Antrag des Regierungsrates vom 4. Juli 2018

5471

Gesetz über die Information und den Datenschutz (IDG)

(Änderung vom . . . . . .;
Anpassung an die europäische Datenschutzreform)

Der Kantonsrat,

nach Einsichtnahme in die Anträge des Regierungsrates vom 4. Juli 2018,

beschliesst:

I. Das Gesetz über die Information und den Datenschutz vom 12. Februar 2007 wird wie folgt geändert:

Geltungsbereich

§ 2. Dieses Gesetz gilt für die öffentlichen Organe.

Ausnahmen a. Kantonsrat

§ 2 a. [1] Dieses Gesetz gilt nicht für das Verhältnis zwischen dem Kantonsrat und seinen ständigen Kommissionen sowie den Behörden und Anstalten, die seiner Oberaufsicht unterstehen.

[2] Soweit der Kantonsrat diesem Gesetz untersteht, stehen der oder dem Beauftragten für den Datenschutz die Befugnisse gemäss § 10 Abs. 2, § 12 a Abs. 1 und 2, § 34 lit. c, d und f sowie §§ 35–36 a nicht zu.

b. Gerichte und Strafverfolgungsbehörden

§ 2 b. [1] Bei Gerichtsverfahren sowie Verfahren von Strafverfolgungsbehörden gemäss § 86 Abs. 1 lit. b und c des Gesetzes über die Gerichts- und Behördenorganisation im Zivil- und Strafprozess vom 10. Mai 2010 richten sich die Rechte der betroffenen Personen und die Einsichtsrechte Dritter nach den spezialgesetzlichen Bestimmungen.

[2] Für die Bearbeitung von Personendaten gilt dieses Gesetz, soweit Spezialgesetze keine Regelungen enthalten.

[3] Soweit die Gerichte diesem Gesetz unterstehen, stehen der oder dem Beauftragten für den Datenschutz die Befugnisse gemäss § 10 Abs. 2, § 12 a Abs. 1 und 2, § 34 lit. c, d und f sowie §§ 35–36 a nicht zu.

c. Teilnahme am wirtschaftlichen Wettbewerb

§ 2 c. [1] Dieses Gesetz gilt nicht, soweit öffentliche Organe am wirtschaftlichen Wettbewerb teilnehmen und dabei nicht hoheitlich handeln.

[2] Für das Bearbeiten von Personendaten ist das Bundesgesetz über den Datenschutz* sinngemäss anwendbar. Die Aufsicht wird von der oder dem Beauftragten für den Datenschutz gemäss §§ 30 ff. ausgeübt.

Begriffe

§ 3. [1] Öffentliche Organe sind:

a. der Kantonsrat, die Gemeindeparlamente sowie die Gemeindeversammlungen,

b. Behörden und Verwaltungseinheiten des Kantons und der Gemeinden,

c. Organisationen und Personen des öffentlichen und privaten Rechts, soweit sie mit der Erfüllung öffentlicher Aufgaben betraut sind.

[2] Informationen sind alle Aufzeichnungen, welche die Erfüllung einer öffentlichen Aufgabe betreffen, unabhängig von ihrer Darstellungsform und ihrem Informationsträger. Ausgenommen sind Aufzeichnungen, die nicht fertig gestellt oder die ausschliesslich zum persönlichen Gebrauch bestimmt sind.

[3] Personendaten sind Informationen, die sich auf eine bestimmte oder bestimmbare Person beziehen.

[4] Besondere Personendaten sind:

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

Ziff. 1 unverändert.

2. die Gesundheit, die Intimsphäre, die ethnische Herkunft sowie genetische und biometrische Daten,

Ziff. 3 und 4 unverändert.

lit. b unverändert.

c. automatisierte Auswertungen von Informationen, um wesentliche persönliche Merkmale zu analysieren oder persönliche Entwicklungen vorherzusagen (Profiling).

[5] Bearbeiten ist jeder Umgang mit Informationen wie das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben oder Vernichten.

[6] Bekanntgeben ist das Zugänglichmachen von Informationen wie das Einsichtgewähren, Weitergeben oder Veröffentlichen.

---

* Das Bundesgesetz vom 19. Juni 1992 (DSG) wird totalrevidiert. In Sinne eines dynamischen Verweises ist einstweilen auf eine Datumsangabe zu verzichten.

Datenschutz-Folgenabschätzung, Vorabkontrolle

§ 10. [1] Das öffentliche Organ bewertet bei einer beabsichtigten Bearbeitung von Personendaten deren Risiken für die Grundrechte der betroffenen Personen.

[2] Es unterbreitet eine beabsichtigte Bearbeitung von Personendaten mit besonderen Risiken für die Grundrechte der betroffenen Personen vorab der oder dem Beauftragten für den Datenschutz zur Prüfung.

Information über die Beschaffung

§ 12. [1] Das öffentliche Organ informiert die betroffenen Personen über die Beschaffung von Personendaten. Dies gilt auch für die Beschaffung bei Dritten.

[2] Die Information enthält Angaben über

a. das verantwortliche öffentliche Organ,
b. die beschafften Daten oder deren Kategorien,
c. die Rechtsgrundlage und den Zweck der Bearbeitung,
d. die Datenempfänger oder die Kategorien der Datenempfänger, falls die Daten Dritten bekannt gegeben werden,
e. die Rechte der betroffenen Person.

[3] Die Informationspflicht entfällt,

a. wenn die betroffene Person bereits über die Angaben gemäss Abs. 2 verfügt,
b. wenn die Beschaffung der Personendaten gesetzlich vorgesehen ist,
c. wenn die Information nicht möglich ist oder einen unverhältnismässigen Aufwand erfordern würde,
d. in den Fällen gemäss § 23.

Meldepflicht

§ 12 a. [1] Das verantwortliche öffentliche Organ meldet der oder dem Beauftragten für den Datenschutz unverzüglich die unbefugte Bearbeitung oder den Verlust von Personendaten, wenn die Grundrechte der betroffenen Person gefährdet sind.

[2] Es informiert die betroffene Person, wenn die Umstände es erfordern oder die oder der Beauftragte für den Datenschutz es verlangt.

[3] Es kann die Information der betroffenen Person ganz oder teilweise einschränken, wenn ein überwiegendes öffentliches oder privates Interesse entgegensteht.

Einhaltung der Datenschutzbestimmungen und Qualitätssicherung

§ 13. [1] Das öffentliche Organ stellt die Einhaltung der Datenschutzbestimmungen insbesondere durch Organisationsvorschriften sicher.

[2] Es kann zur Sicherstellung der Qualität der Informationsbearbeitung seine Verfahren, seine Organisation und seine technischen Einrichtungen durch eine unabhängige und anerkannte Stelle prüfen und bewerten lassen.

Abs. 2 wird zu Abs. 3.

Schutz eigener Personendaten

§ 21. Abs. 1 unverändert.

[2] Wird die Berichtigung oder Vernichtung von Personendaten verlangt und kann weder deren Richtigkeit noch Unrichtigkeit festgestellt werden, bringt das öffentliche Organ den Vermerk an, dass die Personendaten bestritten sind. Es schränkt die Bearbeitung ein.

Empfehlungen

§ 36. Abs. 1 unverändert.

[2] Folgt das öffentliche Organ einer Empfehlung nicht, teilt es dies der oder dem Beauftragten für den Datenschutz unter Angabe der Gründe mit.

Abs. 3 wird aufgehoben.

Verwaltungsmassnahmen

§ 36 a. [1] Folgt das öffentliche Organ bei einer erheblichen Verletzung von Bestimmungen über den Datenschutz einer Empfehlung nicht, kann die oder der Beauftragte verfügen, dass die Bearbeitung ganz oder teilweise angepasst, unterbrochen oder abgebrochen wird und die Personendaten ganz oder teilweise gelöscht oder vernichtet werden.

[2] Das betroffene öffentliche Organ kann Verfügungen des oder der Beauftragten mit Beschwerde beim Verwaltungsgericht anfechten. Parteien sind die oder der Beauftragte und das betroffene öffentliche Organ.

II. Das Verwaltungsrechtspflegegesetz vom 24. Mai 1959 wird wie folgt geändert:

Akteneinsicht a. Grundsatz

§ 8. Abs. 1 und 2 unverändert.

[3] Die Information über Gerichtsverfahren und die Akteneinsicht Dritter richten sich vor Verwaltungsgericht und den ihm unterstellten Gerichten nach der Verordnung des Plenarausschusses der Gerichte gemäss § 73 Abs. 1 lit. d des Gesetzes über die Gerichts- und Behördenorganisation im Zivil- und Strafprozess (GOG) vom 10. Mai 2010.

