Gedanken zur Revision des DSG

Der Revisionsentwurf des Bundesrates zum Datenschutzgesetz vom 15. September 2017 war und bleibt von deutlicher Kritik begleitet. Einerseits aus der Sicht privater Datenbearbeiter durch David Rosenthal und David Vasella. Andererseits - aus der Sicht öffentlich-rechtlicher Datenbearbeiter - von drei kantonalen Datenschutzbeauftragten, namentlich Claudia Mund (ZG), Beat Rudin (BS) und Bruno Baeriswyl (ZH) in der NZZ vom 31. Oktober 2017. Die drei Beauftragten regen an, für die Bundesbehörden eine einfache Separatlösung nach dem Vorbild moderner kantonaler Datenschutzgesetze vorzusehen. In diese Richtung hat sich jüngst auch die Konferenz der schweizerischen Datenschutzbeauftragten geäussert.[1]

Philip Glass, 23. Januar 2018, http://www.datalaw.ch/gedanken-zur-revision-des-dsg/
Zitiervorschlag: Philip Glass, Gedanken zur Revision des DSG, www.datalaw.ch, Rz.

An dieser Stelle soll anhand eines Beispiels dargestellt werden, wodurch sich solche moderne Lösungen im Vergleich zum Entwurf auszeichnen und weshalb eine Trennung des privatrechtlichen und öffentlich-rechtlichen Datenschutzrechts aus Sicht des verfassungsrechtlichen Datenschutzes sinnvoll sein kann.[2] Zu diesem Zweck wird die Problematik anhand eines Kernkonzepts des Datenschutzrechts dargestellt und die unterschiedlichen Varianten von Bund und Kantonen verglichen. Es handelt sich um das Konzept der qualifizierten Datenbearbeitungen bzw. der besonderen und besonders schützenswerten Personendaten.

Besondere vs. besonders schützenswerte Personendaten

[1] In der Schweiz hat sich im Verlaufe der Entwicklung des Datenschutzrechts eine begriffliche Unterscheidung herausgebildet, hinter der sich eine leicht unterschiedliche rechtliche Erfassung von Datenschutzproblemen verbirgt. Während der Bund neben den ("gewöhnlichen" oder "normalen") Personendaten den Begriff der "besonders schützenswerten" Personendaten kennt, unterscheiden manche neuere kantonale Gesetze zwischen (gewöhnlichen) und "besonderen" Personendaten.[3]

Konzeptuelle Unterschiede und Gemeinsamkeiten

[2] Beiden Konzeptionen ist gemeinsam, dass sie für die betreffenden öffentlichen Organe eine Unterscheidung treffen zwischen Bearbeitungen von Personendaten, die auf der Grundlage der zugehörigen Aufgaben-(bzw. Zweck-)norm bearbeitet werden dürfen - und Bearbeitungen von Personendaten, die eine qualifizierte gesetzliche Grundlage voraussetzen. Während jedoch das Bundesrecht (noch) auf die "Herkunft" der Daten abstützt, also auf die Frage, welcher Lebensbereich in den betreffenden Daten informativ abgebildet ist, stellen neuere kantonale Gesetze auf deren Grundrechtsrelevanz ab: Daten gelten dann als "besonders", wenn sie in einem *Kontext* bearbeitet werden, der die Grundrechte der Betroffenen gefährdet; wobei dieser Kontext sowohl die Art und Weise als auch das Umfeld der

[1] Stellungnahme des Büroausschusses von privatim, der Konferenz der schweizerischen Datenschutzbeauftragten, E-DSG: Leider keine souveräne Lösung, digma 2017.4, S. 248 f.

[2] Für weitere Beispiele vgl. die Vernehmlassung von privatim zum Vorentwurf eines revidierten Datenschutzgesetzes, S. 1 f., abrufbar unter http://www.privatim.ch/wpcontent/uploads/2017/03/privatimStellungnahmeVE-DSG.pdf.

