Nachtrag zum Datenschutzgesetz

Botschaft und Entwurf der Regierung vom 9. Oktober 2018

Inhaltsverzeichnis

Zusammenfassung

Am 27. April 2016 beschlossen das Europäische Parlament und der Rat der Europäischen Union eine Reform der bestehenden Datenschutzgesetzgebung und verabschiedeten u.a. die Richtlinie (EU) 2016/680. Diese Richtlinie stellt für die Schweiz eine Weiterentwicklung des Schengen-Besitzstands dar. Aufgrund des Schengen-Assoziierungsabkommens ist die Schweiz verpflichtet, das Schengen-Recht der Europäischen Union (EU) zu übernehmen und in innerstaatliches Recht umzusetzen. Auch der Europarat hat das bestehende Übereinkommen im Bereich Datenschutz revidiert.

Auf Bundesebene wird dementsprechend das Bundesgesetz über den Datenschutz überarbeitet und dem übergeordneten Recht angepasst. Der Vorentwurf zum Bundesgesetz über den Datenschutz befand sich bis 4. April 2017 in der Vernehmlassung. Am 15. September 2017 veröffentlichte der Bundesrat Botschaft und Entwurf eines revidierten Bundesgesetzes über den Datenschutz. Soweit diese Revision für die Übernahme der Richtlinie (EU) 2016/680 erforderlich ist, stimmte die Bundesversammlung der Vorlage in der Schlussabstimmung vom 28. September 2018 zu. Die weiteren Bestimmungen stehen noch in der parlamentarischen Beratung. Für den Kanton St.Gallen ergibt sich aufgrund der Richtlinie (EU) 2016/680 ebenfalls gesetzgeberischer Handlungsbedarf. Das bestehende kantonale Datenschutzgesetz ist entsprechend den übergeordneten Vorgaben anzupassen. Aufgrund der komplexen Thematik und der Tatsache, dass das übergeordnete Recht einen straffen Zeitplan für die Umsetzung vorgibt, ist diese anspruchsvolle Gesetzesrevision im Kanton St.Gallen frühzeitig an die Hand genommen worden.

Beim vorliegenden Gesetzesentwurf handelt es sich um eine vorwiegend technische Umsetzung. Der Datenschutz erfährt durch verschiedene neue Instrumente eine – durch übergeordnetes Recht vorgegebene – Aufwertung. Zudem werden die kantonale Fachstelle für Datenschutz sowie die Gemeindefachstellen für Datenschutz funktional und institutionell an die übergeordneten Vorgaben angepasst. Sie erhalten eine stärkere Überprüfungsbefugnis und erfahren dadurch eine Stärkung ihrer Position. Die kantonale Fachstelle für Datenschutz kann nicht nur wie bisher Massnahmen beantragen, sondern neu auch selbst Verfügungen erlassen. Als Rechtsmittelinstanz ist die Verwaltungsrekurskommission vorgesehen.

Frau Präsidentin
Sehr geehrte Damen und Herren

Wir unterbreiten Ihnen mit dieser Vorlage Botschaft und Entwurf des Nachtrags zum Datenschutzgesetz.

1 Ausgangslage

1.1 Entwicklungen in Europa

1.1.1 Europäische Union

Die Europäische Union (EU) verabschiedete in den letzten Jahrzehnten mehrere Erlasse zum Schutz von Personendaten. Der wichtigste Erlass war die Richtlinie 95/46/EG vom 24. Oktober 1995[1] zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. Diese Richtlinie wurde ergänzt durch den Rahmenbeschluss 2008/977/JI[2] vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden.

Am 27. April 2016 verabschiedeten das Europäische Parlament und der Rat der Europäischen Union eine umfassende Reform der Datenschutzgesetzgebung. Dabei handelte es sich einerseits um die Verordnung (EU) 2016/679[3] zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, welche die Richtlinie 95/46/EG ersetzt. Anderseits wurde die Richtlinie (EU) 2016/680[4] 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 verabschiedet, die den Rahmenbeschluss 2008/977/JI ersetzt[5].

Aufgrund des Abkommens vom 26. Oktober 2004 zwischen der Schweizerischen Eidgenossenschaft, der Europäischen Union und der Europäischen Gemeinschaft über die Assoziierung dieses Staates bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands (nachfolgend Schengen-Assoziierungsabkommen[6]) muss die Schweiz die Richtlinie (EU) 2016/680, die Bestandteil des Schengen-Besitzstands ist, umsetzen. Hingegen ist die Schweiz nicht verpflichtet, die Verordnung (EU) 2016/679 in das Landesrecht zu übernehmen, da es sich dabei gemäss der Europäischen Union nicht um eine Weiterentwicklung des Schengen-Besitzstands handelt.

1.1.2 Europarat

Der Europarat als eigene und nicht der EU zugehörige Organisation hat sich ebenfalls mit der Thematik Datenschutz befasst. Am 28. Januar 1981 verabschiedete der Europarat den ersten völkerrechtlichen Vertrag im Bereich des Datenschutzes. Es handelt sich dabei um das Übereinkommen vom 28. Januar 1981[7] zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (nachfolgend «Übereinkommen SEV 108» oder «E-Konv 108»), das

1 ABl. L 281 vom 23. November 1995, S. 31.

2 ABl. L 350 vom 30. Dezember 2008, S. 60.

3 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), ABl. L 119 vom 4. Mai 2016, S. 1.

4 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 und zur Aufhebung des Rahmenbeschlusses 2008/977 /JI des Rates, ABl. L 119 vom 4. Mai 2016, S. 89.

5 Nach Art. 59 RL 2016/680 wird der Rahmenbeschluss 2008/977/JI mit Wirkung vom 6. Mai 2018 aufgehoben.

6 SR 0.362.31.

7 SR 0.235.1.

von der Schweiz am 2. Oktober 1997 ratifiziert wurde. Dieses ist der wichtigste völkerrechtlich bindende Vertrag zum Schutz des Einzelnen vor Missbrauch bei der elektronischen Verarbeitung personenbezogener Daten.

Im Jahr 2011 leitete der Europarat ein Verfahren zur Revision des Übereinkommens SEV 108 ein. Damit sollen die Herausforderungen für den Schutz der Privatsphäre und der Grundrechte der betroffenen Personen, welche die Globalisierung, die technologischen Entwicklungen und die Zunahme des grenzüberschreitenden Datenverkehrs mit sich bringen, besser bewältigt werden können. Unter schweizerischer Leitung hat der beratende Ausschuss des Übereinkommens SEV 108 einen Entwurf zur Revision des Übereinkommens SEV 108 erarbeitet. Die Arbeiten wurden im Juni 2016 abgeschlossen. Der Inhalt entspricht grösstenteils dem erwähnten Reformvorhaben der Europäischen Union (vgl. Abschnitt 1.1.1), ist aber weniger detailliert als Letzteres. Der Bund sieht vor, die Anforderungen der Richtlinie (EU) 2016/680 sowie des Entwurfs zur Revision des Übereinkommens SEV 108 im Rahmen desselben Gesetzgebungsverfahrens umzusetzen. Das Übereinkommen SEV 108 gilt auch für die Kantone.

1.2 Entwicklungen in der Schweiz

1.2.1 Totalrevision des Bundesgesetzes über den Datenschutz

Auf Bundesebene ist der Datenschutz im Bundesgesetz vom 19. Juni 1992 über den Datenschutz (SR 235.1; im Folgenden CH-DSG) geregelt, das am 1. Juli 1993 in Kraft getreten ist. Das CH-DSG gilt für das Bearbeiten von Daten natürlicher und juristischer Personen durch private Personen und Bundesorgane (vgl. Art. 2 CH-DSG). Das Bundesgesetz ist daher für die Rechtsunterworfenen besonders wichtig. Das kantonale Datenschutzgesetz hingegen regelt im Wesentlichen die Bearbeitung von Personendaten durch Kanton und Gemeinden (siehe im Folgenden Abschnitt 1.3).

In den Jahren 2010 und 2011 wurde das Bundesgesetz über den Datenschutz einer Evaluation[8] unterzogen. Daraus ergab sich ein Bedürfnis nach Aktualisierung des CH-DSG aufgrund der technologischen und gesellschaftlichen Entwicklungen, da das Gesetz teilweise nicht mehr ausreiche, um einen genügenden Schutz zu gewährleisten. Die Wirksamkeit des CH-DSG sollte deshalb verbessert werden. Ausgehend von den Schlussfolgerungen seines Berichts vom 9. Dezember 2011[9] beauftragte der Bundesrat das Eidgenössische Justiz- und Polizeidepartement (EJPD), gesetzgeberische Massnahmen zur Stärkung des Datenschutzes zu prüfen, mit denen den neuen Gefahren für die Privatsphäre Rechnung getragen werden könne. Am 1. April 2015 beauftragte der Bundesrat das EJPD, zusammen mit dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten, dem Eidgenössischen Departement für Wirtschaft, Bildung und Forschung (WBF), dem Eidgenössischen Finanzdepartement (EFD) und dem Eidgenössischen Departement des Innern (EDI) einen Vorentwurf für das Gesetz zu erarbeiten und dabei die Schlussfolgerungen des Berichts und die Entwicklungen im Europarat und in der Europäischen Union zu berücksichtigen.