III. Das Gesetz über die Gerichts- und Behördenorganisation im Zivil- und Strafprozess vom 10. Mai 2010 wird wie folgt geändert:

Datenschutzberatung

§ 88 b. [1] Die Oberstaatsanwaltschaft und die Oberjugendanwaltschaft bezeichnen je eine für die Datenschutzberatung zuständige Person.

[2] Diese hat folgende Aufgaben:

a. Sie berät und unterstützt bei der Bearbeitung von Personendaten.
b. Sie nimmt Datenschutz-Folgenabschätzungen gemäss § 10 Abs. 1 des Gesetzes über die Information und den Datenschutz vom 12. Februar 2007 vor.
c. Sie ist Ansprechperson der oder des Beauftragten für den Datenschutz und arbeitet mit dieser oder diesem zusammen.

Akteneinsicht

§ 151 d. [1] Die Akten abgeschlossener Strafverfahren können eingesehen werden:

lit. a unverändert.

b. von anderen Behörden, wenn sie diese für die Bearbeitung hängiger Zivil-, Straf- oder Verwaltungsverfahren benötigen und der Einsichtnahme keine überwiegenden öffentlichen oder privaten Interessen entgegenstehen.

[2] Dritten steht kein Recht auf Einsicht in Akten abgeschlossener Strafverfahren zu. Die zuständige Strafbehörde kann ihnen Akteneinsicht gewähren, wenn

a. sie ein wissenschaftliches oder ein anderes schützenswertes Interesse geltend machen und
b. der Einsichtnahme keine überwiegenden öffentlichen oder privaten Interessen entgegenstehen.

IV. Das Straf- und Justizvollzugsgesetz vom 19. Juni 2006 wird wie folgt geändert:

Datenschutzberatung

§ 18 a. [1] Die für den Vollzug zuständige Amtsstelle bezeichnet eine für die Datenschutzberatung zuständige Person.

[2] Diese hat folgende Aufgaben:

a. Sie berät und unterstützt die Strafvollzugsbehörden bei der Bearbeitung von Personendaten.
b. Sie nimmt Datenschutz-Folgenabschätzungen gemäss § 10 Abs. 1 des Gesetzes über die Information und den Datenschutz vom 12. Februar 2007 vor.

c. Sie ist Ansprechperson der oder des Beauftragten für den Datenschutz und arbeitet mit dieser oder diesem zusammen.

V. Das Polizeigesetz vom 23. April 2007 wird wie folgt geändert.

Datenbearbeitung

§ 52. Abs. 1 unverändert.

[2] Die Polizei kann Personendaten, einschliesslich besonderer Personendaten, und Persönlichkeitsprofile bearbeiten sowie Profiling vornehmen, soweit es zur Erfüllung der ihr gesetzlich übertragenen Aufgaben unentbehrlich ist.

Abs. 3 unverändert.

[4] Die Polizei kann Personendaten, einschliesslich besonderer Personendaten, anderen öffentlichen Organen sowie den Organen anderer Kantone oder des Bundes und Dritten von Amtes wegen oder auf Ersuchen im Einzelfall unter den Voraussetzungen von §§ 16 und 17 IDG bekannt geben.

Abs. 5 unverändert.

Datenschutzberatung

§ 54 c. [1] Die Polizeien bezeichnen je eine für die Datenschutzberatung zuständige Person.

[2] Diese hat folgende Aufgaben:

a. Sie berät und unterstützt die Polizeien bei der Bearbeitung von Personendaten.

b. Sie nimmt Datenschutz-Folgenabschätzungen gemäss § 10 Abs. 1 IDG vor.

c. Sie ist Ansprechperson der oder des Beauftragten für den Datenschutz und arbeitet mit dieser oder diesem zusammen.

[3] Die für die Datenschutzberatung zuständige Person einer Polizei kann diese Aufgabe für mehrere Polizeien erfüllen. Die beteiligten Polizeien regeln die Einzelheiten.

VI. Diese Gesetzesänderungen unterstehen dem fakultativen Referendum.

Weisung

A. Ausgangslage

1. Auswirkungen der europäischen Rechtsentwicklung auf die Schweiz

Die Europäische Union hat 2016 eine Reform ihrer Datenschutzgesetzgebung verabschiedet. Diese Reform umfasst die Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr (Richtlinie [EU] 2016/680) und die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung). Zusätzlich hat ein Ad-hoc-Ausschuss des Europarates Ende des ersten Halbjahres 2016 seine Arbeiten zur Revision des Übereinkommens vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen SEV 108) und des entsprechenden Zusatzprotokolls vom 8. November 2001 abgeschlossen.

Die Richtlinie (EU) 2016/680 stellt für die Schweiz eine Weiterentwicklung des Schengen-Besitzstands dar, weshalb die Schweiz gemäss den Schengen-Assoziierungsabkommen verpflichtet ist, ihre innerstaatliche Rechtsordnung entsprechend anzupassen. Sie muss diese innert zweier Jahre ab dem Zeitpunkt der Notifikation umsetzen. Da die Notifikation am 1. August 2016 erfolgte, dauert die Frist für die Übernahme des Rechtsaktes bis zum 1. August 2018.

In den Bereichen, die nicht der Schengen-Zusammenarbeit unterstehen, gilt die Schweiz als Drittstaat. Im Gegensatz zur Richtlinie (EU) 2016/680 muss sie die Datenschutz-Grundverordnung, die nicht Gegenstand des Schengen-Acquis ist, deshalb grundsätzlich nicht übernehmen. Allerdings dürfen zwischen einem Drittstaat und den Mitgliedstaaten der Europäischen Union Daten nur ausgetauscht werden, wenn der Drittstaat ein angemessenes Schutzniveau gewährleistet. Die Europäische Kommission hat in einem Angemessenheitsbeschluss vom 26. Juli 2000 bestätigt, dass die Schweiz über ein angemessenes Datenschutzniveau verfügt. Diese Entscheidung beruhte auf dem in der Richtlinie 95/46/EG festgelegten Schutzniveau. Künftig wird die schweizerische Gesetzgebung jedoch anhand der in der Datenschutz-Grundverordnung enthaltenen Anforderungen überprüft werden. Falls die Schweiz den

Angemessenheitsbeschluss beibehalten bzw. im Falle eines Widerrufs erneut eine Bestätigung über das angemessene Datenschutzniveau erhalten möchte, ist von zentraler Bedeutung, dass die schweizerische Gesetzgebung einen den Anforderungen dieser Verordnung entsprechenden Schutz gewährleistet. Die Datenschutz-Grundverordnung beeinflusst die datenschutzrechtlichen Regelungen in der Schweiz daher mittelbar. Die EU wird der Schweiz den Angemessenheitsbeschluss nur bestätigen, wenn Bund und Kantone die Anforderungen der Datenschutz-Grundverordnung im Grundsatz umsetzen. Zusätzlich hat das in der Datenschutz-Grundverordnung verankerte Marktortprinzip einen Einfluss auf die gesetzlichen Normen für öffentliche Organe, die grenzüberschreitend tätig sind. In diesem Bereich werden künftig die Vorgaben der Datenschutz-Grundverordnung gelten.

Der Revisionsentwurf zum Übereinkommen SEV 108 (E-SEV 108) entspricht der Richtlinie (EU) 2016/680 und der Datenschutz-Grundverordnung inhaltlich weitgehend, ist jedoch weniger detailliert. Die Europäische Kommission, welche die Mitgliedstaaten der Europäischen Union bei den Verhandlungen vertrat, hat darauf geachtet, dass der Inhalt des E-SEV 108 mit dem neuen Recht der Europäischen Union vereinbar ist.

2. Umsetzung auf Bundesebene

Der Bundesrat hat die Umsetzungsarbeiten der europäischen Vorlagen koordiniert, obwohl das Übereinkommen SEV 108 noch nicht verabschiedet ist, und den eidgenössischen Räten ein auf diesen Revisionen beruhenden Entwurf zu einer Totalrevision des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz (DSG) unterbreitet. Der Nationalrat hat am 12. Juni 2018 beschlossen, die Revision des Datenschutzrechts in zwei Etappen anzugehen. In einer ersten Etappe hat er die notwendigen Anpassungen an die Anforderungen des EU-Rechts (Richtlinie 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten im Bereich des Strafrechts) für die öffentlichen Organe vorgenommen und das «Bundesgesetz über den Datenschutz im Rahmen der Anwendung des Schengen-Besitzstands in Strafsachen» (Schengen-Datenschutzgesetz, SDSG) verabschiedet. Die zweite Etappe der Revision, welche die Totalrevision des Bundesgesetzes über den Datenschutz umfasst und insbesondere die Datenbearbeitungen durch private Datenbearbeitende regeln soll, wurde zurückgestellt. Die Staatspolitische Kommission des Nationalrates wird jedoch auch diese Revision umgehend in Angriff nehmen. Das Schengen-Datenschutzgesetz wird deshalb voraussichtlich nur während kurzer Zeit gelten, nämlich bis die eidgenössischen Räte die Totalrevision

des Bundesgesetzes über den Datenschutz abgeschlossen haben und diese in Kraft gesetzt sein wird.