[3] Für den Bund vgl. Art. 3 Abs 1 Bst. c DSG (SR 235.1), ähnlich etwa Art. 3 KDSG Bern (152.04); bezüglich der besonderen Personendaten vgl. etwa § 3 Abs. 3 IDG Zürich (170.4) sowie § 3 Abs. 4 IDG Basel-Stadt (153.260).

Bearbeitung umfasst.[4] Bedeutend sind insbesondere der verfassungsrechtliche Persönlichkeitsschutz im Sinne von Art. 10 Abs. 2 BV, Art. 13 Abs. 1 BV und Art. 8 EMRK sowie die damit verbundenen Kommunikations- sowie politischen und wirtschaftlichen Entfaltungsrechte.[5]

Die duale Rechtsnatur der besonders schützenswerten Personendaten

[3] Der bundesrechtliche Begriff der besonders schützenswerten Personendaten umfasst gemäss Art. 3 Abs. 1 Bst. c DSG Daten, die *Informationen* aus bestimmten Lebensbereichen abbilden, die im Gesetz abschliessend aufgelistet sind.[6] Dies bedeutet, dass nicht die Daten an sich sensibel sind, sondern die Verknüpfung der darin enthaltenen Information mit identifizierenden Merkmalen, wie Name, Geburtstag und Kontaktdaten - alles Daten, welche die Wahrscheinlichkeit der Identifikation der betreffenden Person erhöhen. Ausschlaggebend ist demnach die Verknüpfung einer Person mit einem sensiblen Bearbeitungskontext, wie etwa medizinische Therapie, Polizei oder Sozialhilfe. Eine solche informationelle Verknüpfung zeigt eine sehr hohe Wahrscheinlichkeit einer tatsächlichen Verknüpfung zwischen Personen und Lebensumständen an, die in der Regel als privat oder gar intim gelten. Entsprechend verkörpert Art. 3 Abs. 1 Bst. c DSG eine pauschale Vermutung des Gesetzgebers, dass die Bearbeitung solcher Daten einen Missbrauch im Sinne von Art. 13 Abs. 2 BV darstellt und damit die Persönlichkeitsrechte der Betroffenen verletzt.[7]

[4] Zu bedenken ist nun, dass der Begriff der besonders schützenswerten Personendaten auch für private Datenbearbeiter gilt. Dies bedeutet, dass die in Frage stehenden Persönlichkeitsverletzungen sowohl privatrechtlicher als auch verfassungsrechtlicher Natur sein können.[8] Der Unterschied liegt auf der Hand: während das erlaubte Restrisiko für staatliche Akteure an den Grundrechten gemessen wird, gilt für jenes der privaten Datenbearbeiter in erster Linie der Persönlichkeitsschutz des ZGB.[9] Damit ist bereits angedeutet, weshalb eine Trennung des privatrechtlichen und öffentlich-rechtlichen allgemeinen Datenschutzrechts sinnvoll wäre.

Risikoanalysen im Entwurf DSG

[5] Im Zuge der Revision des Datenschutzgesetzes möchte der Bund mehrere gesetzliche Risikoanalysen bezüglich der Grundrechtsgefährdung von Datenbearbeitungen einführen. Die Grundlagen hierzu finden sich im Gesetzesentwurf, welcher der Botschaft vom 15. September 2017 beigelegt wurde.[10] Zum

---

[4] Zum Ganzen PHILIP GLASS, Die rechtsstaatliche Bearbeitung von Personendaten in der Schweiz - Regelungs- und Begründungsstrategien des Datenschutzrechts mit Hinweisen zu den Bereichen Polizei, Staatsschutz, Sozialhilfe und elektronische Informationsverarbeitung, Diss. Uni Basel 2016, Zürich St. Gallen 2017, S. 120 ff. m.w.H.

[5] PHILIP GLASS, Die rechtsstaatliche Bearbeitung von Personendaten in der Schweiz, S. 164 f.

[6] Siehe dazu MAURER-LAMBROU/ KUNZ, BSK-DSG, Art. 3 N. 30.