8 Büro Vatter / Institut für Europarecht, Evaluation des Bundesgesetzes über den Datenschutz – Schlussbericht, Bern, 10. März 2011, https://www.bj.admin.ch/dam/data/bj/staat/evaluation/schlussber-datenschutzeval-d.pdf.

9 Bericht des Bundesrates vom 9. Dezember 2011 über die Evaluation des Bundesgesetzes über den Datenschutz, BBl 2012, 335.

1.2.2 Entwurf für eine Totalrevision des Bundesgesetzes über den Datenschutz

Der Vorentwurf für eine Totalrevision des Bundesgesetzes über den Datenschutz befand sich bis 4. April 2017 in der Vernehmlassung. Aufgrund der Vernehmlassungsergebnisse wurde der Vorentwurf in einigen Punkten angepasst.[10] Am 15. September 2017 verabschiedete der Bundesrat schliesslich Botschaft und Entwurf über die Totalrevision des Bundesgesetzes über den Datenschutz.[11] Aufgrund des engen Sachzusammenhangs zu dieser Vorlage werden die wichtigsten Punkte im Folgenden kurz vorgestellt.

Im Entwurf wird die Systematik des Gesetzes überarbeitet und es werden einige Ausnahmen vom Geltungsbereich angepasst. Die Definition des «Profiling» wird an das europäische Recht angeglichen und zudem wird eine klärende Definition für die Verletzung der Datensicherheit eingefügt. Weiter werden einzelne Bestimmungen angepasst bzw. präzisiert, so beispielsweise die Bestimmungen zur Datensicherheit, zur Verletzung der Datensicherheit, zur Regelung der Bekanntgabe von Personendaten, zur Informationspflicht und deren Ausnahmen sowie zum Auskunftsrecht.

Betreffend den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (Beauftragter) sieht der Entwurf ebenfalls gewisse Änderungen vor. Anders als im Vorentwurf, wonach der Beauftragte im Fall einer Verletzung der Datenschutzvorschriften entscheiden konnte, ob er eine Untersuchung einleitet oder nicht, ist er nach dem Entwurf nun dazu verpflichtet. Er kann nur dann von der Eröffnung einer Untersuchung absehen, wenn die Verletzung der Datenschutzvorschriften von geringfügiger Bedeutung ist. Der Katalog der Verwaltungsmassnahmen, die der Beauftragte anordnen kann, wird zudem ergänzt, wobei die Verfügungskompetenzen des Beauftragten durch diese Änderung nicht erweitert werden. Es wird lediglich präzisiert, dass der Beauftragte verfügen kann, dass der Verantwortliche bestimmte Pflichten, wie die Informations- oder Meldepflichten, beachtet. Schliesslich erhält der Beauftragte im Vergleich zum Vorentwurf neu die Kompetenz, unter bestimmten Voraussetzungen eine Verwarnung auszusprechen.

Weiter werden im Entwurf gewisse Änderungen am System der strafrechtlichen Sanktionen vorgenommen. So wird die Bussenobergrenze auf Fr. 250'000.– festgesetzt. Die Liste der strafbaren Verhaltensweisen wird gekürzt und konzentriert sich nun auf die Verletzung wesentlicher Pflichten des Verantwortlichen. Die Verletzung der beruflichen Schweigepflicht ist wieder als Übertretung ausgestaltet und die Bekanntgabe von Daten, die zu kommerziellen Zwecken bearbeitet wurden, wird darin nicht mehr erfasst. Um der fehlenden direkten Strafbarkeit des Unternehmens entgegenzuwirken, schlägt der Bundesrat vor, die strafrechtliche Verantwortlichkeit der leitenden Organe zu verschärfen. Zudem sieht er die Einführung einer Strafe wegen Missachtens von Verfügungen des Beauftragten vor, die es erleichtert, die leitende Person innerhalb des Unternehmens zu identifizieren und zu verurteilen, die für die Einhaltung der Verfügung verantwortlich war.

1.2.3 Schengen-Besitzstand

Für die Schweiz stellt ausschliesslich die Richtlinie (EU) 2016/680 eine Weiterentwicklung des Schengen-Besitzstands dar. Gemäss dem Schengen-Assoziierungsabkommen ist die Schweiz verpflichtet, die Anforderungen dieses Erlasses innerhalb von zwei Jahren ab der Notifikation durch die Europäische Union, die am 1. August 2016 erfolgt ist, in ihrer innerstaatlichen Rechtsordnung umzusetzen. Die Schengen-Assoziierung der Schweiz ist auch für die Kantone verbindlich. Die Bestimmungen der Richtlinie (EU) 2016/680 müssen daher unter Einhaltung der verfassungsmässigen Kompetenzverteilung in nationales Recht übertragen werden. Wie bereits er-

10 Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, Ziff. 1.6.2.1, BBl 2017, 6978 ff.

11 BBl 2017, 6941 ff.

wähnt, ist die Schweiz hingegen nicht verpflichtet, die Verordnung (EU) 2016/679 in das Landesrecht zu übernehmen, da es sich dabei gemäss der Europäischen Union nicht um eine Weiterentwicklung des Schengen-Besitzstands handelt (vgl. Abschnitt 1.1.1).

Im Rahmen der Schengen-Evaluation überprüft die Europäische Union regelmässig die Schengen-Staaten und damit auch die Schweiz darauf, ob diese ihren Verpflichtungen nachkommen. Die letzte Schengen-Evaluation der Schweiz fand im ersten Halbjahr 2014 statt. Am 11. September 2014 hat der Rat der Europäischen Union den Bericht des Evaluationsausschusses zum Datenschutz in der Schweiz genehmigt. Demnach erfüllte damals die schweizerische Gesetzgebung im Bereich des Datenschutzes die Anforderungen des Schengen-Besitzstands bis zur nächsten Evaluation.

1.2.4 Angemessenheitsbeschluss

In allen internationalen Bereichen, die nicht der Schengen-Zusammenarbeit unterstehen, gilt die Schweiz als Drittstaat. Zwischen einem Drittstaat und den Mitgliedstaaten der Europäischen Union durften nach EU-Recht Daten nur ausgetauscht werden, wenn der Drittstaat ein angemessenes Schutzniveau nach der Richtlinie 95/46/EG gewährleistete. Dieses Schutzniveau wird durch die Europäische Kommission periodisch überprüft und in einem sogenannten Angemessenheitsbeschluss festgehalten. Wie unter Abschnitt 1.1.1 erwähnt, wurde im April 2016 die Richtlinie 95/46/EG durch die Verordnung (EU) 2016/679 ersetzt. Somit wird die schweizerische Gesetzgebung künftig anhand der in der Verordnung (EU) 2016/679 enthaltenen Anforderungen überprüft. Falls die Schweiz den Angemessenheitsbeschluss beibehalten bzw. im Fall eines Widerrufs erneut eine Bestätigung über das angemessene Datenschutzniveau erhalten möchte, ist es wichtig, dass die schweizerische Gesetzgebung einen den Anforderungen dieser Verordnung entsprechenden Schutz gewährleistet. Insbesondere die Schweizer Wirtschaft ist auf diesen Angemessenheitsbeschluss angewiesen. Zu diesem Zweck wird das Datenschutzgesetz des Bundes an die Verordnung (EU) 2016/679 angenähert, ohne dass diese jedoch vollständig umgesetzt wird. Dasselbe gilt auch für den Kanton St.Gallen.

1.2.5 Gestaffelte Beschlussfassung der Bundesversammlung

Nationalrat und Ständerat haben beschlossen, die vom Bundesrat vorgelegte Totalrevision des CH-DSG (Vorlage 17.059) aufzuteilen und jene Bereiche vorzuziehen, die zur Umsetzung der übergeordneten Richtlinie (EU) 2016/680 erforderlich sind. Dem entsprechenden Bundesgesetz – das ein neues Schengen-Datenschutzgesetz[12] und Anpassungen an verschiedenen Bundesgesetzen umfasst – sowie dem Bundesbeschluss zur Übernahme der Richtlinie (EU) 2016/680 haben die eidgenössischen Räte in den Schlussabstimmungen vom 28. September 2018 mit deutlicher Mehrheit (Nationalrat) bzw. einstimmig (Ständerat) zugestimmt. Die übrigen Teile der vom Bundesrat vorgelegten Totalrevision des CH-DSG werden derzeit noch von der Staatspolitischen Kommission des Nationalrates (Erstrat) vorberaten.

1.3 Situation im Kanton St.Gallen

Im Kanton St.Gallen ist der Datenschutz im Datenschutzgesetz vom 20. Januar 2009 (sGS 142.1; abgekürzt DSG) geregelt, das am 25. November 2008 vom Kantonsrat erlassen und nach unbenützter Referendumsfrist am 20. Januar 2009 rechtsgültig wurde. Das DSG ist seit 1. Januar 2009 in Vollzug für den Kanton und die selbständigen öffentlich-rechtlichen Anstalten des Kantons sowie seit 1. Januar 2010 für Gemeinden, selbständige öffentlich-rechtliche Gemeindeunternehmen sowie Gemeindeverbände und Zweckverbände.