3. Umsetzung auf kantonaler Ebene

Mit der vorliegenden Revision soll sichergestellt werden, dass die Anforderungen der EU-Richtlinie zum Datenschutz (Richtlinie [EU] 2016/680), die als Weiterentwicklung des Schengen/Dublin-Besitzstands zwingend ist, erfüllt werden. Zudem sollen die Voraussetzungen geschaffen werden, dass die Schweiz weiterhin einen Angemessenheitsbeschluss erwirken und die revidierte Europarats-Konvention zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen SEV 108) unterzeichnen kann.

Für die Umsetzung in den Kantonen hat die Arbeitsgruppe Datenschutz der interkantonalen Begleitorganisation Schengen/Dublin der Konferenz der Kantone den Leitfaden «EU-Datenschutzreform/Modernisierung der Europarats-Konvention 108: Anpassungsbedarf bei den kantonalen (Informations- und) Datenschutzgesetzen» (nachfolgend Leitfaden) erarbeitet, der sich allerdings auf die in der Datenschutzgesetzgebung notwendigen Anpassungen beschränkt. Dieser Leitfaden bildet die Grundlage der Vorlage. Zusätzlich sind Anpassungen in verschiedenen Spezialgesetzen gestützt auf die Richtlinie [EU] 2016/680 vorzunehmen. Soweit sich zusätzlicher Anpassungsbedarf in Spezialgesetzen für privatwirtschaftlich und grenzüberschreitend tätige öffentlich-rechtliche Anstalten ergeben sollte, ist die Revision des Bundesgesetzes über den Datenschutz abzuwarten und allfällige Änderungen sind erst im Anschluss daran vorzunehmen. Dabei werden auch allenfalls notwendige Anpassungen gestützt auf das in der Datenschutz-Grundverordnung verankerte Marktortprinzip umzusetzen sein.

Im Unterschied zum vom Nationalrat angestrebten Vorgehen erscheint für den Kanton Zürich eine (weitere) Aufteilung des Revisionsvorhabens mit einer zusätzlichen Beschränkung auf die Teile, die als Weiterentwicklung des Schengen/Dublin-Besitzstands zwingend sind, nicht zielführend. Gegen eine weitere Aufteilung sprechen folgende Gründe:

– Die Konferenz der Kantone (KdK) hat an ihrer Plenarversammlung vom 24. Juni 2016 festgehalten, dass die Richtlinie von den Kantonen umgesetzt werden muss. Eine Arbeitsgruppe der KdK hat zuhanden der Kantone diejenigen Punkte herausgearbeitet, die voraussichtlich in den meisten Kantonen in die Revision der Datenschutzgesetzgebung aufgenommen werden müssen, und den Kantonen einen entsprechenden Leitfaden zur Verfügung gestellt. Sie hat

ihre Arbeiten mit den Entwürfen des Bundes zur Umsetzung der Richtlinie und zur Übernahme des Übereinkommens SEV 108 koordiniert. Verschiedene Kantone haben ihre Gesetzgebungsarbeiten in diesem Sinne auch bereits weit vorangetrieben.

– Der Geltungsbereich des Gesetzes über die Information und den Datenschutz (IDG; LS 170.4) ist auf öffentliche Organe beschränkt. Demgegenüber gilt das Bundesgesetz über den Datenschutz auch für Private. Insbesondere die (mittelbaren) Auswirkungen der Datenschutz-Grundverordnung auf die Privaten müssen von den eidgenössischen Räten noch eingehend beraten werden. Der Bund kann daher einen wesentlichen Teil der Umsetzungsarbeiten aufschieben und so eher gewährleisten, dass die Umsetzung als Folge des Schengen/Dublin-Nachvollzugs fristgerecht erfolgen kann.

Die Umsetzungsarbeiten in den Kantonen sind demgegenüber weit weniger aufwendig und können mit einer Teilrevision entsprechend dem Leitfaden mit überschaubarem Aufwand umgesetzt werden.

– Die Aufteilung im Kanton Zürich hätte zur Folge, dass im Kanton für die Strafgerichte andere Regeln gelten würden als für die Zivilgerichte, da eine Umsetzung nur für den Strafbereich Gegenstand des Schengen-Acquis ist. Dies ist für den Kanton Zürich, der keine separaten Gesetze für die Zivil- und Strafgerichtsbarkeit hat, sondern die Prozessgesetze des Bundes einheitlich umgesetzt hat (Gesetz über die Gerichts- und Behördenorganisation im Zivil- und Strafprozess [GOG; LS 211.1]), kein gangbarer Weg und würde zu einer Vielzahl von komplizierten Bestimmungen führen, die innert Kürze wieder überarbeitet werden müssten. Festzuhalten ist sodann, dass auch die vom Nationalrat verabschiedete Vorlage im Bereich der Gerichte Änderungen im Sinne der Vorschläge des Leitfadens vorsieht (Art. 2 Abs. 1 E-SDSG).

In diesem Zusammenhang bleibt zudem darauf hinzuweisen, dass die Staatspolitische Kommission des Nationalrates die Anpassungen zum Schengen/Dublin-Nachvollzug ebenfalls ohne Verzug in Angriff nehmen will. Der Nationalrat geht denn auch davon aus, dass im besten Fall das Schengen-Datenschutzgesetz gar nie in Kraft treten wird, wird dieses doch mit der anstehenden Totalrevision des Bundesgesetzes über den Datenschutz wieder aufgehoben werden. Eine Aufteilung im Kanton Zürich rechtfertigt sich folglich auch aus diesem Grund nicht, müsste doch der nach der Umsetzung des Schengen/Dublin-Nachvollzugs verbleibende Anpassungsbedarf ebenfalls unverzüglich umgesetzt werden.

B. Hauptsächlicher Anpassungsbedarf

1. Geltungsbereich

Für alle gerichtlichen Verfahren (zivil- und strafrechtliche sowie verwaltungsrechtliche Verfahren) ist eine Anpassung notwendig, da eine allgemeine Ausnahme vom Geltungsbereich gestützt auf die Richtlinie (EU) 2016/680 bzw. das Übereinkommen SEV 108 künftig nicht mehr zulässig sein wird. Festzuhalten ist dabei, dass die Verfahrensgesetze ihre Bedeutung weiterhin behalten, in den Verfahren der Zivil- und Strafrechtspflege zusätzlich aber die Grundsätze des Datenschutzrechts Anwendung finden. Gemäss dem erwähnten Leitfaden soll, um Kollisionen zwischen den verfahrensrechtlichen und den datenschutzrechtlichen Informationsansprüchen der Parteien bzw. betroffenen Personen zu vermeiden, deshalb vorgesehen werden, dass sich die Rechte und Ansprüche der betroffenen Personen während hängiger Verfahren der Zivil- und Strafrechtspflege ausschliesslich nach dem anwendbaren Verfahrensrecht richten. Die Vorlage berücksichtigt diese Anliegen, nimmt aber nicht nur die hängigen, sondern auch die abgeschlossenen Verfahren von der Geltung des Gesetzes über die Information und den Datenschutz aus. Dies entspricht im Kanton Zürich geltendem Recht, und es besteht kein Grund, von dieser Regelung abzuweichen. Allerdings sind die gesetzlichen Grundlagen etwas anzupassen. Zusätzlich sollen die Datenbearbeitungen in hängigen und abgeschlossenen gerichtlichen Verfahren von der Aufsicht der oder des Datenschutzbeauftragten ausgenommen werden.

Zusätzlich sind bei den Begriffsbestimmungen des Gesetzes über die Information und den Datenschutz gewisse Anpassungen notwendig (bezüglich biometrischer und genetischer Daten, Daten zum Sexualleben bzw. zur sexuellen Orientierung sowie im Zusammenhang mit Profiling).