[7] PHILIP GLASS, Die rechtsstaatliche Bearbeitung von Personendaten in der Schweiz, S. 122 f.

[8] So ausdrücklich die Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBl 2017 6941, 7059 (https://www.admin.ch/opc/de/federalgazette/2017/6941.pdf; Stand: Januar 2018).

[9] Im Ergebnis ebenso DAVID ROSENTHAL, Personendaten ohne Identifizierbarkeit?, digma 2017.4, S. 198 f., der insbesondere darauf Wert legt, dass die Drittwirkung von Grundrechten im Schweizer Recht die Ausnahme sei; präzisierend ist anzufügen, dass damit die direkte Drittwirkung gemeint ist; siehe GIOVANNI BIAGGINI, Kommentar BV, 2. überarbeitete und erweiterte Auflage,Zürich 2017, BV 35, N 18; ähnlich die Vernehmlassung der Konferenz der Schweizerischen Datenschutzbeauftragten (privatim), zum Vorentwurf eines revidierten Datenschutzgesetzes, S. 1; unterschiedliche "Rechtfertigungskonzepte" (Legalitätsprinzip vs. Vertragsfreiheit/Einwilligung).

[10] Entwurf des Bundesgesetzes über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer

einen soll Art. 30 E-DSG mehrere (implizite) Pflichten zur Risikoanalyse enthalten. Zum anderen soll das Gesetz für gewisse Datenbearbeitungen in Art. 20 E-DSG ausdrücklich eine sog. *Datenschutz-Folgenabschätzung*[11] verlangen.

Grundrechtliche Risikoanalyse als Voraussetzung der Datenbearbeitung

[6] Der Entwurf zum totalrevidierten DSG sieht in Art. 30 Abs. 2 Bst. c E-DSG vor, dass für die Bearbeitung von Personendaten dann eine Grundlage in einem Gesetz erforderlich ist, wenn "der Bearbeitungszweck oder die Art und Weise der Datenbearbeitung "[...] zu einem schwerwiegenden Eingriff in die Grundrechte der betroffenen Person führen [können]".[12] Dieses Erfordernis tritt als neue Form der Qualifikation neben die Bearbeitung von besonders schützenswerten Personendaten (Bst. a) und Profiling (Bst. b). Damit würde das Bundesrecht den neueren kantonalen Datenschutzgesetzen angeglichen. Der Unterschied etwa zum IDG Zürich bestünde darin, dass die Kategorie der besonders schützenswerten Personendaten nach wie vor als eigenständiger Qualifikationsgrund bestehen bliebe und nicht als Unterfall der Grundrechtsgefährdung behandelt würde.

[7] Umgekehrt soll Art. 30 Abs. 3 Bst. b ermöglichen, in Fällen der Bearbeitung von besonders schützenswerten Personendaten, die keine besonderen Gefahren für die Grundrechte der Betroffenen aufweisen, auf eine qualifizierte gesetzliche Grundlage zu verzichten. Hier würde eine Rechtsgrundlage in einem gesetzeskonkretisierenden Erlass ausreichen.[13]

[8] Daraus folgt, dass künftig für jede Bearbeitung von Personendaten durch Organe des Bundes eine grundrechtliche Risikoanalyse notwendig sein wird. Je nach Ausgang dieser Analyse wäre eine Bearbeitungsgrundlage in einem Gesetz oder einem kompetenzmässig erlassenen Rechtssatz notwendig. Hinzu tritt nun die datenschutzrechtliche Folgeabschätzung, welche auch für private Datenbearbeiter gilt. Das Verhältnis der beiden Vorschriften zueinander ist nicht klar, sie scheinen sich in einem Punkt gar zu widersprechen.