12 Bundesgesetz vom 28. September 2018 über den Datenschutz im Rahmen der Anwendung des Schengen-Besitzstands in Strafsachen (Schengen-Datenschutzgesetz; abgekürzt SDSG); Referendumsvorlage: BBl 2018, 6003 ff.

Wie bereits ausgeführt, ergibt sich aufgrund des Erlasses der Richtlinie (EU) 2016/680 in der Europäischen Union für den Kanton St.Gallen gesetzgeberischer Handlungsbedarf, da diese Richtlinie Bestandteil des Schengen-Besitzstands ist. Die Schengen-Assoziierung der Schweiz ist für die Kantone verbindlich. Daher müssen die Bestimmungen der Richtlinie (EU) 2016/680 in nationales Recht übertragen werden. Entsprechend ist es notwendig, das kantonale Datenschutzgesetz in Teilen zu revidieren, um den Anforderungen der Richtlinie (EU) 2016/680 bzw. des Schengen-Besitzstands zu genügen und auch die bundesrechtlichen Vorgaben einzuhalten. Da im Übrigen die Verordnung (EU) 2016/679 und die Richtlinie (EU) 2016/680 die gleichen allgemeinen Grundsätze enthalten (vgl. Abschnitt 3.1), wird das DSG analog zum Bund ebenfalls an die Verordnung (EU) 2016/679 angenähert. Weil sodann auch das Abkommen SEV 108 für die Kantone verbindlich ist (vgl. Abschnitt 1.1.2), ist vorgesehen, dieses Übereinkommen im Rahmen der vorliegenden Teilrevision ebenfalls umzusetzen.

Die Änderungen in der vorliegenden Teilrevision des Datenschutzgesetzes sind auf diese Anforderungen ausgerichtet. Als Ausgangspunkt diente der Leitfaden der Konferenz der Kantonsregierungen (KdK) vom 2. Februar 2017 (nachfolgend Leitfaden der KdK), der den Anpassungsbedarf bei den kantonalen Datenschutzgesetzen aufgrund der EU-Datenschutzreform und der Modernisierung des Übereinkommens SEV 108 behandelt und speziell für die Umsetzung dieser Reformen in den Kantonen erarbeitet wurde. Bei der Erarbeitung des vorliegenden Gesetzesentwurfs wurde darauf geachtet, die Vorgaben des übergeordneten Rechts umzusetzen und dabei auf einen ressourcenmässig kostspieligen weiteren Ausbau des Datenschutzes zu verzichten. Dies erachtet die Regierung auch nicht für nötig, zumal das EU-Recht einen bemerkenswert hohen Datenschutzstandard aufweist.

Wie im Abschnitt 1.2.3 ausgeführt, gilt für den Kanton St.Gallen eine Frist von zwei Jahren für die Umsetzung der Richtlinie (EU) 2016/680 in das kantonale DSG. Aus diesem Grund muss die vorliegende Gesetzesrevision umgehend an die Hand genommen werden. Eine Sistierung – wie in der Vernehmlassung mehrfach vorgeschlagen wurde – ist ausgeschlossen.

2 Datenschutz als Persönlichkeitsschutz

Im Sinn einer Vorbemerkung ist festzuhalten, dass der Datenschutz – anders als es der Name vielleicht vermuten lässt – nicht Daten schützen will, sondern die Persönlichkeitsrechte von Personen, deren Daten bearbeitet werden.[13] Im Datenschutzgesetz des Bundes wird entsprechend festgehalten, dass dieses Gesetz den Schutz der Persönlichkeit und der Grundrechte von Personen bezweckt, über die Daten bearbeitet werden (Art. 1 CH-DSG). Bestimmungen zum Persönlichkeitsschutz finden sich weiter auch in Art. 10 und 13 der Bundesverfassung (SR 101; abgekürzt BV) sowie in Art. 27 ff. des Schweizerischen Zivilgesetzbuches (SR 210; abgekürzt ZGB).

Obwohl die vorliegende Teilrevision des DSG in erster Linie der Umsetzung der erwähnten übergeordneten Rechtsgrundlagen dient, trägt sie mit Blick auf die Herausforderungen der Zukunft auch der Modernisierung und den Anforderungen des immer wichtiger werdenden Persönlichkeitsschutzes Rechnung.

3 Inhaltlicher Handlungsbedarf

3.1 Aufbau und Inhalt der Richtlinie (EU) 2016/680

Die Richtlinie (EU) 2016/680 ist als rechtstechnisches Dokument aufzufassen, das einheitliche Regeln für die verschiedenen Schengen-Mitglieder mit unterschiedlicher Rechtstradition aufstellt

13 Vgl. dazu Maurer-Lambrou / Kunz, in: Basler Kommentar zum Datenschutzgesetz, Art. 1 N 3.

und den Sachverhalt – anders als im schweizerischen Recht üblich – umfassend und detailliert regelt. Nachfolgend wird daher die Richtlinie (EU) 2016/680 vorgestellt und ihr Aufbau und wesentlicher Inhalt dargelegt.[14]

Die Richtlinie (EU) 2016/680 ist darauf ausgerichtet, natürliche Personen bei der Verarbeitung personenbezogener Daten zu schützen, die zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung bearbeitet werden. Die Richtlinie soll ein hohes Schutzniveau gewährleisten und den Austausch personenbezogener Daten zwischen den zuständigen Behörden der verschiedenen Schengen-Staaten erleichtern. Der Wortlaut der Richtlinie ist auf die Verordnung (EU) 2016/679 abgestimmt, wodurch die gleichen allgemeinen Grundsätze zur Anwendung gelangen.

Die Richtlinie (EU) 2016/680 umfasst 65 Artikel, die in 10 Kapitel eingeteilt sind. Kapitel I mit der Überschrift «Allgemeine Bestimmungen» enthält den Gegenstand und die Ziele der Richtlinie, den Anwendungsbereich und die Begriffsbestimmungen.

Kapitel II der Richtlinie (EU) 2016/680 statuiert verschiedene Grundsatzbestimmungen. Art. 4 legt u.a. fest, dass personenbezogene Daten für einen festgelegten Zweck zu erheben sind und nur zu diesem Zweck bearbeitet werden dürfen. Die Daten sind durch geeignete technische und organisatorische Massnahmen vor unbefugter oder unrechtmässiger Bearbeitung sowie vor Verlust, Zerstörung oder Beschädigung zu schützen. Zudem sind nach Art. 5 für die Löschung personenbezogener Daten angemessene Fristen vorzusehen. Art. 8 regelt die Rechtmässigkeit der Bearbeitung, was bedeutet, dass Datenbearbeitungen im Wesentlichen auf einer gesetzlichen Grundlage beruhen müssen. Art. 10 enthält Grundsätze für die Bearbeitung besonderer Kategorien personenbezogener Daten, wie beispielsweise für ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, genetische oder biometrische Daten oder Gesundheitsdaten.

In Kapitel III der Richtlinie (EU) 2016/680 sind die Rechte der betroffenen Person geregelt. In Art. 13 wird festgehalten, welche Informationen der betroffenen Person zur Verfügung zu stellen sind. Art. 14 regelt das Auskunftsrecht. Eine betroffene Person hat das Recht, Aufschluss darüber zu erhalten, ob Daten über sie bearbeitet werden, und gegebenenfalls gewisse weitere Auskünfte zu erhalten. Dieses Recht kann aus verschiedenen Gründen ganz oder teilweise eingeschränkt werden (Art. 15). Weiter hat eine betroffene Person das Recht, die Berichtigung von unrichtigen Daten oder in gewissen Fällen die Löschung der Daten zu verlangen (Art. 16). Schliesslich sieht Art. 17 vor, dass die betroffene Person in bestimmten Fällen die Möglichkeit haben muss, ihre Rechte über eine Aufsichtsbehörde auszuüben.

Kapitel IV der Richtlinie (EU) 2016/680 regelt die Pflichten des Verantwortlichen (d.h. des öffentlichen Organs, das die Personendaten bearbeitet) und des Auftragsverarbeiters. In den Art. 19 und 20 wird festgelegt, dass der Verantwortliche geeignete technische und organisatorische Massnahmen umsetzen muss, um nachweisen zu können, dass eine Datenbearbeitung in Übereinstimmung mit den Vorgaben der Richtlinie (EU) 2016/680 erfolgt. Der Verantwortliche hat zudem angemessene technische und organisatorische Massnahmen zu treffen, um Datenschutzgrundsätze wirksam umzusetzen. Weiter legt die Richtlinie (EU) 2016/680 in Art. 22 Regeln für eine Datenbearbeitung im Auftrag fest. Wird eine Drittperson mit einer Datenbearbeitung beauftragt, ist sicherzustellen, dass der Auftragsverarbeiter hinreichende Garantien dafür bietet, dass die Bearbeitung im Einklang mit den Anforderungen der Richtlinie (EU) 2016/680 erfolgt. Ausserdem sind die Verantwortlichen nach Art. 27 verpflichtet, in bestimmten Fällen eine Datenschutz-Folgenabschätzung durchzuführen. Art. 28 enthält das Instrument der Vorabkonsultation, bei dem bestimmten Vorhaben der Aufsichtsbehörde vorab zur Konsultation vorzulegen sind. Sowohl die

14 Vgl. dazu Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, Ziff. 2.1.2, BBl 2017, 6989 ff.

Datenschutz-Folgenabschätzung als auch die Vorabkonsultation gehören zu den zentralen Neuerungen in dieser Gesetzesrevision und weisen eine beachtliche Relevanz auf. Die Art. 30 und 31 der Richtlinie (EU) 2016/680 verpflichten den Verantwortlichen schliesslich, in gewissen Fällen der Aufsichtsbehörde eine Datenschutzverletzung zu melden und gegebenenfalls die betroffene Person zu benachrichtigen.