2. Transparenzbestimmungen

Gestützt auf die Richtlinie (EU) 2016/680 bzw. das Übereinkommen SEV 108 treffen das für die Datenbearbeitung verantwortliche Organ neu verschiedene Pflichten, so die Pflicht zur Vornahme einer Datenschutz-Folgenabklärung, die Informationspflicht und die Pflicht, den betroffenen Personen Verletzungen der Datenschutzbestimmungen mitzuteilen. Diese Pflichten sind dem kantonalen Recht allerdings nicht völlig neu. Der Nachweis der Einhaltung der Datenschutzbestimmungen bei jeder geplanten Bearbeitung von Personendaten (Datenschutz-Folgenabschätzung) war zwar bis anhin im Gesetz über die Infor-

mation und den Datenschutz nicht ausdrücklich erwähnt. Allerdings ist bereits unter geltendem Recht «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» zu unterbreiten (Vorabkontrolle; § 10 IDG). Diese Pflicht konnte allerdings bereits bis anhin wohl nur erfüllt werden, wenn bei jedem Vorhaben, das eine Bearbeitung von Personendaten zum Inhalt hatte, geprüft wurde, ob dieses mit besonderen Risiken für die Rechte und Freiheiten der betroffenen Personen verbunden war. Neu ist deshalb lediglich, dass das Ergebnis der Prüfung dokumentiert werden muss. An diese Dokumentation müssen jedoch keine hohen Anforderungen gestellt werden. Mit der in § 12 IDG festgehaltenen Pflicht, dass die Beschaffung von Personendaten und insbesondere der Zweck ihrer Bearbeitung erkennbar sein müssen (Abs. 1) und bei der Beschaffung von besonderen Personendaten die betroffene Person vom Inhaber der Datensammlung über den Zweck der Datenbearbeitung informiert werden muss (Abs. 2), war auch eine Informationspflicht bereits im geltenden Recht – wenn auch in eingeschränkterem Mass – enthalten. Allerdings sind in Bezug auf die Informationspflicht Ausnahmen von den Vorgaben in der Richtlinie (EU) 2016/680 möglich. Davon soll im Kanton Zürich auch Gebrauch gemacht werden. Neu zu regeln ist des Weiteren die Meldepflicht an die Beauftragte oder den Beauftragten für den Datenschutz bei einer unbefugten Bearbeitung oder einem Verlust von Personendaten, wenn die Grundrechte der betroffenen Person gefährdet sind. Diese letzte Pflicht ist neu. Sie sollte aber, da davon auszugehen ist, dass solche Fehlleistungen nur äusserst selten vorkommen, nicht mit regelmässigem Aufwand verbunden sein, wobei in Einzelfällen ein erheblicher Aufwand anfallen kann.

3. Aufsichtsbereich

Gemäss den Vorgaben der Richtlinie (EU) 2016/680 müssen die Aufsichtsfunktionen der oder des Datenschutzbeauftragten (in der Terminologie der EU entspricht dies der «Aufsichtsbehörde») gestärkt werden. So muss die Möglichkeit geschaffen werden, dass die oder der Datenschutzbeauftragte Verfügungen zulasten der für die Datenbearbeitung verantwortlichen Stelle erlassen kann. Gemäss europäischem Recht muss auch die Kompetenz zum Erlass vorsorglicher Massnahmen bestehen. Diese Möglichkeit besteht gestützt auf § 6 des Verwaltungsrechtspflegegesetzes vom 24. Mai 1959 (VRG; 175.2) ohnehin, sodass sich eine Regelung im Gesetz über die Information und den Datenschutz erübrigt.

Nicht umgesetzt werden soll das «Recht auf Beschwerde an die oder den Beauftragten für den Datenschutz» (Leitfaden 5.10). Der Leitfaden geht davon aus, dass damit das Recht auf Aufsichtsbeschwerde gemeint ist, wird doch verlangt, dass jede betroffene Person unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs das «Recht auf Beschwerde» bei der oder dem Datenschutzbeauftragten hat, wenn sie der Ansicht ist, dass die Bearbeitung der sie betreffenden Personendaten gegen die datenschutzrechtlichen Vorschriften verstösst. Gemäss Leitfaden soll die Pflicht der oder des Beauftragten für den Datenschutz, Anzeigen bzw. Beschwerden von betroffenen Personen innert angemessener Frist zu behandeln, in einem Gesetz festgehalten werden. Die Aufsichtsbeschwerde ist ein blosser Rechtsbehelf, der sich aus der Aufsichtsbefugnis ableitet. Sie erlaubt der Aufsichtsbehörde ein Eingreifen allerdings nur, wenn kein eigentliches Rechtsmittel gegeben ist. Gesetzlich geregelt ist sie im VRG nicht. Im Kanton Zürich werden aber in der Praxis sämtliche Aufsichtsbeschwerden behandelt. Die heutige Bestimmung in § 34 lit. b IDG, wonach die oder der Beauftragte für den Datenschutz Privatpersonen berät, ist folglich als ausreichend zu erachten, und eine Ergänzung, dass sie oder er ihre Eingaben auch zu behandeln hätte, brächte keinen gesetzgeberischen Mehrwert.

4. Revision weiterer Gesetze

Für Datenbearbeitungen im Bereich der Strafverfolgung und des Strafvollzugs ist eine Datenschutzberaterin oder ein Datenschutzberater einzuführen. Diese Anforderung ist im GOG, im Polizeigesetz (PolG; LS 550.1) sowie im Straf- und Justizvollzugsgesetz (StJVG; LS 331) umzusetzen.

C. Ergebnis der Vernehmlassung

Die vorgeschlagenen Anpassungen wurden in der Vernehmlassung weitgehend wohlwollend aufgenommen. In Einzelfragen wurden kleinere Anpassungen vorgeschlagen. Ein Kritikpunkt bildete die neue Regelung von § 2b IDG. Kritisch betrachtet wurde dabei deren systematische Einordnung. Der Beauftragte für den Datenschutz regte an, Abs. 1 sei im Anschluss an den bestehenden § 20 Abs. 3 IDG zu regeln. Mit Bezug auf § 2b Abs. 3 regte er eine Regelung unter dem Titel «VII. Beauftragte oder Beauftragter für Datenschutz» des Gesetzes über die Information und den Datenschutz an. Die Kritik ist zwar zum

Teil berechtigt und die Einordnung der Bestimmung befriedigt in der Tat nicht völlig. Allerdings führt eine Einordnung bei § 20 IDG zu neuen Unklarheiten. Die Sonderregelung der Rechte der betroffenen Personen und der Einsichtsrechte Dritter bei gerichtlichen Verfahren und Verfahren von Strafverfolgungsbehörden gemäss § 86 Abs. 1 lit. b und c GOG soll – wie unter bisherigem Recht – auch für abgeschlossene Verfahren gelten. Das Informationszugangsrecht richtet sich damit nicht nach dem Gesetz über die Information und den Datenschutz, weshalb sich eine Regelung unter dem Titel «IV. Informationszugangsrecht und weitere Rechtsansprüche» eben gerade nicht aufdrängt. Eine Regelung des neuen § 2b Abs. 3 im Titel VII ist nicht zielführend, da der Begriff «Aufsicht» im Zusammenhang mit der Beraterin oder dem Berater für den Datenschutz im Gesetz nicht vorkommt. Zudem ist in Betracht zu ziehen, dass sich im Bereich des Datenschutzrechts, wie vorn erwähnt, weiterer Handlungsbedarf abzeichnet. Die Frage der Einordnung kann dann nochmals eingehend geprüft werden.

Zudem kritisierte der Beauftragte für den Datenschutz die Ausnahmeregelung für den Kantonsrat in § 2a IDG, die er als nicht EU-konform erachtet. Diesbezüglich ist darauf hinzuweisen, dass sich im Entwurf zum Bundesgesetz über den Datenschutz ebenfalls eine Ausnahmebestimmung für die eidgenössischen Räte findet (Art. 2 Abs. 2 Bst. b E-DSG: «Es ist nicht anwendbar auf: … Personendaten, die von den eidgenössischen Räten und den parlamentarischen Kommissionen im Rahmen ihrer Beratungen bearbeitet werden»). Eine Anpassung von § 2a E-IDG, der § 2 Abs. 2 lit. b IDG übernimmt, drängt sich damit nicht auf.