Folgenabschätzung vs. Risikoanalyse nach Art. 30 E-DSG

[9] Offensichtlich ist zunächst, dass die Datenschutz-Folgenabschätzung nach Art. 20 E-DSG und die Risikoanalyse nach Art. 30 E-DSG in zwei verschiedenen Kapiteln geregelt sind: die Folgeabschätzung im Kapitel "Pflichten des Verantwortlichen und des Auftragsbearbeiters", die grundrechtliche Risikoanalyse im Kapitel "Besondere Bestimmungen zur Datenbearbeitung durch Bundesorgane". Die Botschaft betont, dass die Folgeabschätzung sowohl von Bundesorganen und Privaten gleichermassen durchzuführen ist (dies legt auch die Systematik des Gesetzes nahe) und daher sowohl im Hinblick auf die Gefährdung von Persönlichkeitsrechten des ZGB (Private) als auch der Grundrechte (Bundesorgane) Anwendung findet.[14] Demgegenüber gilt Art. 30 E-DSG nur für Bundesorgane. Dies bedeutet, dass das

---

Erlasse zum Datenschutz, BBl 2017 7193 (https://www.admin.ch/opc/de/federal-gazette/2017/7193.pdf; Stand Januar 2018).

[11] Diese wird aus dem EU-Recht übernommen; vgl. Botschaft E-DSG, BBl 2017 6941, 7059; sie ist im kantonalen Recht bereits in der Form der datenschutzrechtlichen Vorabkontrolle bekannt (vgl. z.B. § 10 IDG-ZH).

[12] Der Entwurf schreibt für schwerwiegende Grundrechtsgefährdungen eine Rechtsgrundlage in einem Gesetz ("Gesetz im formellen Sinn") vor, gibt indes keine Anhaltspunkte dafür, wie eine solche Grundlage inhaltlich auszugestalten ist bzw. welche Fragen darin zu regeln wären; vgl. dagegen die Liste der zu regelnden Punkte im Urteil des EGMR Vukota-Bojic gegen die Schweiz vom 18. Oktober 2016 (Nr. 61838/10).

[13] "Gesetz im materiellen Sinn", OFK-BIAGGINI, BV 36, N 14: "d.h. eine kompetenzgemäss erlassene generell-abstrakte Norm".

[14] Botschaft BBl 2017 6941, 7059 f.; "Die vorliegende Bestimmung gilt sowohl für private Verantwortliche als auch für

Gesetz für diese zwei Risikoanalysen vorsieht. Zwei Punkte springen hier ins Auge.

[10] Ein hohes Risiko im Sinne der Folgeabschätzung liegt gemäss Art. 20 Abs. 2 Bst. a E-DSG "bei der umfangreichen Bearbeitung besonders schützenswerter Personendaten" vor. Würde dieses Kriterium auf die Ausnahme in Art. 30 Abs. 3 Bst. b E-DSG angewendet, bedeutete dies umgekehrt, dass Bearbeitungen von besonders schützenswerten Personendaten, die nicht "umfangreich" sind, stets als nicht besonders riskant eingestuft werden könnten. Dadurch droht die Ausrichtung von Art. 30 E-DSG ausgehebelt zu werden, der als grundrechtliche Schutzbestimmung auf die Belastung in Einzelfällen ausgerichtet ist. Ein hohes Risiko liegt nach der Bestimmung zur Folgeabschätzung sodann vor, wenn es sich bei der Bearbeitung um ein *Profiling* handelt (Art. 20 Abs. 2 Bst. b E-DSG). Gemäss Art. 30 Abs. 3 Bst. b E-DSG muss ein Profiling jedoch nicht notwendigerweise ein hohes Risiko für die Grundrechte bedeuten.[15] Auf der anderen Seite wird dagegen kritisiert, dass für private Bearbeiter - für die Art. 30 E-DSG nicht gilt - Profiling *immer* ein hohes Risiko darstellt und daher auch in unbedenklichen Fällen eine Pflicht zur Folgeabschätzung auslöst.[16]