Das Kapitel V der Richtlinie (EU) 2016/680 regelt die Übermittlung von Daten an Drittländer oder internationale Organisationen. Art. 36 regelt die Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses. Personenbezogene Daten dürfen an ein Drittland übermittelt werden, wenn dieses ein angemessenes Schutzniveau bietet.

Kapitel VI der Richtlinie (EU) 2016/680 regelt die Unabhängigkeit der Aufsichtsbehörden (Art. 41 bis 44) sowie deren Zuständigkeiten, Aufgaben und Befugnisse (Art. 45 bis 49). Die Schengen-Staaten sind verpflichtet, im Bereich des Datenschutzes unabhängige Aufsichtsbehörden einzusetzen (Art. 41 und 42). Art. 43 regelt die allgemeinen Bedingungen für die Mitglieder der Aufsichtsbehörde. Dabei muss jedes Mitglied über die für die Erfüllung der Aufgaben und Ausübung der Befugnisse erforderliche Qualifikation, Erfahrung und Sachkunde insbesondere im Bereich des Schutzes personenbezogener Daten verfügen. Art. 44 regelt die Errichtung der Aufsichtsbehörde und legt u.a. eine bestimmte Amtszeit für deren Mitglieder fest. Als Aufgaben der Aufsichtsbehörde werden beispielsweise genannt (Art. 46):
– Sensibilisierung der Verantwortlichen und Auftragsverarbeiter für die Pflichten, die sich aus der Richtlinie (EU) 2016/680 ergeben;
– Beratung über legislative und administrative Massnahmen;
– Information der betroffenen Personen auf Antrag über ihre Rechte und Befassung mit Beschwerden;
– Untersuchung über die Anwendung der Richtlinie (EU) 2016/680 und Durchsetzung der Vorschriften;
– Kenntnis des aktuellen Stands der Entwicklungen im Bereich Informations- und Kommunikationstechnologie;
– Zusammenarbeit mit anderen Aufsichtsbehörden.

Weiter verpflichtet Art. 47 Abs. 1 die Schengen-Staaten, vorzusehen, dass die Aufsichtsbehörde über wirksame Untersuchungsbefugnisse verfügt. Nach Abs. 2 muss die Aufsichtsbehörde auch über wirksame Abhilfebefugnisse verfügen, wie beispielsweise die Möglichkeit der Verwarnung eines Verantwortlichen oder eines Auftragsverarbeiters, der Anordnung von vorschriftsgemässen Verarbeitungen sowie der Verhängung einer vorübergehenden oder endgültigen Beschränkung der Verarbeitung, einschliesslich eines Verbots.

Kapitel VII der Richtlinie (EU) 2016/680 regelt die Zusammenarbeit unter den Behörden (Art. 50 bis 51) und Kapitel VIII der Richtlinie (EU) 2016/680 die Rechtsbehelfe, die Haftung und die Sanktionen (Art. 52 bis 57). Art. 52 und 53 sehen vor, dass die betroffene Person das Recht auf Beschwerde bei einer Aufsichtsbehörde sowie das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen einen sie betreffenden Entscheid der Aufsichtsbehörde hat. Nach Art. 55 können sich die betroffenen Personen unter bestimmten Umständen vertreten lassen. Die Kapitel IX und X der Richtlinie enthalten verschiedene Schlussbestimmungen.

Diese sehr umfassende Richtlinie (EU) 2016/680 muss nun in nationales Recht, d.h. auf Bundesebene in das Bundesgesetz über den Datenschutz und im Kanton St.Gallen in das kantonale Datenschutzgesetz, übertragen werden. Aufgrund des hohen Regelungsgehalts in der Richtlinie (EU) 2016/680 wird das kantonale Datenschutzgesetz im Rahmen der vorliegenden Teilrevision – die wie bereits erwähnt nur eine Minimalumsetzung der Schengen-Vorgaben darstellt – zwangsläufig mit relativ detaillierten Bestimmungen angefüllt. Von den oben erwähnten Kapiteln der Richtlinie (EU) 2016/680 sind dabei insbesondere die Kapitel II bis IV und VI von Bedeutung.

Nachfolgend werden die verschiedenen Änderungen, die aufgrund der Richtlinie (EU) 2016/680 im kantonalen Datenschutzgesetz notwendig werden, kurz skizziert.

3.2 Umsetzung der Richtlinie (EU) 2016/680 im kantonalen Datenschutzgesetz

In Art. 1 DSG werden aufgrund der Vorgaben der Richtlinie (EU) 2016/680 mehrere neue Begriffsdefinitionen eingefügt bzw. bestehende Definitionen leicht abgeändert. Neu werden beispielsweise die Begriffe «ethnische Zugehörigkeit», «genetische Daten» und «biometrische Daten» bei den besonders schützenswerten Personendaten eingeführt und der englische Ausdruck «Profile» geregelt, der aus Gründen der rechtstechnischen Eindeutigkeit verwendet werden soll (vgl. Art. 1 Abs. 1 Bst. b und d^{bis} DSG). In Art. 2 DSG wird zudem der Geltungsbereich des Gesetzes angepasst.

Der Inhalt von Art. 4 der Richtlinie (EU) 2016/680, der die Grundsätze in Bezug auf die Verarbeitung personenbezogener Daten regelt – wie beispielsweise, dass Daten nur für einen bestimmten Zweck, rechtmässig und nach dem Grundsatz von Treu und Glauben bearbeitet werden dürfen und die Bearbeitung verhältnismässig sein muss –, ist im Wesentlichen bereits im kantonalen Datenschutzgesetz enthalten.

Aufgrund der Richtlinie (EU) 2016/680 sind zwei neue Instrumente zu schaffen, die in die neuen Art. 8a und 8b DSG aufgenommen werden. Art. 8a DSG regelt die sogenannte Datenschutz-Folgenabschätzung nach Art. 27 der Richtlinie (EU) 2016/680. Dabei sind vorfrageweise datenschutzrechtliche Abklärungen mit Unterstützung der Fachstelle für Datenschutz durchzuführen, wenn konkrete Anhaltspunkte vorliegen, welche die Annahme rechtfertigen, dass der Datenschutz durch neue Verwaltungsprozesse (wie Gesetzgebungsarbeiten oder EDV-Projekte) in unzulässiger Weise beeinträchtigt werden könnte (vgl. Abschnitt 4.2.2 und neuen Art. 8a DSG). Art. 8b DSG regelt die Vorabkonsultation nach Art. 28 der Richtlinie (EU) 2016/680. Dabei sind bestimmte Vorhaben (wie Rechtsetzungsprojekte oder bestimmte Bearbeitungen von Personendaten) vorab der Fachstelle für Datenschutz zur Durchführung einer Konsultation vorzulegen (vgl. Abschnitt 4.2.3).

Die bestehende Regelung für Datenbearbeitung durch Dritte (Art. 9 DSG) wird aufgrund von Art. 22 f. die Richtlinie (EU) 2016/680 leicht angepasst. So wird beispielsweise neu festgehalten, dass die Weiterübertragung einer Datenbearbeitung der vorgängigen schriftlichen Zustimmung des auftraggebenden öffentlichen Organs bedarf. Weiter werden aufgrund der Richtlinie (EU) 2016/680 die Rechte von betroffenen Personen im DSG ausgebaut. Für öffentliche Organe besteht neu eine Informationspflicht (mit gewissen Ausnahmen) bei der Beschaffung von Personendaten.

Funktionale und institutionelle Neuerungen gibt es aufgrund der Richtlinie (EU) 2016/680 für die Fachstellen für Datenschutz. Dabei sind insbesondere die Art. 42 bis 44, 46, 47 und 52 der Richtlinie (EU) 2016/680 von Bedeutung. So erhalten die Fachstellen für Datenschutz eine stärkere Überprüfungsbefugnis und dadurch eine Stärkung ihrer Position. Die Fachstellen für Datenschutz müssen neu ihre Aufsicht- und Schutzfunktion aktiver und stärker wahrnehmen sowie sich vermehrt in Verwaltungsverfahren einbringen. Dies ist beispielsweise bei der Vorabkonsultation (Art. 8b DSG) der Fall, bei der u.a. Rechtsetzungsprojekte, die den Datenschutz betreffen, vorab der Fachstelle für Datenschutz zu einer Vorabkonsultation vorzulegen sind. Die Fachstellen für Datenschutz haben somit eine gewichtige Rolle bei Rechtsetzungsprojekten. Sie werden von Beginn an in den Prozess miteinbezogen, um die datenschutzrechtlichen Aspekte frühzeitig zu prüfen. Für die Vorabkonsultation bestehen konkrete Fristen für die Fachstellen für Datenschutz, die sich ebenfalls aus der Richtlinie (EU) 2016/680 ergeben. Die kantonale Fachstelle für Datenschutz

kann zudem nicht nur wie bisher Massnahmen beantragen, sondern neu auch selbst Verfügungen erlassen (Art. 35a DSG). Die kantonale Fachstelle für Datenschutz erhält somit eine viel stärker juristisch ausgerichtete Aufgabe. Bezüglich des Rechtsschutzes ist vorgesehen, dass Verfügungen der kantonalen Fachstelle für Datenschutz an die Verwaltungsrekurskommission weitergezogen werden können (Art. 35a DSG, Art. 41 Bst. j des Gesetzes über die Verwaltungsrechtspflege [sGS 951.1; abgekürzt VRP]).