D. Finanzielle Auswirkungen

Die zwingenden Änderungen des Gesetzes über die Information und den Datenschutz gestützt auf die geänderten internationalen Rahmenbedingungen (vorne B.) ziehen Kosten nach sich. Insbesondere die neu zu schaffende Möglichkeit der oder des Beauftragten für den Datenschutz, Verfügungen zu erlassen und vorsorgliche Massnahmen zu ergreifen, wird für diese oder diesen zu einem grösseren Mittelbedarf führen. Aber auch auf die Verwaltung kommen zusätzliche Pflichten zu, die zu – wenn auch wohl nur geringen – Mehrkosten führen werden. Es ist davon auszugehen, dass die grosse Mehrheit der Verwaltungseinheiten bereits heute über taugliche Organisationsvorschriften verfügt, ist dies doch für eine wirkungsorientierte Verwaltungsführung unerlässlich. Bezüglich der neu gesetzlich geregelten Pflichten im Bereich der Datenschutz-Folgenabschätzungen sollten auf die kantonale

Verwaltung keine zusätzlichen Kosten zukommen. Bereits heute ist bei den Unterlagen zur in der kantonalen Verwaltung verwendeten Projektmanagementmethode eine Checkliste zur Informationssicherheit und zum Datenschutz enthalten. Die neuen Pflichten im Bereich der Meldepflicht von Datenschutzverletzungen sollten wie erwähnt lediglich ausnahmsweise zum Tragen kommen, können aber zu erheblichen Kosten führen. Diese erscheinen allerdings im Sinne eines besseren Schutzes der Rechtsunterworfenen auch als gerechtfertigt. Dasselbe gilt für die künftige Pflicht, einen Vermerk bei Personendaten anzubringen, wenn sie bestritten sind und weder ihre Richtigkeit noch ihre Unrichtigkeit nachgewiesen werden kann. Diese Möglichkeit wird allenfalls eine Anpassung der bestehenden IT-Systeme bedingen. Der berechtigte Schutz der betroffenen Personen vor den Nachteilen nicht als richtig nachgewiesener Personendaten rechtfertigt diese Aufwendungen jedoch. Die entsprechenden Kosten können nicht abgeschätzt werden, sollten jedoch mit den bestehenden Mitteln abgedeckt werden können.

E. Regulierungsfolgeabschätzung

Da das Gesetz über die Information und den Datenschutz nur auf öffentliche Organe anwendbar ist, kann eine zusätzliche administrative Belastung der Unternehmen ausgeschlossen werden.

F. Bemerkungen zu den einzelnen Bestimmungen

1. Änderungen im Gesetz über die Information und den Datenschutz

§ 2. Geltungsbereich

Die Gerichte können gemäss den neuen europäischen Rechtsgrundlagen nicht mehr allgemein von der Geltung des Datenschutzrechts ausgenommen werden. Ausnahmen sind jedoch für die Verfahren sowie im Bereich der Aufsicht möglich. Die Ausnahme in § 1 Abs. 1 Satz 2 wird deshalb durch eine entsprechende Regelung in § 2b E-IDG ersetzt.

§ 2a. Ausnahmen a. Kantonsrat

Abs. 1: Die Regelung in § 2a E-IDG entspricht der bisherigen Regelung in § 2 Abs. 2 lit. b IDG. Auch im Bundesgesetz über den Datenschutz soll eine Ausnahme für das Parlament vorgesehen werden (Art. 2 Abs. 2 Bst. b E-DSG: «Personendaten, die von den eidgenössischen

Räten und den parlamentarischen Kommissionen im Rahmen ihrer Beratungen bearbeitet werden» und Art. 3 Abs. 2 Bst. a E-DSG: «Von der Aufsicht durch den Beauftragten sind ausgenommen: a. die Bundesversammlung»).

Die geltende Fassung, die seit dem 1. Januar 2015 in Kraft ist (Gesetz über die Stärkung der Informationsrechte der Aufsichtskommissionen vom 26. Mai 2014 [OS 69, 482; ABl 2014-01-10]) ist deshalb beizubehalten.

Abs. 2: Der Kantonsrat als Wahlbehörde der oder des Beauftragten für den Datenschutz soll von der Aufsicht durch diese bzw. diesen ausgenommen werden. Da die Aufsichtstätigkeit nicht allgemein geregelt ist, sind die Bestimmungen, die einen aufsichtsrechtlichen Inhalt aufweisen, an dieser Stelle aufzuzählen.

§ 2b. Gerichte und Strafverfolgungsbehörden

Vorbemerkungen

Mit Bezug auf die Unterstellung der Gerichte unter die Regeln des IDG ergibt sich mit den neuen europäischen Rechtsgrundlagen eine Änderung gegenüber der bisherigen Ausgangslage, indem für die Gerichte keine allgemeinen Ausnahmen vom Geltungsbereich mehr vorgesehen werden dürfen.

Das bedeutet aber keineswegs, dass die Prozessordnungen nicht mehr gelten: Sie behalten als bereichsspezifisches Datenschutzrecht (wie die anderen Spezialgesetze, z. B. das Polizeigesetz, das Schulgesetz oder das Bundesgesetz über den Allgemeinen Teil des Sozialversicherungsrechts) ohnehin weiter ihre Gültigkeit (vgl. dazu Beat Rudin, Überholte Ausnahmen beim Geltungsbereich, digma 2016, 122 ff.). Das heisst: Die Regelungen z. B. der Strafprozessordnung gelten weiterhin – zusätzlich sind aber auch die Grundsätze des (Informations- und) Datenschutzgesetzes anwendbar (z. B. die Regeln zur verantwortlichen Behörde, zur Informationssicherheit usw.).

Die folgenden zwei Bereiche sind zusätzlich zu regeln:

- Um Kollisionen zwischen den verfahrensrechtlichen und den datenschutzrechtlichen Informationsansprüchen der Parteien bzw. der betroffenen Personen zu vermeiden, muss vorgesehen werden, dass sich die Rechte und Ansprüche der betroffenen Personen und die Einsichtsrechte Dritter während hängiger und abgeschlossener Verfahren der Zivil- und Strafrechtspflege ausschliesslich nach dem anwendbaren Verfahrensrecht richten (Abs. 1).
- Ausserdem soll die Datenbearbeitung der Gerichte nicht der Aufsicht der oder des Datenschutzbeauftragten unterstehen (Abs. 3).

Abs. 1: Der Kanton Zürich regelt – anders als der Bund – den Datenschutz und den Umgang der öffentlichen Organe mit Informationen in einem gemeinsamen Erlass. Dies ist insofern von Bedeutung, als die Richtlinie (EU) 2016/680 und die Revision des Übereinkommens SEV 108 keinen Bezug zum Umgang mit Informationen haben. Soweit das IDG diesen Bereich regelt, was im vorliegenden Zusammenhang vorab im Zusammenhang mit den Einsichtsrechten Dritter von Bedeutung ist, kann dessen Geltung für Gerichtsverfahren auch weiterhin ohne Weiteres ausgenommen werden. Die Einsichtsrechte Dritter sollen sich nach wie vor nicht nach dem IDG, sondern nach den spezialgesetzlichen Regelungen richten. Zusätzlich sollen sich auch die Rechte der Parteien weiterhin nicht nach dem IDG richten und §§ 20–22 IDG sollen nicht anwendbar sein. Für den Bereich der Strafverfolgung ist dies gemäss der Richtlinie (EU) 2016/680 zulässig, da die Richtlinie die Mitgliedstaaten nicht daran hindert, nationale Vorschriften zu erlassen für die Bearbeitung personenbezogener Daten durch Gerichte und andere Justizbehörden. Soweit die Spezialgesetze keine Regelungen enthalten, gelten also insbesondere die Regelungen zur Bekanntgabe von Informationen (§§ 14 ff. IDG) auch für Gerichte und Strafverfolgungsbehörden.

Der Bund verwendet diesbezüglich den Begriff «Verfahrensrecht» (Art. 2 Abs. 3 E-DSG). Dieser Begriff scheint jedoch etwas zu kurz zu greifen, da die entsprechenden Bestimmungen nicht nur in den Verfahrensordnungen enthalten sind. Der in § 2b verwendete Begriff «Verfahren» umfasst sodann sowohl die laufenden als auch die abgeschlossenen Verfahren, was die Regelung auch von derjenigen für die Verwaltungs- und Verwaltungsjustizverfahren gemäss § 20 Abs. 3 unterscheidet.

Das Verfahren umfasst insbesondere auch den von den Jugendanwaltschaften angeordneten Vollzug. Ein allgemeiner Ausschluss der Anwendbarkeit des IDG auf den Bereich des Justizvollzugs ist demgegenüber nicht vorgesehen, weshalb sich beim Vollzug gegenüber Erwachsenen die Einsichtsrechte nach § 20 richten.

