter ausbauen, über neue Datenschutzinstrumente sowie deren Umsetzung informieren und gleichzeitig die Integration dieser neuen Instrumente in die Projektmethodik Hermes bewirken.

Aufbau der Zusammenarbeit

Der Datenschutzbeauftragte nahm nach der Verabschiedung der Digitalisierungsstrategie die direkte Zusammenarbeit auf mit den involvierten Stellen der kantonalen Digitalisierungsprojekte. 2019 wurden diese Zusammenarbeiten intensiviert. Mit der Abteilung Digitale Verwaltung und E-Government der Staatskanzlei, die für die Koordination der Projekte des Impulsprogrammes zuständig ist, etablierte sich ein regelmässiger Austausch. In diesen Gesprächen konnte die rechtzeitige Integration des Datenschutzbeauftragten in Digitalisierungsvorhaben thematisiert werden. Die sehr gute Zusammenarbeit machte es dem Datenschutzbeauftragten verschiedene Male möglich, über seine Dienstleistungen und die anstehenden Neuerungen im Datenschutzrecht zu informieren. Seine Informationen stiessen auf grosses Interesse, und er wurde von zahlreichen Projektleiterinnen und Projektleitern für eine Beratung oder Begleitung ihres Projekts angefragt. An einer Mittagsveranstaltung zum Impulsprogramm informierte der Datenschutzbeauftragte über die neuen Datenschutzinstrumente, die im revidierten Gesetz über die Information und den Datenschutz festgehalten sind.

Dank der neu aufgebauten Zusammenarbeiten wurde der Datenschutzbeauftragte zur Beratung und Begleitung zahlreicher Projekte des Impulsprogramms Digitale Verwaltung eingeladen. Er berät das Projektteam beispielsweise in folgenden Projekten: Rechtliche Grundlagen elektronischer Rechtsverkehr DigiLex (IP 2.1), Studie Blockchain (IP 1.5), Strategie Datenmanagement und Data Governance (IP 3.1), Geschäftsarchitektur Digitale Verwaltung und E-Government (IP 7.3), ZHweb2019 (IP 4.1), Erneuerung Transaktionsplattform ZHServices, eBaugesucheZH (IP 1.1), eEinbürgerungenZH (IP 1.2), Online-Bewilligungen (IP 1.4) und Serviceorganisation eFormulare (IP 2.2).

Integration der neuen Datenschutz-Instrumente

Mit der Revision sind im Gesetz über die Information und den Datenschutz (IDG) neue Datenschutzinstrumente verankert worden. Eines dieser Instrumente ist die Datenschutzfolgenabschätzung (DSFA) (§ 10 Abs. 1 IDG). Darin bewerten öffentliche Organe bei einer geplanten Bearbeitung von Personendaten die Risiken für die Grundrechte der betroffenen Personen. Sie dient dem öffentlichen Organ zur Sicherstellung und zum Nachweis der Einhaltung der Datenschutzvorschriften. Die DSFA wird vom öffentlichen Organ selbst vor jeder geplanten Bearbeitung von Personendaten durchgeführt. Stellt das öffentliche Organ dabei besondere Risiken für die Grundrechte der betroffenen Personen fest, hat es das Projekt dem Datenschutzbeauftragten zur Vorabkontrolle vorzulegen.

Der Datenschutzbeauftragte schlug vor, dass die DSFA sowie die Vorabkontrolle in der Projektmethode Hermes abgebildet werden. Hermes wurde vom Regierungsrat als Projektmethode für alle Projekte des Impulsprogramms Digitale Verwaltung festgelegt. Die Integration der neuen Datenschutzinstrumente im vorgeschriebenen Projekttool erleichtert die Arbeit der Projektleiterinnen und Projektleiter. Sie werden beim Abarbeiten der Hermes-Checkliste zum richtigen Zeitpunkt auf die Notwendigkeit einer DSFA und die Abklärung für eine Vorabkontrolle aufmerksam gemacht. Die Datenschutzfolgenabschätzung wird in der Hermes-Projektmethode zunächst in der Initialisierungsphase durchgeführt. Bei Veränderungen am Projekt ist die DSFA später erneut durchzuführen. Die Frage nach der Vorabkontrolle wird in Hermes in der Konzeptphase gestellt.

Projektleiterinnen und Projektleiter finden auf der Website des Datenschutzbeauftragten alle weiteren Informationen und Unterlagen für die Durchführung der Datenschutzfolgenabschätzung und der Vorabkontrolle. Er steht den Projektteams in jeder Projektphase für eine Beratung zur Verfügung. Diese Hilfestellung wurde im Rahmen des Impulsprogramms im Jahr 2019 rege genutzt.

Neue datenschutzrechtliche Leitplanken

Der Kantonsrat hat das revidierte Gesetz über die Information und den Datenschutz (IDG) verabschiedet und der Regierungsrat hat eine neue Verordnung zur Informationsverwaltung und -sicherheit (IVSV) erlassen. Während das IDG klare Rahmenbedingungen setzt, verpasst es die IVSV, einheitliche Sicherheitsstandards im Kanton vorzugeben.