Betreffend die Fachstellen für Datenschutz kann somit festgehalten werden, dass sie aufgrund der Richtlinie (EU) 2016/680 eine bedeutend gewichtigere Position erhalten und bei verschiedenen Projekten mit Bezug zum Datenschutz frühzeitig miteinbezogen werden müssen.

3.3 Vernehmlassungsverfahren

Das Sicherheits- und Justizdepartement unterstellte Bericht und Entwurf für einen Nachtrag zum DSG vom 19. März bis 15. Juni 2018 einem breit angelegten Vernehmlassungsverfahren. Insgesamt wurden knapp 30 Stellungnahmen von politischen Parteien, Gemeinden, Verbänden, Gerichten, Departementen und der Staatskanzlei eingereicht. Die Vernehmlassungsvorlage wurde grundsätzlich begrüsst, gleichzeitig aber auch kritisch betrachtet. Die einzelnen Rückmeldungen wurden – soweit sinnvoll und aufgrund des übergeordneten Rechts umsetzbar – berücksichtigt und in Botschaft und Entwurf eingebaut bzw. ergänzt. Hierauf wird jeweils bei den Erläuterungen zu den einzelnen Bestimmungen hingewiesen.

4 Bemerkungen zu den einzelnen Bestimmungen

4.1 Allgemeine Bestimmungen

Art. 1 enthält die für das Datenschutzrecht relevanten Begriffe in Gestalt von Legaldefinitionen, die zu aktualisieren oder zu ergänzen sind. Dabei geht es wie bisher um die Abgrenzung der datenschutzrechtlich verwendeten Begriffe vom allgemeinen Sprachgebrauch und um die Vermeidung von Unklarheiten. Neu wird in Art. 1 Abs. 1 Bst. a festgehalten, dass sich der Begriff Personendaten nur noch auf Angaben beschränkt, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen. Anders als die internationalen Vorgaben (und diejenigen der meisten europäischen Staaten) schützen die schweizerischen Datenschutzgesetze bisher nicht nur natürliche, sondern auch juristische Personen. Der Bund sieht vor, diese schweizerische Spezialität bei der Revision des eidgenössischen Erlasses aufzugeben. Entsprechend ist kein Grund mehr gegeben, weshalb dieses gesetzliche Unikum im ohnehin eingeschränkten Anwendungsbereich des kantonalen DSG beibehalten werden soll. Es erscheint sinnvoll, diese Materie gleich wie im Bund zu regeln. Zum Begriff «Personendaten» ist festzuhalten, dass dieser als Oberbegriff auch besonders schützenswerte Personendaten, Persönlichkeitsprofile und Profiles umfasst.

In *Art. 1 Abs. 1 Bst. a^{bis}* wird aus systematischen Gründen eine Definition für den Begriff «Daten» eingefügt. Dieser wird verstanden als alle Angaben, die auf einem Datenträger abgelegt sind. Darunter fallen Personendaten und andere Informationen, die nur mittelbar datenschutzrechtliche Relevanz aufweisen.

In *Art. 1 Abs. 1 Bst. b Ziff. 2* soll auf den bisher verwendeten Begriff «Rassenzugehörigkeit» verzichtet werden. Neu wird an dessen Stelle der Begriff «ethnische Zugehörigkeit» verwendet. Modernere Gesetze sprechen von «Angaben über die Ethnie» bzw. «ethnische Zugehörigkeit/Herkunft». Damit gemeint ist die Zugehörigkeit zu einer Gruppe von Menschen, die sich aufgrund ihrer Kultur, Geschichte, Sprache, Sitten, Traditionen und Gebräuche als untereinander verbunden und dadurch als von der übrigen Bevölkerung differente Gemeinschaft erleben und/oder von der übrigen Bevölkerung als differente Gruppe wahrgenommen werden.

Art. 1 Abs. 1 Bst. b Ziff. 2bis hält neu ausdrücklich fest, dass genetische Daten zu den besonders schützenswerten Personendaten zählen. Die Begriffsdefinition ergibt sich aus dem Bundesgesetz über genetische Untersuchungen beim Menschen (SR 810.12). Zudem werden neu in *Art. 1 Abs. 1 Bst. b Ziff. 2ter* auch biometrische Daten ausdrücklich zu den besonders schützenswerten Personendaten gezählt. Diese Begriffsdefinition wurde inhaltlich aus der Richtlinie (EU) 2016/680 übernommen.

In *Art. 1 Abs. 1 Bst. c* werden die juristischen Personen sowie die Personengemeinschaften analog zum Bundesrecht neu von der Begriffsdefinition ausgenommen. Der Bund führt in der Botschaft[15] über die Totalrevision des CH-DSG aus, dass in den datenschutzrechtlichen Bestimmungen der Europäischen Union und des Europarates sowie der meisten ausländischen Rechtsordnungen kein Schutz für juristische Personen vorgesehen ist. Der Schutz von Daten juristischer Personen ist nur von geringer praktischer Bedeutung. Wenn er aufgehoben wird, sollte dies keine negativen Auswirkungen haben, insbesondere mit Blick auf den Schutz, der durch andere spezifische Gesetze gewährleistet wird (Persönlichkeitsschutz, unlauterer Wettbewerb, Urheberrecht).

Art. 1 Abs. 1 Bst. dbis führt den Begriff des «Profiles» (englischer Begriff) im DSG ein. Aufgrund des übergeordneten Rechts[16] ist die Auswertung von Daten, um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen, insbesondere bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, Intimsphäre oder Mobilität, in das DSG aufzunehmen. Diese Formulierung entspricht im Wesentlichen dem heute insbesondere in der Technik und im EDV-Bereich weit verbreiteten englischen Begriff «Profiling». Der Begriff «Profiling» wird im DSG jedoch nicht verwendet. Das «Profile» in Art. 1 Abs. 1 Bst. dbis wird verstanden als die Erkenntnisse, die sich aus Daten ergeben, die ausgewertet werden, um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen, insbesondere bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, Intimsphäre oder Mobilität. Dabei wird der Begriff «Daten» verwendet, da die Auswertung nicht auf Personendaten beschränkt ist.

Der Begriff «Profile» muss vom Begriff «Persönlichkeitsprofil» unterschieden werden. Im DSG war bisher nur der Begriff «Persönlichkeitsprofil» enthalten. Ein Persönlichkeitsprofil wird verstanden als eine Zusammenstellung von Personendaten, welche die Beurteilung der Persönlichkeit einer natürlichen Person erlaubt (Art. 1 Abs. 1 Bst. d DSG). Das Profile und das Persönlichkeitsprofil sind keineswegs identische Begriffe, weshalb sie beide im DSG getrennt voneinander bestehen können und müssen. Der Bund schlägt im Rahmen des Entwurfs über die Totalrevision des CH-DSG vor, das bisherige Persönlichkeitsprofil aufzuheben[17], weil es nicht mehr gebraucht wird und dafür den Begriff «Profiling» zu verwenden. Dies erscheint nicht zweckmässig, weil für beide Begriffe je getrennte Anwendungsfälle bestehen. Daher ist die Regierung der Ansicht, dass es sich rechtfertigt, den Begriff «Persönlichkeitsprofil» beizubehalten. Somit enthält das DSG nun einerseits das bisherige «Persönlichkeitsprofil» und führt den neuen Begriff «Profile» als eigenständigen Begriff ein. Die Gefahr, dass der qualitativ wesentliche Unterschied[18] zwischen den beiden Begriffen in der Praxis nicht richtig wahrgenommen wird, sollte unbedingt vermieden werden. Nachfolgend werden die verschiedenen Begriffe tabellarisch dargestellt.

---

15 Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, Ziff. 9.1.2, BBl 2017, 7010 ff.