Abs. 2: Eine allgemeine Ausnahme vom IDG für die Gerichte ist nicht zulässig (vgl. dazu die Vorbemerkungen) und erscheint zudem auch nicht zielführend. Einerseits verweisen die massgebenden Verfahrensordnungen zum Teil ihrerseits wiederum auf die datenschutzrechtlichen Bestimmungen (z. B. Art. 99 Abs. 1 StPO), und anderseits enthalten sie zum Teil gar keine (Zivilprozessordnung) oder lediglich bruchstückhafte Regelungen (z. B. Art. 98 StPO). Enthalten Spezialgesetze eine Regelung, geht diese dem IDG jedoch vor. Das IDG ist also immer dann anwendbar, wenn die Spezialgesetze keine Regelungen enthalten. Falls dereinst datenschutzrechtliche Regeln allgemeiner Art in die Prozessgesetze eingefügt werden sollten, werden diese den Regelungen des IDG ohne Weiteres vorgehen.

Abs. 3: Es ist eine Regelung ins Gesetz aufzunehmen, die festhält, dass die oder der Datenschutzbeauftragte für die Gerichte, soweit sie dem IDG unterstehen, nicht zuständig ist, sondern diese die Aufsicht selbstständig regeln (vgl. Art. 3 Abs. 2 Bst. c E-DSG). Diese Ausnahme ist in Art. 30 der Richtlinie (EU) 2016/680 ausdrücklich vorgesehen und auch gestützt auf Art. 9 Abs. 1a E-SEV 108 zulässig. Festzuhalten ist, dass sich ein entsprechender Ausschluss für die Strafverfolgungsbehörden gemäss § 86 Abs. 1 lit. b und c GOG nicht rechtfertigt. Diese sind Verwaltungseinheiten, weshalb eine Unterstellung unter die Aufsicht der oder des Beauftragten für den Datenschutz angemessen erscheint.

Die Gerichte sind für die Einrichtung einer Aufsichtsinstanz in diesen Bereichen verantwortlich.

§ 2c. c. Teilnahme am wirtschaftlichen Wettbewerb

Bereits unter geltendem Recht galt das IDG nicht für das privatwirtschaftliche Handeln öffentlicher Organe. Soweit öffentliche Organe privatrechtlich handeln, sollen die Regeln des IDG weiterhin nicht gelten. Die Regelung des bisherigen Rechts in § 2 Abs. 2 lit. a wird deshalb unverändert übernommen. Allerdings müssen nach den neuen Vorgaben auch für sie – wie für Private, die dem Bundesgesetz über den Datenschutz unterstehen – Datenschutzregeln gelten. Es ist zulässig, die Regeln des Bundesgesetzes über den Datenschutz für privates Datenbearbeiten anwendbar zu erklären. Da solche kantonalen öffentlichen Organe jedoch öffentliche Organe bleiben und nicht Private werden, sondern nur wie Private handeln, bleibt – analog zur Regelung im Bund (Art. 23 Abs. 2 DSG und Art. 32 Abs. 2 E-DSG) – die kantonale Aufsichtsbehörde zuständig. Da es sich zudem um kantonale Organe handelt, sind die Bestimmungen des Bundesgesetzes über den Datenschutz sinngemäss anwendbar. Festzuhalten ist allerdings, dass sich die Regeln für privatrechtliche handelnde öffentliche Organe erst nach der Änderung des Bundesgesetzes über den Datenschutz ändern werden.

Damit die Regeln des geänderten Bundesgesetzes über den Datenschutz ohne weitere Änderung des kantonalen Rechts gelten, ist bei der Verweisung auf das Bundesgesetz über den Datenschutz ausnahmsweise auf ein Datum zu verzichten, mithin eine dynamische Verweisung einzufügen.

§ 3. Begriffe

Die Gliederung dieses Paragrafen soll übersichtlicher gestaltet werden. Damit das Zitieren der Bestimmungen einfacher wird, werden Absatznummerierungen eingefügt. Abs. 1 und 2 werden deshalb formell angepasst.

Abs. 3 (Personendaten): Anders als die internationalen Vorgaben (und die meisten europäischen Staaten) schützen die schweizerischen Datenschutzgesetze bisher nicht nur natürliche, sondern auch juristische Personen. Diese Besonderheit soll bei der Revision des DSG aufgegeben werden (Art. 2 Abs. 1 E-DSG). Die Kantone sind nicht verpflichtet, diese Anpassung nachzuvollziehen. Festzuhalten ist in diesem Zusammenhang, dass das Gesetz über die Information und den Datenschutz im Gegensatz zum DSG nur für die öffentlichen Organe gilt. Eine Aufhebung der Anwendbarkeit des IDG auf die Daten juristischer Personen hätte zur Folge, dass sämtliche Gesetzesgrundlagen, welche die Bearbeitung von Personendaten regeln, auf juristische Personen nicht mehr anwendbar wären und allenfalls angepasst werden müssten. Zudem unterstehen auch juristische Personen dem Schutz der Privatsphäre, auch wenn der Schutzgehalt gegenüber demjenigen natürlicher Personen eingeschränkt ist. Bei einer Beschränkung des Geltungsbereichs auf natürliche Personen müsste folglich einerseits bei sämtlichen Bestimmungen in der zürcherischen Gesetzessammlung, die sich auf «Personendaten» beziehen, überprüft werden, ob sie auch für Daten juristischer Personen gelten sollen, und anderseits müsste der Schutzbedarf für die Daten juristischer Personen festgelegt werden (vgl. Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, S. 33, und die entsprechende Regelung im Regierungs- und Verwaltungsorganisationsgesetz vom 21. März 1997 [RVOG; SR 172.010]). Auf eine entsprechende Einschränkung des Geltungsbereichs von Abs. 3 ist deshalb einstweilen zu verzichten.

Abs. 4: «Genetische Daten» sollen neu ausdrücklich in die Kategorie der besonders schützenswerten (besonderen) Personendaten fallen. Die Begriffsdefinition der «ethnischen Herkunft» enthält wohl im weitesten Sinn auch genetische Daten, dies insbesondere, da die Aufzählung in lit. a nicht abschliessend ist. Um Unklarheiten auszuräumen, erscheint eine Ergänzung in diesem Teilbereich jedoch sinnvoll.

Art. 3 Ziff. 4 der Richtlinie (EU) 2016/680 regelt neu das Profiling (als besondere, «gefährliche» Art des Bearbeitens von Personendaten), das denselben Anforderungen genügen muss wie das Bearbeiten von besonders schützenswerten Personendaten (also nur gestützt auf eine Grundlage in einem Gesetz im formellen Sinn). Dies muss auch in die kantonalen Gesetze übernommen werden. Im Interesse der einfachen Formulierung und Verständlichkeit ist «Profiling» in die Begriffsdefinitionen aufzunehmen. Wird das Profiling als zusätzliche Kategorie bei den besonderen Personendaten eingefügt, geltend die Anforderungen, die an die Bearbeitung von besonderen Personendaten gestellt werden, insbesondere § 8 Abs. 2, der eine hinreichend bestimmte Regelung in einem formellen Gesetz verlangt.

Die bereits im geltenden Recht enthaltene Erstellung von Persönlichkeitsprofilen (Abs. 4 lit. b) deckt nicht dasselbe ab und kann deshalb unverändert beibehalten werden.

Abs. 5 und 6 sind formell anzupassen.

§ 10. Datenschutz-Folgenabschätzung, Vorabkontrolle

Abs. 1: Art. 27 der Richtlinie (EU) 2016/680 und Art. 8bis Ziff. 2 E-SEV 108 verlangen eine Datenschutz-Folgenabschätzung durch das verantwortliche öffentliche Organ. Diese Abschätzung soll Folgendes enthalten:

– eine allgemeine Beschreibung der geplanten Bearbeitungsvorgänge,
– eine Bewertung der in Bezug auf die Grundrechte der betroffenen Personen bestehenden Risiken,
– eine Darstellung der Massnahmen, durch die der Schutz der Grundrechte der betroffenen Personen sichergestellt werden kann (insbesondere durch datenschutzfreundliche Voreinstellungen bei der Technikgestaltung).

Durch die Datenschutz-Folgenabschätzung schafft das verantwortliche öffentliche Organ auch die Voraussetzungen dafür, dass es den Nachweis der Einhaltung der Datenschutzvorschriften erbringen kann. Eine Abschätzung der Risiken einer geplanten Datenbearbeitung muss zwar in jedem Fall durchgeführt werden, was ohne Zweifel zu einem gewissen Aufwand bei jedem Datenbearbeitungsprojekt führen wird. Allerdings werden an diese Einschätzung keine übermässigen Anforderungen gestellt. Besteht bei einer geplanten Datenverarbeitung keine besondere Gefahr und folglich kein Bedarf nach besonderen Vorkehrungen, kann dies im Projekt mit einer Aktennotiz dokumentiert werden. Die Einzelheiten, etwa die Dokumentation in den Akten, können auf Verordnungsstufe festgelegt werden. Eine Risikoabschätzung im Sinne dieser Bestimmung ist zudem sinnvoll und muss notwendigerweise Teil jedes IT-Projekts sein. Wenn auch im Gesetz nicht ausdrücklich verlangt, musste eine derartige Abschätzung wohl auch nach geltendem Recht immer durchgeführt werden. Besondere Risiken verpflichteten bereits nach § 10 Abs. 1 zu einer Vorabkontrolle. Da aber besondere Risiken nur erkannt werden können, wenn eine Risikoeinschätzung der geplanten Datenbearbeitung durchgeführt wird, musste eine Risikoabschätzung wohl bereits unter geltendem Recht immer vorgenommen werden.