Das revidierte IDG setzt die neuen datenschutzrechtlichen Anforderungen um, die sich aus der Schengen-Zusammenarbeit der Schweiz mit der EU und aus der angepassten Konvention 108+ des Europarats ergeben. Eine weitergehende Reform des IDG auf dem Hintergrund der Digitalisierung der Verwaltung hat der Regierungsrat für die Legislatur 2019 – 2023 vorgesehen. Anträge im Kantonsrat, die bereits heute weitere Anpassungen des IDG verlangten, wurden vom Regierungsrat für die neue Reform entgegengenommen.

Das revidierte IDG enthält einige wichtige Bestimmungen, die einerseits klare Rahmenbedingungen für die öffentlichen Organe setzen und andererseits mehr Transparenz über die Datenbearbeitungen für die Bürgerinnen und Bürger bringen.

Öffentliche Organe haben neue Projekte mit einer Risikoabwägung auf die Folgen für die Persönlichkeitsrechte der Bürgerinnen und Bürger zu prüfen. Vorhaben mit besonderen Risiken sind wie bisher dem Datenschutzbeauftragten zur Vorabkontrolle zu unterbreiten. Öffentliche Organe stellen mit Organisationsvorschriften sicher, dass die Datenschutzbestimmungen eingehalten werden. Bei Datenschutzverletzungen hat das öffentliche Organ den Datenschutzbeauftragten beizuziehen.

Der Datenschutzbeauftragte hat neu die Kompetenz, das öffentliche Organ mit einer Verfügung zu einer datenschutzkonformen Bearbeitung zu verpflichten. In einem ersten Schritt gibt er wie bisher eine Empfehlung ab. Er kann aber auch aufgrund des Verwaltungsrechtspflegegesetzes (VRG) vorsorgliche Massnahmen verfügen, wie dies der Regierungsrat in seiner Weisung zum IDG ausführt. Weiter beaufsichtigt der Datenschutzbeauftragte neu auch die öffentlichen Organe, die privatrechtlich handeln, wie die Zürcher Kantonalbank.

Beschwerden von Bürgerinnen und Bürger hat der Datenschutzbeauftragte in jedem Fall zu bearbeiten, wie der Regierungsrat in der Weisung festhält. Damit wird das Instrument der Individualbeschwerde gestärkt.

Mit der IVSV wurde die bisherige Informatiksicherheitsverordnung (ISV) auf Ende 2019 ausser Kraft gesetzt. Die ISV hatte ausführliche Bestimmungen, wie die öffentlichen Organe die Sicherheit ihrer Datenbearbeitungen zu gewährleisten hatten. In zahlreichen Teilen war sie inhaltlich und begrifflich veraltet. Mit der IVSV wurde ein Ersatz geschaffen, der jedoch inhaltlich nicht gleichwertig ist. Es handelt sich um wenige Rahmenbedingungen, die für die Praxis nur hilfreich sind, wenn konkrete Leitplanken geschaffen werden. Das Amt für Informatik (AFI) erstellt diese zurzeit für die kantonale Verwaltung. Wie die Gemeinden, Hochschulen und weiteren öffentlich-rechtlichen Anstalten diese Konkretisierung vornehmen werden, bleibt offen. Angesichts der zunehmenden Digitalisierung und den damit einhergehenden Sicherheitsrisiken, erscheint es aus heutiger Sicht fahrlässig, in diesem Bereich für den Kanton Zürich keine einheitlichen Standards zu setzen.

Datenschutz- erklärungen, Banner, Pop-ups und andere Scheinlösungen

Fast jede Website ist heute mit einer Datenschutzerklärung versehen. Die Nutzerinnen und Nutzer sollen darüber aufgeklärt werden, in welche Datenbearbeitungen sie explizit oder implizit einwilligen. Im privatrechtlichen Bereich ist dies vorgeschrieben. Vor allem im Geltungsbereich der EU-Datenschutz-Grundverordnung (DSGVO) kommen noch die allgegenwärtigen Banner und Pop-ups dazu, die eine ausdrückliche Einwilligung in die Verwendung von Cookies und Auswertungen verlangen. Anlässlich der Neugestaltung des Internetauftritts der kantonalen Verwaltung prüfte der Datenschutzbeauftragte die Rechtslage für Websites öffentlicher Organe vertieft.

Öffentliche Organe brauchen für ihre Datenbearbeitungen eine Rechtsgrundlage. Die Einwilligung der Betroffenen kann diese Grundlage nicht ersetzen. Das gilt auch für den Umgang mit Daten, die bei der Website-Nutzung anfallen. Personenbezogene Auswertungen mit Cookies oder Tracking Tools sind für Websites öffentlicher Organe nicht erlaubt.

Der Datenschutzbeauftragte kommt zum Schluss, dass öffentliche Organe für ihre Websites keine Datenschutzerklärungen erstellen müssen. Gleichzeitig rät der Datenschutzbeauftragte davon ab, Mechanismen wie Cookie-Warnungen einzusetzen, die dem Nutzer eine Einwilligung vorgaukeln. Damit würde ein missverständlicher Eindruck erweckt. Der Betrieb einer datenschutzfreundlichen, gesetzeskonformen Behörden-Website kommt ohne solche Scheinlösungen aus.