16 Art. 3 Ziff. 4 RL 2016/680.

17 Vgl. Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, Ziff. 9.1.3.1, BBl 2017, 7019 ff.

18 Vgl. Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, Ziff. 9.1.3.1, BBl 2017, 7021.

Begriff	Definition	Erläuterung
Persönlichkeitsprofil	Zusammenstellung von Personendaten, welche die Beurteilung der Persönlichkeit einer natürlichen Person erlaubt (Art. 1 Abs. 1 Bst. d DSG).	Begriff war bisher bereits im DSG enthalten und wird auch mit der vorliegenden Teilrevision beibehalten.
Profiling	Die Bewertung bestimmter Merkmale einer Person auf der Grundlage von automatisiert bearbeiteten Personendaten, insbesondere um die Arbeitsleistung, die wirtschaftlichen Verhältnisse, die Gesundheit, das Verhalten, die Vorlieben, den Aufenthaltsort oder die Mobilität zu analysieren oder vorherzusagen (vgl. Art. 3 Abs. 1 Bst. b SDSG).	Der Begriff «Profiling» wird im DSG nicht verwendet (vgl. auch unten). Der Bund schlägt vor, den Begriff des Persönlichkeitsprofils aufzuheben und dafür den Begriff «Profiling» zu verwenden. Dies scheint nicht zweckmässig, da für beide Begriffe je getrennte Anwendungsfälle bestehen (vgl. Definition).
Profile	Erkenntnisse, die sich aus der Auswertung von Daten ergeben, um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen, insbesondere bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, Intimsphäre oder Mobilität (Art. 1 Abs. 1 Bst. d^{bis} DSG).	Während das «Profiling» als eine Tätigkeit verstanden werden kann, regelt das DSG das «Profile» als die Erkenntnisse, die sich aus der Auswertung ergeben (vgl. Definition).

Das Bearbeiten von Personendaten wird in *Art. 1 Abs. 1 Bst. e* präzisiert. Dabei wird die beispielhafte Aufzählung leicht erweitert. Unter Bearbeitung wird jeder Umgang mit Personendaten verstanden und umfasst neu auch die Umarbeitung, Archivierung, Löschung von Personendaten sowie die Durchführung logischer oder rechnerischer Operationen mit diesen Personendaten. Bezüglich der Begriffe «Löschung» und «Vernichtung» ist festzuhalten, dass «Vernichten» wie bisher das endgültige, physische Zerstören meint. Eine «Löschung» kann hingegen teilweise oder vollständig durch technische oder naturwissenschaftliche Vorgänge rückgängig gemacht werden. Diese Ergänzung der Definition wird vorgenommen, weil das übergeordnete Recht[19] sie vorsieht und vermutlich alle Kantone diese Ergänzung übernehmen werden.[20] Dadurch können unnötige Abgrenzungsfragen vermieden werden.

In *Art. 1 Abs. 1 Bst. e^{bis}* wird der Begriff der «Datenschutzverletzung» eingeführt. Diese wird definiert als unrechtmässige Bearbeitung von Daten, so dass bearbeitete Personendaten vernichtet werden oder verloren gehen, unbeabsichtigt oder unrechtmässig verändert oder offenbart werden oder dass Unbefugte Zugang zu solchen Personendaten erhalten.

Der Geltungsbereich nach *Art. 2* bleibt im Wesentlichen unverändert. In *Abs. 1* wird festgehalten, dass der Erlass jegliche Bearbeitung von Personendaten durch öffentliche Organe regelt, d.h. unabhängig davon, ob eine Person sich in einem Verfahren befindet oder nicht und auch unabhängig davon, welche Mittel angewendet werden. Das DSG ist somit nur auf die Bearbeitung von Personendaten anwendbar. Dazu ist anzumerken, dass das Profile (vgl. Art. 1 Abs. 1 Bst. d^{bis}) die Auswertung auch anderer Daten umfassen kann. Da das Profile jedoch persönliche Merkmale oder Entwicklungen abzeichnet, stellt es inhaltlich immer eine Auswertung von Personendaten dar und wird dementsprechend als Personendaten behandelt.

19 Art. 3 Ziff. 2 RL 2016/680.

20 Vgl. Leitfaden der KdK (S. 5).

Abs. 2 Bst. a bleibt unverändert. Anzumerken ist, dass, soweit ein öffentliches Organ am wirtschaftlichen Wettbewerb teilnimmt und dabei privatrechtlich handelt, die entsprechenden Regeln des Bundesgesetzes über den Datenschutz anwendbar sind. Für die datenschutzrechtliche Aufsicht über ein öffentliches Organ, das am wirtschaftlichen Wettbewerb teilnimmt und dabei nicht hoheitlich handelt, bleibt allerdings die kantonale Fachstelle für Datenschutz zuständig. Diese Zuständigkeit ergibt sich deshalb, weil kantonale öffentliche Organe, die privatrechtlich handeln, sich rechtlich nicht zu Privatpersonen wandeln, sondern nur wie private Akteure handeln.

Die Formulierung von *Art. 2 Abs. 2 Bst. b* soll unverändert bleiben. Bezüglich des «ausschliesslich persönlichen Gebrauchs» ist ergänzend anzumerken, dass damit handschriftliche oder elektronische Notizen gemeint sind, die ausschliesslich der betroffenen Person als Gedankenstütze für die Erstellung von Verfahrensakten dienen.

Art. 2 Abs. 2 Bst. c sah bisher eine generelle Ausnahme vom Geltungsbereich des DSG für hängige Verfahren der Zivil-, der Straf- und der gerichtlichen Verwaltungsrechtspflege sowie in hängigen Rechtshilfeverfahren vor. Aufgrund der übergeordneten Vorgaben[21] ist diese generelle Ausnahme vom Geltungsbereich nicht mehr zulässig. Das heisst, dass sowohl die Prozessordnungen (als bereichsspezifisches Datenschutzrecht) als auch die Grundsätze des Datenschutzgesetzes gleichzeitig gültig sind. In den Prozessgesetzen sind spezifische datenschutzrechtliche Bestimmungen enthalten, so dass diese vorgehen. Bei einer Lücke gelangt das DSG (als lex generalis) zur Anwendung. Beispielsweise finden die Regelungen der Schweizerischen Strafprozessordnung (SR 312.0) weiterhin Anwendung – aber auch die Grundsätze des Datenschutzgesetzes (z.B. die Regeln zur verantwortlichen Behörde oder zur Informationssicherheit). Dabei sollten jedoch Kollisionen zwischen den verfahrensrechtlichen und den datenschutzrechtlichen Informationsansprüchen der Parteien oder der betroffenen Personen vermieden werden. Deshalb wird neu vorgesehen, dass sich die Rechte und Ansprüche der betroffenen Personen während hängigen Verfahren der Zivil- und Strafrechtspflege sowie der Verwaltungsgerichtsbarkeit ausschliesslich nach dem anwendbaren Verfahrensrecht richten. Beispielsweise können die Parteien in dieser Phase nur ihr verfahrensrechtliches Akteneinsichtsrecht geltend machen, nicht aber ihr datenschutzrechtliches Recht auf Auskunft. Demgemäss wird in *Art. 2 ein neuer Abs. 3* eingefügt, der bestimmt, dass in hängigen Verfahren der Zivil-, der Straf- und der gerichtlichen Verwaltungsrechtspflege sowie in hängigen Rechtshilfeverfahren die Rechte und Ansprüche der betroffenen Person sich nach dem jeweiligen Verfahrensrecht richten. Mit der Formulierung «Verfahren der Strafrechtspflege» wird neben dem Verfahren vor dem Strafgericht auch die Strafuntersuchung durch die Staatsanwaltschaft erfasst. Somit gilt von der Eröffnung eines Verfahrens bis zur rechtlichen Erledigung (z.B. durch Entscheid, Abschreibung, Nichteintretensentscheid) das entsprechende Verfahrensrecht. Davor und danach gilt das DSG. Der Vorteil dieser Konstruktion ist, dass der Datenschutz in allen Bereichen lückenlos geregelt wird.

4.2 Bearbeitung von Personendaten

4.2.1 Bearbeitung von Personendaten im Allgemeinen

Art. 3 bleibt im Wesentlichen unverändert. Neu wird aufgrund der Vorgaben des übergeordneten Rechts[22] zusätzlich ein dritter Absatz eingefügt, der besagt, dass das öffentliche Organ für die Einhaltung der Datenschutzbestimmungen beweispflichtig ist.

Dieser Nachweis kann beispielsweise durch eine Zertifizierung mit sogenannten ISO-Standards erbracht werden. Wird darauf verzichtet, ist festzulegen, welche Dokumente notwendig sind, um den Nachweis erbringen zu können. Beispiele dafür sind ein Informationssicherheitskonzept oder

21 Art. 2 RL 2016/680; Art. 3 E-Konv 108.

22 Art. 4 Abs. 4 RL 2016/680; Art. 8bis Ziff. 1 E-Konv 108.

ein Zugriffskonzept. Bei fachlichen Fragen wird sich das öffentliche Organ sinnvollerweise an eine Fachstelle für Datenschutz wenden, die wie bisher in Anwendung von Art. 30 Abs. 1 Bst. b DSG beratend unterstützt.

Die Richtlinie (EU) 2016/680 sieht vor, dass die Grundsätze von Treu und Glauben und der Verhältnismässigkeit einzufügen sind. Nach dem übergeordneten Recht hat eine Bearbeitung immer nach Treu und Glauben[23] zu erfolgen und muss verhältnismässig[24] sein. Die Verhältnismässigkeit beinhaltet zudem eine zeitliche Komponente, d.h. eine Bearbeitung darf nicht länger dauern, als es zur Zweckerreichung erforderlich ist. Die beiden Grundsätze Treu und Glauben sowie Verhältnismässigkeit sind in Art. 5 der Bundesverfassung (SR 101) sowie Art. 8 der Kantonsverfassung (sGS 111.1) enthalten. Sie sind in der Schweizer Rechtstradition verankert und gelten für jegliches staatliche Handeln. Eine Wiederholung im Datenschutzgesetz ist somit nicht notwendig.