[11] Die beiden Konstellationen könnten aus Sicht des öffentlich-rechtlichen Datenschutzrechts auf einfache Weise aufgelöst werden, wenn man davon ausginge, dass die in Art. 20 Abs. 2 E-DSG genannten Fälle als gesetzliche Vermutungen schwerer Grundrechtsgefährdung im Sinne von Art. 30 Abs. 2 Bst. c E-DSG gelten sollen. Doch das Gesetz selbst zählt diese ausdrücklich "namentlich" auf und die Botschaft macht deutlich, dass es sich hierbei um Fälle handelt, "in denen ein hohes Risiko *vorliegt*".[17] Man muss daher davon ausgehen, dass der Begriff des "hohen Risikos für die Persönlichkeit oder die Grundrechte der betroffenen Person" nicht identisch ist mit der in Art. 30 Abs. 2 Bst. c E-DSG vorausgesetzten Risikos eines "schwerwiegenden Eingriffs in die Grundrechte der betroffenen Personen", sondern ein eigenständiger Rechtsbegriff in Bezug auf die Voraussetzungen der Folgeabschätzung. Erfasst sind wohl zusätzlich Risiken unterhalb der schweren Eingriffsschwelle, die aber aufgrund der hohen Wahrscheinlichkeit ihrer Verwirklichung dennoch sichernde Massnahmen erfordern. Solche Risiken müssten in einem separaten Schritt *zusätzlich* auf ihr Gefährdungspotenzial im Sinne von Art. 30 Abs. 2 Bst. c E-DSG geprüft werden (bzw. umgekehrt).

Die Lösung neuerer kantonaler Datenschutzgesetze

[12] Im Vergleich zum bundesrechtlichen Entwurf lösen moderne kantonale Datenschutzgesetze diese Probleme eleganter - was durchaus auch dem Umstand zu verdanken sein dürfte, dass sie nicht zugleich öffentlich-rechtliche und privatrechtliche Datenbearbeitungen regeln müssen.

Das Gesetz über die Information und den Datenschutz des Kantons Zürich (IDG; 170.4) etwa definiert den Unterschied zwischen gewöhnlichen und besonderen (i.e. qualifizierten) Personendaten in § 3

Bundesorgane, weshalb nicht nur von einem Risiko für die Persönlichkeit der betroffenen Person, sondern auch für deren Grundrechte die Rede ist"; sowie: "Bei der Konkretisierung dieses Risikos stehen das Recht auf informationelle Selbstbestimmung sowie das Recht auf Privatsphäre im Vordergrund. Diese schützen sowohl die Autonomie des Einzelnen als auch dessen Würde und Identität" (7060).

[15] Ausdrücklich Botschaft, BBl 2017 6941, 7079: "Es ist denkbar, dass ein Profiling in bestimmten Fällen keine besonderen Risiken für die Grundrechte der betroffenen Person birgt".

[16] DAVID ROSENTHAL, Der Entwurf für ein neues Datenschutzgesetz - Was uns erwartet und was noch zu korrigieren ist, in: Jusletter vom 27. November 2017, Rz. 49.; DAVID VASELLA, Zum Entwurf des DSG vom 15. September 2017, www.datenrecht.ch, Beitrag vom 30. Oktober 2017, S. 4.

[17] Botschaft BBl 2017 6941, 7060 (Hervorhebung durch den Autor).

IDG wie folgt:[18]

Personendaten:

> Informationen, die sich auf eine bestimmte oder bestimmbare Person beziehen.

Besondere Personendaten:

> a. Informationen, bei denen wegen ihrer Bedeutung, der Art ihrer Bearbeitung oder der Möglichkeit ihrer Verknüpfung mit anderen Informationen die besondere Gefahr einer Persönlichkeitsverletzung besteht, wie Informationen über
>
> 1. die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten,
> 2. die Gesundheit, die Intimsphäre, die Rassenzugehörigkeit oder die ethnische Herkunft,
> 3. Massnahmen der sozialen Hilfe,
> 4. administrative oder strafrechtliche Verfolgungen oder Sanktionen.