In diesem Zusammenhang ist zudem darauf hinzuweisen, dass die kantonale Verwaltung eine einheitliche Projektmanagementmethode verwendet (HERMES). Die im Rahmen dieser Methode zur Verfügung stehende Checkliste enthält auch die Frage nach dem «ISDS-Konzept». Dieses Konzept bildet die Grundlage für die Festlegung der Massnah-

men für die Informationssicherheit und den Datenschutz. Es zeigt die Restrisiken auf, die mit dem Betrieb des IT-Systems und der Organisation verbunden sind, und beschreibt das Notfallkonzept. Dies ist nichts anderes als eine Datenschutz-Folgenabschätzung.

Das mit der Bestimmung Verlangte ist deshalb weder grundsätzlich neu, noch werden übermässige Anforderungen gestellt. Vielmehr ist davon auszugehen, dass sämtliche öffentlichen Organe diese Anforderungen ohne erheblichen Mehraufwand erfüllen können.

Abs. 2: Die in Art. 28 Richtlinie (EU) 2016/680 verlangte Vorabkonsultation der oder des Datenschutzbeauftragten ist mit dem bisherigen § 10 ausreichend erfüllt, weshalb eine rein formale Anpassung erfolgt (Verweisung auf «Grundrechte» anstelle von «Rechte und Freiheiten» der betroffenen Person).

§ 12. Information über die Beschaffung

Abs. 1: Gestützt auf Art. 13 der Richtlinie (EU) 2016/680 müssen den betroffenen Personen bei der Bearbeitung von Personendaten gewisse Informationen «zur Verfügung gestellt werden». Die Bestimmung zielt auf eine aktive Informationspflicht des öffentlichen Organs, nicht aber auf den individuellen Zugang der Personen auf ihre Daten. Die gesetzliche Pflicht gemäss § 12 Abs. 2, die bis anhin lediglich für besondere Personendaten galt, ist somit auf sämtliche Personendaten auszuweiten. Festzuhalten ist, dass die Information nicht individuell erfolgen muss, sondern auch in allgemeiner Form, z.B. auf einer Website, erfolgen kann.

Abs. 2: Die Information über den Zweck der Bearbeitung, die nach geltendem Recht auf die besonderen Personendaten beschränkt waren, wird neu auf sämtliche Personendaten ausgedehnt. Zudem wird die Informationspflicht inhaltlich an die Vorgaben des EU-Rechts angeglichen. Angaben sind nötig über das verantwortliche öffentliche Organ (lit. a), die beschafften Daten oder deren Kategorien (lit. b), die Rechtsgrundlage und den Zweck der Bearbeitung (lit. c), die Empfänger der Daten oder die Kategorien von Empfängern, falls die Daten Dritten bekannt gegeben werden (lit. d), sowie die Rechte der betroffenen Personen (lit. e). Da bei den beschafften Daten und den Datenempfängern die Angabe von Kategorien genügt, wird die Handhabung der Bestimmung vereinfacht, können doch die Datenarten (z.B. Einbürgerungsdaten) bzw. die Empfänger (z.B. Verwaltungsstellen, die mit der Leistung persönlicher Hilfe befasst sind) zusammengefasst werden.

Abs. 3: Gestützt auf die Vorgaben in der Richtlinie (EU) 2016/680 sind Ausnahmen von der Informationspflicht möglich. Davon wird in Abs. 3 Gebrauch gemacht. Dabei ist festzuhalten, dass gemäss § 8 Abs. 1 die Bearbeitung und damit auch die Beschaffung von Personendaten

ohnehin nur zur Erfüllung einer gesetzlich umschriebenen Pflicht zulässig ist. In Anbetracht der Ausnahme in Abs. 3 lit. b sind folglich kaum Anwendungsbereiche für die neue Bestimmung ersichtlich, sie muss jedoch gleichwohl eingefügt werden, um der Richtlinie (EU) 2016/680 Genüge zu tun.

Gemäss lit. c soll, analog zur Regelung im Entwurf zum Bundesgesetz über den Datenschutz, auf Informationen verzichtet werden können, wenn eine Offenlegung unmöglich ist oder mit unverhältnismässigem Aufwand verbunden wäre (vgl. Art. 18 Abs. 2 E-DSG).

Die Information soll im gleichen Masse eingeschränkt werden können wie der Zugang zu den eigenen Personendaten gemäss § 23 (lit. d). Durch eine Verweisung ist diese Möglichkeit der Einschränkung sicherzustellen.

§ 12a. Meldepflicht

Abs. 1: Gestützt auf Art. 7 Ziff. 2 E-SEV 108 sowie auf Art. 30 und 31 der Richtlinie (EU) 2016/680 muss eine Meldepflicht bei Datenschutzverletzungen festgelegt werden. Wer innerhalb einer Organisationseinheit für die Erfüllung der Meldepflicht zuständig sein soll, ist von der Organisationseinheit gestützt auf § 1 Abs. 3 der Verordnung über die Information und den Datenschutz vom 28. Mai 2008 (IDV; LS 170.41) festzulegen.

Festzuhalten ist, dass diese Pflicht auch für die Bearbeitung im Auftrag gelten muss. Dieser Anforderung ist jedoch mit der Regelung in § 6 Genüge getan: da das öffentliche Organ verantwortlich bleibt, ist es auch für die Meldung bei unbefugter Datenbearbeitung verantwortlich. Dies setzt voraus, dass die Dritten gemäss § 6 die unbefugte Bearbeitung oder den Verlust von Informationen unverzüglich dem verantwortlichen öffentlichen Organ melden. Allfällige Ergänzungen können in § 25 IDV angebracht werden.

Abs. 2 und 3: Die betroffenen Personen müssen über Vorgänge gemäss Abs. 1 informiert werden. Allerdings ist auch diese Information ganz oder teilweise verzichtbar, wenn ein überwiegendes öffentliches oder privates Interesse entgegensteht.

§ 13. Einhaltung der Datenschutzbestimmungen und Qualitätssicherung

Abs. 1: Gemäss Art. 4 und 8 der Richtlinie (EU) 2016/680 muss in den Datenschutzvorschriften die Forderung nach der Nachweisbarkeit der Einhaltung der Datenschutzbestimmungen enthalten sein. Festzuhalten ist, dass dieser Nachweis insbesondere durch den Erlass geeigneter Organisationsvorschriften, Informationssicherheitsrichtlinien und Zugriffskonzepte erbracht werden soll. Die Anforderungen an die Um-

setzung (z. B. Detaillierungsgrad der Zugriffskonzepte) sollen dabei dem Risiko entsprechen, das mit einer Bearbeitung der betroffenen Personendaten verbunden ist. Die Anforderungen werden bei gewöhnlichen Personendaten weniger weit gehen als bei besonderen Personendaten. Festzuhalten ist, dass keine Verpflichtung der öffentlichen Organe besteht, zertifizierte Datenmanagementsysteme einzuführen. Damit fallen auch die Aufwendungen für die Umsetzung kaum ins Gewicht, ist doch der Erlass von Organisationsvorschriften, Informationssicherheitsrichtlinien und Zugriffskonzepten bereits heute üblich.

Der bisherige Abs. 1 ist lediglich formal anzupassen.