Art. 5: In Abs. 2 werden auch für die Profile dieselben Anforderungen wie für die Bearbeitung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen vorausgesetzt.

4.2.2 Datenschutz-Folgenabschätzung

Art. 8a (neu): Inskünftig verlangt das übergeordnete Recht[25] eine sogenannte Datenschutz-Folgenabschätzung durch das öffentliche Organ bei Gefahr für eine Datenschutzverletzung. Das heisst, dass beim Vorliegen konkreter Anhaltspunkte, die den Datenschutz durch neue Verwaltungsprozesse (z.B. umfangreiche Gesetzgebungsarbeiten, EDV-Projekte mit sensiblen Personendaten etc.) in unzulässiger Weise beeinträchtigen könnten, vorfrageweise datenschutzrechtliche Abklärungen durchzuführen sind (sogenannte Datenschutz-Folgenabschätzung). Die Fachstellen für Datenschutz haben dabei eine unterstützende Rolle.

Eine Datenschutz-Folgenabschätzung enthält wenigstens eine allgemeine Beschreibung der geplanten Bearbeitungsvorgänge, eine Bewertung der in Bezug auf Grundrechte von betroffenen Personen bestehenden Risiken sowie eine Darstellung und Bewertung der geplanten Abhilfemassnahmen. Als Abhilfemassnahmen sind beispielsweise Garantien oder Sicherheitsvorkehren zu verstehen, durch die der Schutz der Grundrechte der möglichen betroffenen Personen sichergestellt wird. Es handelt sich dabei um ein formalisiertes Vorbereitungsverfahren des öffentlichen Organs, damit dieses zu einem späteren Zeitpunkt die Voraussetzungen für den Nachweis der Einhaltung der Datenschutzvorschriften schnell und effizient erbringen kann.

Stellt das öffentliche Organ bei der Datenschutz-Folgenabschätzung ein datenschutzrechtliches Problem fest, ist eine Vorabkonsultation (siehe Abschnitt 4.2.3 und Art. 8b) durchzuführen. Stellt das öffentliche Organ nach der Datenschutz-Folgenabschätzung hingegen fest, dass keine datenschutzrechtlichen Probleme bestehen (d.h. dass keine Personendaten in unzulässiger Weise bearbeitet werden), ist das Vorgehen für das öffentliche Organ abgeschlossen. Die Unterlagen über die Datenschutz-Folgenabschätzung sind in jedem Fall vom öffentlichen Organ aufzubewahren, um allenfalls zu einem späteren Zeitpunkt den Nachweis der Einhaltung der Datenschutzvorschriften erbringen zu können.

Anzumerken ist, dass in diesem Erlass der unbestimmte Rechtsbegriff «Gefahr für eine Datenschutzverletzung» verwendet werden muss, weil eine scharfe Normierung der entsprechenden Fälle abschliessend nicht möglich ist. Der Begriff «Gefahr für eine Datenschutzverletzung» soll grundsätzlich auf objektive Gesichtspunkte abstellen. Die Praxis wird den Begriff mitzugestalten haben. Kriterien für eine «Gefahr für eine Datenschutzverletzung» können beispielsweise die An-

---

23 Art. 4 Abs. 1 Bst. a RL 2016/680; Art. 5 Ziff. 4 Bst. a E-Konv 108.

24 Art. 4 Abs. 1 Bst. c RL 2016/680; Art. 5 Ziff. 1 und Art. 5 Ziff. 4 Bst. c E-Konv 108.

25 Art. 27 RL 2016/680; Art. 8bis Ziff. 2 E-Konv 108.

zahl oder die Sensibilität der Personendaten darstellen. Zudem ist an dieser Stelle auf die Definition der Datenschutzverletzung zu verweisen (Art. 1 Abs. 1 Bst. e^{bis} DSG). Dieser zufolge ist eine Datenschutzverletzung zu verstehen als eine unrechtmässige Verwendung von Daten, so dass bearbeitete Personendaten vernichtet werden oder verloren gehen, unbeabsichtigt oder unrechtmässig verändert oder offenbart werden oder Unbefugte Zugang zu solchen Personendaten erhalten.

4.2.3 Vorabkonsultation

Art. 8b (neu): Im Rahmen der Anpassung des Datenschutzgesetzes an das übergeordnete Recht[26] wird ein neuer Artikel betreffend die Vorabkonsultation eingefügt. Die Vorgaben der Richtlinie (EU) 2016/680 führen dazu, dass bestimmte Vorhaben vorab einer Fachstelle für Datenschutz zur Durchführung einer Konsultation vorzulegen sind. Es handelt sich dabei um zwei verschiedene Konstellationen (Bst. a und b):

– *Rechtsetzungsprojekte, die den Datenschutz betreffen* (Bst. a): Durch die Vorabkonsultation soll insbesondere bei Rechtsetzungsvorhaben dafür gesorgt werden, dass die datenschutzrechtlichen Vorgaben berücksichtigt werden.
– *Vorhaben zur Bearbeitung von Personendaten, die zu einer Gefahr für eine Datenschutzverletzung für betroffene Personen führen* (Bst. b): Darunter werden alle Arten von Grundrechtsverletzungen der betroffenen Personen verstanden. Wie bereits unter Abschnitt 4.2.2 erwähnt, muss das öffentliche Organ, wenn es bei der Datenschutz-Folgenabschätzung ein datenschutzrechtliches Problem feststellt, das Vorhaben einer Fachstelle für Datenschutz zur Vorabkonsultation vorlegen. Ebenfalls müssen nach Bst. b Vorhaben zur Bearbeitung von Personendaten, die neue Technologien, Mechanismen oder Verfahren verwenden und zu einer Gefahr für Datenschutzverletzungen führen, einer Fachstelle für Datenschutz zur Vorabkonsultation vorgelegt werden.[27]

Das Konzept der datenschutzrechtlichen Vorabkonsultation sieht vor, dass sich eine Fachstelle für Datenschutz bereits von Beginn an mit der datenschutzrechtlichen Problematik eines entsprechenden Projekts auseinandersetzen und aufgrund ihres datenschutzrechtlichen Fachwissens und ihrer Erfahrung die entsprechenden Punkte (Bearbeitungsvorgänge) zusammenstellen kann, die einer besonderen datenschutzrechtlichen Betrachtung bedürfen (Abs. 3) und die ihr vorab zur Konsultation vorzulegen sind. Das öffentliche Organ hat diese Punkte zu beantworten. Diese Angaben dienen als Ausgangslage für die weitere Projektarbeit und stellen sicher, dass heikle datenschutzrechtliche Konstellationen bereits in einem frühen Stadium erkannt und untersucht werden können, so dass eine effiziente und zeitgerechte Erledigung der entsprechenden Vorarbeiten sichergestellt ist. Zugleich erhalten die öffentlichen Organe geeignete datenschutzrechtliche Zielvorgaben, um ihre Projekte vernünftig planen und die notwendigen Ressourcen bereitstellen zu können.

Die zuständige Fachstelle für Datenschutz kann als Kriterien für die Bearbeitungsvorgänge, die ihr vorab zur Konsultation vorzulegen sind, beispielsweise die Zahl der erfassten Personen, die Zahl der beteiligten öffentlichen Organe oder die Sensibilität der Daten verwenden. Obwohl Abs. 3 eine «Kann-Formulierung» enthält, wird die Fachstelle für Datenschutz wohl regelmässig davon Gebrauch machen. Aus Gründen der Effizienz ist davon auszugehen, dass die Fachstelle für Datenschutz ein grosses Interesse hat, die Bearbeitungsvorgänge, die aus ihrer Sicht einer besonderen datenschutzrechtlichen Betrachtung bedürfen, zu definieren. Das öffentliche Organ hat die entsprechenden Angaben der Fachstelle für Datenschutz vorzulegen. Mit diesem Vorge-

---

26 Art. 28 RL 2016/680.

27 Die Formulierung des neuen Artikels lehnt sich an diejenige des Leitfadens der KdK und nicht an diejenige des Bundes an, da die Bestimmung im Vorentwurf zum Bundesgesetz über den Datenschutz von Fachkreisen kritisiert wurde. Vgl. Leitfaden der KdK (S. 16 ff.) sowie die Medienmitteilung der Vereinigung der schweizerischen Datenschutzbeauftragten Privatim vom 9. März 2017 (www.privatim.ch).

hen können bereits in einem frühen Projektstadium allfällige Problemfelder eingegrenzt werden, so dass nach der Vorabkonsultation das Projekt effizient und abgesichert weitergeführt werden kann.