Die **Gesetzmässigkeit** der Datenbearbeitung ist in § 8 IDG geregelt:

> 1 Das öffentliche Organ darf Personendaten bearbeiten, soweit dies zur Erfüllung seiner gesetzlich umschriebenen Aufgaben geeignet und erforderlich ist.
>
> 2 Das Bearbeiten besonderer Personendaten bedarf einer hinreichend bestimmten Regelung in einem formellen Gesetz.

Schliesslich regelt § 10 IDG die **Vorabkontrolle**:

> Das öffentliche Organ unterbreitet eine beabsichtigte Bearbeitung von Personendaten mit besonderen Risiken für die Rechte und Freiheiten der betroffenen Personen vorab der oder dem Beauftragten für den Datenschutz zur Prüfung.

[13] Dieser Regelungskomplex unterscheidet sich von jenem des bundesrechtlichen Entwurfs in den folgenden Aspekten:

- Die Unterscheidung zwischen gewöhnlichen und besonderen Personendaten ist funktional auf die Bearbeitung im Kontext des verfassungsrechtlichen Grundrechtsschutzes ausgerichtet und nicht auf eine abschliessende Liste von Lebensbereichen; geschützt sind nicht die Daten, sondern grundrechtlich relevante Verwendungszusammenhänge. Die Datenbearbeitungen, welche zur Vorabkontrolle vorgelegt werden müssen, bilden daher eine Teilmenge der besonderen Personendaten.

- Durch die grundrechtliche Ausrichtung der besonderen Personendaten wird der Begriff direkt mit der Gefährdung von Grundrechten der Betroffenen verknüpft. Dadurch kann eine umständliche Lösung, wie sie nun der bundesrechtliche Entwurf vorsieht, vermieden werden. Insbesondere werden keine Bestimmungen benötigt, um Personendaten, die nicht einem besonders schützenswerten Bereich entstammen, nachträglich dennoch als sensibel zu qualifizieren, und - noch bedeutsamer - es wird vermieden, eine Ausnahmeregelung schaffen zu müssen, wonach besonders schützenswerte Personendaten und Profile bei nachweislich geringem Risiko für die Grundrechte als unbedenklich "entqualifiziert" werden.[19]

---

[18] Ähnliche Bestimmungen finden sich beispielsweise in den Informations- und Datenschutzgesetzen der Kantone Basel-Stadt und Basel-Landschaft.

[19] Bedeutend ist in diesem Zusammenhang auch, dass das Erfordernis der gesetzlichen Grundlage ausdrücklich auf eine

- Die Bestimmung in § 3 IDG-ZH enthält dieselbe Liste von persönlichkeitsrechtlich riskanten Datenkategorien wie das Bundesrecht.[20] Im Gegensatz zum bundesrechtlichen DSG werden sie jedoch *beispielhaft* aufgezählt.[21]

- Die Entscheidung für eine Vorabklärung ist das Ergebnis einer routinemässigen verfassungsrechtlich ausgerichteten Risikoanalyse, wie sie aufgrund von § 3 IDG-ZH für jede Datenbearbeitung (mehr oder weniger aufwendig) durchgeführt werden muss. Sie fügt sich daher nahtlos in die entsprechenden Prozessabläufe der Behörden ein. Dagegen wird bei Durchlesen des Entwurfs zur Revision des DSG nicht klar, in welchem Verhältnis die Datenschutz-Folgeabklärung zur Beurteilung des grundrechtlichen Risikos im Hinblick auf die erforderliche gesetzliche Grundlage stehen soll. Auch die Botschaft schweigt zu dieser Frage.