Nationales System zur Abfrage von Adressen

Der Vorentwurf für das Bundesgesetz über das nationale System zur Abfrage von Adressen natürlicher Personen (Adressdienstgesetz) bildet die Grundlage für die Errichtung eines nationalen Adressdienstes. Verwaltungen und Dritte mit gesetzlichem Auftrag sind in den unterschiedlichsten Geschäftsfällen darauf angewiesen oder rechtlich dazu verpflichtet, Personen schriftlich zu kontaktieren. Dazu benötigen sie die aktuellen Adressen dieser Personen, um Fehlzustellungen zu vermeiden. Die Einwohnerkontrollen der Gemeinden verfügen über aktuelle Adressdaten ihrer Einwohnerinnen und Einwohner. Ein neuer nationaler Adressdienst soll verhindern, dass Behörden bei allen in Frage kommenden Gemeinden Adressabklärungen vornehmen und diese zahlreiche unnötige Anfragen beantworten müssen. Für den nationalen Adressdienst wird auf den bestehenden Datenlieferungsprozessen aufgebaut.

Kantone und Gemeinde erheben gestützt auf das Registerharmonisierungsgesetz heute Adressdaten und übermitteln sie an das Bundesamt für Statistik. Sie werden neu auf Bundesebene in einem Informationssystem zusammengefasst und allen Gemeinwesen in einer einheitlichen Form und über eine einheitliche Schnittstelle zur Verfügung gestellt.

Der Datenschutzbeauftragte prüfte, ob im Vorentwurf die datenschutzrelevanten Punkte ausreichend geregelt sind. Die erhobenen Adressdaten sind Personendaten, jedoch keine besonders schützenswerten Personendaten oder Persönlichkeitsprofile. Der Zugriff auf das Informationssystem ist beschränkt auf Behörden, Organisationen und Personen, die zur Erfüllung ihrer gesetzlichen Aufgaben die Adressen der natürlichen Personen in der Schweiz benötigen und die die AHV-Nummer systematisch verwenden dürfen. Das Auskunftsrecht der betroffenen Personen ist im Vorentwurf ausdrücklich geregelt. Die Zugriffe auf die Daten des Informationssystems werden protokolliert, damit nachvollziehbar ist, wer wann auf sie zugegriffen hat. Die Dauer der Aufbewahrung sowie die Vernichtung der Daten sind geregelt. Die Verantwortung für den Schutz der Daten im nationalen Adressdienst wird dem Bundesamt für Statistik übertragen. Der Erlass von Ausführungsbestimmungen wird an den Bundesrat delegiert. Der Vorentwurf zum Adressdienstgesetz schafft die notwendigen gesetzlichen Grundlagen für diese Delegation.

Der Datenschutzbeauftragte beurteilte den Vorentwurf zum Adressdienstgesetz als datenschutzkonform.

Online-Publikation von Einbürgerungs- daten

Bei der Publikation von Personendaten auf einer Website stellt sich die Frage, welche dieser Personendaten zu welchem Zeitpunkt wieder gelöscht werden müssen. Der Datenschutzbeauftragte beschäftigte sich mit dieser Frage im Zusammenhang mit Ratsprotokollen eines Gemeindeparlaments, die auf der Website publiziert waren. Die Protokolle enthielten auch Informationen zu Einbürgerungsgeschäften. Anfang 2018 trat eine neue Bestimmung der Kantonalen Bürgerrechtsverordnung in Kraft, wonach Angaben zu Einbürgerungsgeschäften nach Eintritt der Rechtskraft des Einbürgerungsentscheids aus dem Protokoll gelöscht werden müssen.

Eine Gemeinde fragte den Datenschutzbeauftragten, ob diese Bestimmung auch für die Gemeinderatsprotokollen aus dem Zeitraum vor Inkrafttreten der neuen Bestimmung gelte. Die neue Bestimmung sorgt dafür, dass die Informationen zu Einbürgerungsgeschäften gelöscht werden, sobald die Veröffentlichung ihren Zweck erfüllt hat. Der Datenschutzbeauftragte wies darauf hin, dass sich diese Pflicht bei der Publikation von Einbürgerungsdaten im Internet schon aus dem verwaltungs- und datenschutzrechtlichen Grundsatz der Verhältnismässigkeit ergebe, ganz unabhängig von der neuen Bestimmung. Die Publikation von Einbürgerungsdaten hat zum Zweck, die Öffentlichkeit über aktuell erfolgte Einbürgerungen zu informieren. Das Informationsinteresse der Öffentlichkeit nimmt in der Zeitachse laufend ab, während das Interesse der betroffenen Personen am Schutz ihrer Privatsphäre zunimmt. Der Datenschutzbeauftragte kam zum Schluss, dass die Informationen zu den Einbürgerungsgeschäften aus den Gemeinderatsprotokollen und anderen Dokumente zu entfernen sind, auch wenn diese vor Inkrafttreten der neuen Bestimmung auf der Website veröffentlicht worden sind.