§ 21. Schutz eigener Personendaten

Der Vollständigkeit halber ist darauf hinzuweisen, dass Personendaten, die von öffentlichen Organen bearbeitet werden, richtig sein müssen. Dieser Anspruch (Art. 4 Abs. 1 Bst. d Richtlinie [EU] 2016/680 und Art. 5 Ziff. 4 Bst. d E-SEV 108) ist durch § 21 ausreichend abgedeckt. Die Regelung in § 21 umfasst auch weitere in der Richtlinie garantierte Ansprüche, wie den Anspruch auf Berichtigung unrichtiger Daten (Art. 12 und 16 Richtlinie [EU] 2016/680 und Art. 8 Ziff. 1 Bst. e E-SEV 108) und den Anspruch auf Unterlassung, Beseitigung und Feststellung unrichtiger Datenbearbeitung (Art. 54 Richtlinie [EU] 2016/680 und Art. 8 E-SEV 108). Auch die verlangte Kostenlosigkeit ist erfüllt, wäre doch die Auferlegung von Kosten nur denkbar mit einer gesetzlichen Grundlage. Zu ergänzen ist, dass das von der Richtlinie verlangte «Handeln innert angemessener Frist» ein genereller Grundsatz des Verwaltungsrechts ist, der gegebenenfalls mit einer Rechtsverweigerungsbeschwerde durchgesetzt werden kann.

Abs. 2: Unter Umständen kann der Nachweis der Richtigkeit oder der Unrichtigkeit aufgrund der Art der Daten gar nicht erbracht werden (z. B. bei Werturteilen oder bei Daten, die das öffentliche Organ von einem Dritten erhalten hat). In diesen Fällen bringt das öffentliche Organ auf Verlangen der betroffenen Person einen Bestreitungsvermerk an und schränkt die Bearbeitung der entsprechenden Personendaten ein. Eine Einschränkung könnte etwa darin bestehen, dass die Daten nur mit dem Bestreitungsvermerk weitergegeben werden dürfen.

Festzuhalten ist, dass dieses Recht der betroffenen Person während eines laufenden Strafverfahrens nicht zusteht, da die StPO die Rechte der betroffenen Personen abschliessend regelt (Art. 98 StPO).

§ 36. Empfehlungen

Abs. 2: Gestützt auf die Richtlinie (EU) 2016/680 und den Entwurf des Übereinkommens SEV 108 muss die oder der Beauftragte für den Datenschutz einschneidendere Kontrollbefugnisse haben als bis anhin. Das bisherige System mit einer Anfechtungsmöglichkeit von begründeten Ablehnungen des öffentlichen Organs durch die oder den Beauftragten für den Datenschutz ist deshalb nicht mehr ausreichend (vgl. neuen § 36a).

§ 36a. Verwaltungsmassnahmen

Abs. 1: Gestützt auf Art. 47 Abs. 2 Bst. b und c der Richtlinie (EU) 2016/680 und Art. 12bis Ziff. 2 Bst. c E-SEV 108 muss die oder Beauftragte für den Datenschutz bei Verstössen gegen das Datenschutzrecht verbindliche Anordnungen in Form einer Verfügung treffen können. Diese Verfügungsmöglichkeit muss ins IDG übernommen werden. Sie ist jedoch auf Fälle zu beschränken, bei denen eine erhebliche Verletzung von Bestimmungen über den Datenschutz vorliegen.

Auf das Verfahren sind die Bestimmungen des VRG anwendbar. Deshalb ist eine zusätzliche Regelung vorsorglicher Massnahmen im IDG nicht notwendig. Die Regelung von § 6 VRG gilt auch für von der oder dem Beauftragen für den Datenschutz erlassene Verfügungen.

Der Vollständigkeit halber ist festzuhalten, dass betroffene Personen, die sich gegen die Datenbearbeitung öffentlicher Organe zur Wehr setzen wollen, die Handlungen der öffentlichen Organe direkt anfechten können. Dazu steht ihnen der normale Rechtsmittelweg zur Verfügung. Die oder der Beauftragte für den Datenschutz ist an den entsprechenden Verfahren nicht beteiligt.

Abs. 2: Der vorliegende Rechtsmittelzug ans Verwaltungsgericht entspricht den Regelungen etwa in § 46 des Universitätsgesetzes vom 15. März 1998 (UniG; LS 415.11) oder in § 8a des EKZ-Gesetzes vom 19. Juni 1983 (LS 732.1).

2. Änderungen im Verwaltungsrechtspflegegesetz

§ 8. Akteneinsicht a. Grundsatz

Abs. 3: Gemäss dem Ingress der Akteneinsichtsverordnung der obersten Gerichte ist diese zwar auch auf das Baurekurs- und das Steuerrekursgericht anwendbar, eine ausdrückliche gesetzliche Grundlage für die entsprechende Verordnungskompetenz fehlt jedoch. Diese ist mit dem neuen Abs. 3 ausdrücklich vorzusehen.

3. Änderungen im Gesetz über die Gerichts- und Behördenorganisation im Zivil- und Strafprozess (GOG)

§ 88b. Datenschutzberatung

In den Bereichen der Strafverfolgung und des Strafvollzugs ist gestützt auf Art. 32 der Richtlinie (EU) 2016/680 ein «Datenschutzberater» einzusetzen. Die Richtlinie (EU) 2016/680 spricht diesbezüglich von «Datenschutzbeauftragtem». Dieser Begriff ist in der Schweiz und im Kanton Zürich jedoch bereits besetzt. Die Aufgaben, die in der Schweiz die oder der Datenschutzbeauftragte ausübt, werden in der Richtlinie (EU) 2016/680 der sogenannten Aufsichtsbehörde übertragen.

§ 151d. Akteneinsicht

Abs. 1: § 151d wurde ins GOG aufgenommen, um für die Akteneinsicht bei von den Strafuntersuchungsbehörden (Staatsanwaltschaften und Jugendanwaltschaften) abgeschlossenen Verfahren dieselben Regeln anwenden zu können wie für gerichtliche Verfahren. Für die Gerichte galten bis anhin die Regeln gemäss der Verordnung der obersten kantonalen Gerichte über die Information über Gerichtsverfahren und die Akteneinsicht bei Gerichten durch Dritte (Akteneinsichtsverordnung der obersten Gerichte; LS 211.15), die gestützt auf § 73 Abs. 1 lit. d GOG erlassen wurde. Die Akteneinsichtsverordnung wiederum verweist auf Art. 101 Abs. 3 und Art. 102 StPO bzw. Art. 15 JStPO, die sich mit der Einsicht in laufende Strafverfahren befassen und auf abgeschlossene Verfahren bis anhin analog angewendet wurden. Die gesetzliche Grundlage in § 151d GOG ist deshalb auch auf die Gerichtsverfahren auszudehnen.

Der Wortlaut von Abs. 1 lit. b entspricht Art. 101 Abs. 2 StPO sowie der bereits bestehenden Regelung für zivilprozessuale Verfahren in § 131 Abs. 1 GOG.

Abs. 2 entspricht der Regelung in Art. 101 Abs. 3 StPO sowie der bereits bestehenden Regelung für zivilprozessuale Verfahren in § 131 Abs. 3 GOG.

Die Einzelheiten des Akteneinsichtsrechts für die Gerichte soll der Plenarausschuss gestützt auf § 73 Abs. 1 lit. d GOG erlassen.

4. Änderungen im Straf- und Justizvollzugsgesetz

§ 18. Datenschutzberatung

Zur Begründung kann auf die Erläuterungen zu § 88b GOG verwiesen werden.

5. Änderungen im Polizeigesetz (PolG)

§ 52. Datenbearbeitung

In Abs. 2 dieser Bestimmung ist das Profiling zu ergänzen, das für die Polizeiarbeit unabdingbar ist. Eine ausdrückliche Verweisung auf die Bestimmung zum Profiling im Gesetz über die Information und den Datenschutz ist nicht notwendig, da sich dies bereits aus der systematischen Einordnung der Bestimmung im 7. Abschnitt (Information, Datenbearbeitung und Datenschutz) und insbesondere aus § 51 PolG ergibt.

In Abs. 4 wird zudem ergänzt, dass die Polizei Personendaten unter den Voraussetzungen von §§ 16 und 17 IDG «von Amtes wegen oder auf Ersuchen im Einzelfall» bekannt geben kann. Dabei handelt es sich nicht um eine Neuerung. Es handelt sich vielmehr um eine Verdeutlichung eines Grundsatzes, der für alle öffentlichen Organe Geltung hat.

§ 54c. Datenschutzberatung

Abs. 1: Auch für diese Bestimmung kann auf die Erläuterungen zu § 88b GOG verwiesen werden. Festzuhalten ist, dass grundsätzlich jede Polizei eine eigene für die Datenschutzberatung zuständige Person bezeichnet.

Abs. 3: Es soll möglich sein, dass die für die Datenschutzberatung zuständige Person einer kommunalen Polizei diese Aufgaben auch für andere kommunale Polizeien übernimmt. Damit könnten kleinere Polizeien die Aufgaben gemeinsam erfüllen bzw. an eine grössere Polizei abtreten.

Im Namen des Regierungsrates

Der Präsident:	Die Staatsschreiberin:
Thomas Heiniger	Kathrin Arioli