Abschliessende Überlegungen: Zwei Massstäbe in einem Gesetz sorgen für Verwirrung

[14] Die grundrechtliche Ausrichtung der neueren kantonalen Datenschutzgesetze wäre auch für den Bund eine Lösung. Allerdings wird dies durch die duale Natur des Bundesdatenschutzrechts als zugleich öffentlich- und zivilrechtlich erschwert. Im Rahmen der privatrechtlichen Datenbearbeitung stehen privatrechtliche Prinzipien des ZGB und des OR im Vordergrund, insbesondere die Privatautonomie und die privatrechtlichen Rechtfertigungsvoraussetzungen des ZGB inkl. der Einwilligung in sensible Bearbeitungen.[22] Begrenzt werden diese durch das Verbot der übermässigen Bindung, das Verbot der Übervorteilung sowie die Auslegung dieser Bestimmungen im Sinne der Wahrnehmung von grundrechtlichen Schutzpflichten. Im Rahmen der öffentlich-rechtlichen Datenbearbeitung orientiert sich der Massstab am verfassungsrechtlichen Persönlichkeitsschutz, d.h. an den Grundrechten, bzw. deren Gefährdung, dem öffentlichen Interesse an der Durchsetzung der Grundrechte sowie dem Transparenz- bzw. Mitwirkungsprinzip. Die Idee, das privatrechtliche Datenschutzrecht aus dem DSG auszugliedern und an den Persönlichkeitsbestimmungen des ZGB auszurichten sollte daher dringend geprüft werden.

Präzisierung: Am 11. Januar 2018 beschloss die Staatspolitische Kommission des Nationalrates, auf die Vorlage des Bundesrates für die Totalrevision und die Änderung weiterer Erlasse zum Datenschutz einzutreten, diese aber in zwei Teile zu gliedern: vorgezogen wird zunächst die Anpassung an das europäische Recht, bevor in einem zweiten Schritt die Totalrevision des DSG erfolgen soll.[23] Verhalten

---

"hinreichend bestimmte Regelung" abstützt; im Ergebnis kann in unbedenklichen Fällen eine implizite Grundlage im formellen Gesetz (evtl. auf Ebene einer VO konkretisiert) ausreichen; zu den impliziten Bearbeitungsbefugnissen siehe GLASS, Bearbeitung, S. 193 ff.

[20] Die Auflistung der besonders schützenswerten Datenkategorien entstammt ursprünglich Art. 6 des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten des Europarates (Konvention Nr. 108; 0.235.1).

[21] BEAT RUDIN, in: Baeriswyl/Rudin (Hrsg.), Praxiskommentar zum Informationsund Datenschutzgesetz des Kantons Zürich (IDG), Zürich Basel Genf 2012, § 3 Rz. 20; "nicht abschliessend" aufgezählte Kategorien der "sensitiven Personendaten".

[22] Dagegen kann die Einwilligung im öffentlich-rechtlichen Bereich mangels Verfügungsmacht über den gesamten Einwilligungsgegenstand für die meisten Formen der Bearbeitung von besonderen Personendaten gerade nicht rechtfertigend wirken; siehe GLASS, Bearbeitung, S. 235 f.; im Ergebnis ebenso TOBIAS FASNACHT, Die Einwilligung im Datenschutzrecht, Diss. Freiburg 2017, Zürich Basel Genf 2017, S. 94; "Wird die staatliche Aufgabe im Gesetz nicht klar umschrieben, dürfte dies sodann dem Legalitätsprinzip widersprechen; ein Zustand, der durch eine datenschutzrechtliche Einwilligung nicht behoben werden kann.

[23] Siehe dazu die Medienmitteilung der SPK-N vom 12. Januar 2018.

kritisch äusserte sich der EDOEB, der mit Sicht auf die Notwendigkeit eines den wachsenden Risiken der fortschreitenden Digitalisierung gerecht werdenden Datenschutzes insbesondere eine "zügige Gesamtablösung des geltenden DSG" fordert, "das aus dem Jahre 1993 stammt".[24] Damit bleibt denkbar, dass das zivilrechtliche Datenschutzrecht aus dem DSG herausgelöst oder zumindest innerhalb einer Gesamtkodifizierung deutlicher am ZGB ausgerichtet wird.

[24] Siehe die Medienmitteilung des EDOEB vom 12. Januar 2018.