Somit bestehen Sinn und Zweck der Vorabkonsultation darin, bei neuen Vorhaben den Datenschutz frühzeitig sicherzustellen. Als weiterer Vorteil der Vorabkonsultation erweist sich, dass insbesondere bei Rechtsetzungsvorhaben dafür gesorgt werden soll, dass die verfassungs- und datenschutzrechtlichen Vorgaben berücksichtigt werden. Nach Erhalt des Ersuchens um Durchführung einer Vorabkonsultation hat die zuständige Fachstelle für Datenschutz innert sechs Wochen (unter Berücksichtigung der Komplexität des Vorhabens längstens innert zehn Wochen) ihre Beurteilung (Empfehlung) abzugeben bzw. ihre Befugnisse auszuüben. Die Frist läuft dabei ab dem Zeitpunkt, an dem das Gesuch vollständig eingereicht worden ist. Ihr stehen dabei die verschiedenen Instrumente des Datenschutzgesetzes zur Verfügung. Kleine Vorabkonsultationen sollten zeitnah erledigt werden können; bei grossen Projekten wird die Vorabkonsultation voraussichtlich in verschiedenen Projektphasen gestaffelt stattfinden. Die genannte Frist wird durch die Richtlinie (EU) 2016/680 vorgegeben. Sie verdeutlicht die Wichtigkeit der Durchführung einer Vorabkonsultation und unterstreicht in der heutigen schnelllebigen Zeit die Bedeutung einer zeitnahen Beurteilung des Vorhabens.

Ein Beispiel für ein Vorhaben, bei dem eine Vorabkonsultation durchgeführt werden muss, findet sich im Bereich der kantonalen Einwohnerdatenplattform.[28] Rechtsetzungsprojekte im Gesetz über Niederlassung und Aufenthalt (sGS 453.1) können den Datenschutz betreffen. Daher werden inskünftig Revisionen dieses Gesetzes der Fachstelle für Datenschutz zur Durchführung einer Vorabkonsultation zu unterbreiten sein. Bei solchen Rechtsetzungsprojekten im Zusammenhang mit der kantonalen Einwohnerdatenplattform kann mit dem neuen Instrument der Vorabkonsultation sichergestellt werden, dass sich die Fachstelle für Datenschutz von Beginn an mit der datenschutzrechtlichen Problematik (z.B. der Einführung neuer Software oder neuer technischer Abfragemöglichkeiten) auseinandersetzt.

Auch wenn der Anschein erweckt werden könnte, dass die Vorabkonsultation der bisherigen Bearbeitung mit besonderen Risiken für den Grundrechteschutz (Art. 8 DSG) entspricht, ist festzuhalten, dass sich diese beiden Instrumente grundlegend unterscheiden und es sich bei der Vorabkonsultation um ein neues Verfahren im DSG handelt. Während bei der Bearbeitung von Personendaten mit besonderen Risiken für den Grundrechteschutz nach Art. 8 DSG das öffentliche Organ die Bearbeitung im Voraus der Fachstelle für Datenschutz nur meldet, hat die Fachstelle für Datenschutz beim Verfahren nach Art. 8b DSG eine Vorabkonsultation durchzuführen und innert Frist ihre Beurteilung (Empfehlung) abzugeben bzw. ihre Befugnisse auszuüben (Art. 8b Abs. 2 DSG).

4.2.4 Bearbeitung durch Dritte

Art. 9 regelt die Bearbeitung von Personendaten durch Dritte. In Abs. 1 werden neu sowohl Gesetz als auch Verordnung erwähnt. Mit der vorgeschlagenen Formulierung werden die Vorgaben des übergeordneten Rechts erfüllt. Die Richtlinie (EU) 2016/680[29] stellt weitere Voraussetzungen für das Datenbearbeiten durch Dritte auf, weshalb dem Artikel ein neuer Abs. 4 hinzuzufügen ist. Dabei werden bei einer Weiterübertragung der Datenbearbeitung Dienste einer weiteren Drittperson nur mit vorgängiger schriftlicher Genehmigung durch das auftraggebende öffentliche Organ in Anspruch genommen.

28 Vgl. Art. 15 f. des Gesetzes über Niederlassung und Aufenthalt (sGS 453.1).

29 Art. 22 f. RL 2016/680.

Nach der Richtlinie (EU) 2016/680 müssen Dritte, die Daten im Auftrag bearbeiten, hinreichende Garantien dafür bieten, dass durch geeignete technische und organisatorische Massnahmen sichergestellt wird, dass die Bearbeitung gesetzeskonform erfolgt und die Rechte der betroffenen Personen gewährleistet sind. Die Übertragung der Datenbearbeitung muss durch einen förmlichen Akt wie einen Vertrag oder ein anderes Rechtsinstrument erfolgen, das den Dritten bindet (beispielsweise durch Gesetz, Verordnung oder Regierungsbeschluss). Der Übertragung wird vermutlich in den meisten Fällen ein Vertrag zugrunde liegen. Darin müssen der Gegenstand und die Dauer der Bearbeitung, die Art der Bearbeitung, die Art der zu bearbeitenden Daten, die Kategorien möglicher betroffener Personen und die Rechte und Pflichten des Dritten und des auftraggebenden öffentlichen Organs festgelegt werden. Insbesondere muss gewährleistet sein, dass der Dritte, der Daten im Auftrag bearbeitet, nur auf Weisung des auftraggebenden öffentlichen Organs handelt, die beigezogenen Personen sich zur Vertraulichkeit verpflichtet haben (oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen) und die Rechte der betroffenen Personen uneingeschränkt wahrgenommen werden können. Bei Vertragsende sind die Daten nach Wahl des auftraggebenden öffentlichen Organs zu vernichten oder ihm zurückzugeben.

Selbstverständlich bleibt das auftraggebende öffentliche Organ dabei für den Umgang mit Personendaten nach Art. 3 DSG verantwortlich. Da im st.gallischen Recht keine Änderung der datenschutzrechtlichen Verantwortlichkeit vorgesehen ist, besteht diesbezüglich kein weiterer Regelungsbedarf.

4.2.5 Meldung von Datenschutzverletzungen

Aufgrund des übergeordneten Rechts[30] wird die Einfügung eines neuen *Art. 9a* im DSG notwendig, der die Meldung von Datenschutzverletzungen regelt. Eine Datenschutzverletzung ist unverzüglich der Fachstelle für Datenschutz zu melden, sofern es sich nicht um einen leichten Fall handelt. Das öffentliche Organ benachrichtigt ausserdem die betroffene Person, wenn die Umstände es erfordern oder die Fachstelle für Datenschutz es verlangt. Die Fachstelle für Datenschutz schreitet ein, wenn ihr eine Datenschutzverletzung gemeldet wird und es sich nicht um einen leichten Fall handelt. Immerhin kann die Benachrichtigung der betroffenen Person ganz oder teilweise eingeschränkt oder aufgeschoben werden, wenn öffentliche oder private Geheimhaltungsinteressen überwiegen. Dabei ist in erster Linie an die Gefährdung von Rechtsgütern wie beispielsweise Leib und Leben zu denken. Für das öffentliche Organ besteht eine Pflicht zur Meldung an die Fachstelle für Datenschutz, ausser es handelt sich um einen leichten Fall. Im Fall einer vorsätzlichen Nichtmeldung kann dies zwar nicht aus dem DSG, aber aufgrund anderer Gesetze zu Konsequenzen führen (z.B. Amtsdelikte aus dem Strafrecht oder in einem äussersten Fall Schadenersatz aufgrund von Widerrechtlichkeit). Falls die Datenschutzverletzung bei einer Datenbearbeitung durch Dritte geschieht, hat dieser unverzüglich das auftraggebende öffentliche Organ zu benachrichtigen, das dann die Verletzung der jeweils zuständigen Fachstelle für Datenschutz meldet. Dazu kann der Dritte durch vertragliche Abmachung (allenfalls auch mit einer Konventionalstrafe) verpflichtet werden.

In der vorliegenden Bestimmung (wie allgemein in einem «Grundsatz- oder Querschnittsgesetz» wie dem DSG) lässt sich ein rechtlicher Interpretationsspielraum nicht vermeiden, wenn die Regelung einer Meldepflicht nicht unnötig starr sein soll. Es braucht etwas Zeit, bis sich eine konstante Praxis herausgebildet hat. Es obliegt schlussendlich auch der Fachstelle für Datenschutz, eine Grenze zu setzen, welche Fälle (noch) als «leichter Fall» zu verstehen sind und welche nicht (mehr). Als leichter Fall könnte beispielsweise ein einfaches Versehen taxiert werden. Jedenfalls scheint es ausgeschlossen, die Fallkonstellationen, wie teilweise in der Vernehmlassung gefordert, präziser zu umschreiben.

30 Art. 30 und 31 RL 2016/680, Art. 7 Ziff. 2 E-Konv 108.

Um eine Meldepflicht an die Fachstelle für Datenschutz zu bejahen, ist denkbar, an verschiedene Merkmale anzuknüpfen: Das Vorliegen eines Kontrollverlusts über Daten, eine erhebliche Anzahl betroffene Personen, keine Möglichkeit der raschen Behebung und keine Möglichkeit zur sofortigen Minimierung des Risikos für die betroffenen Personen oder andere qualifizierende Merkmale (Hinweise auf kriminellen Hintergrund, systematisches Vorgehen, gezielter Hackerangriff). Für die Frage, ob eine Meldepflicht gegenüber der betroffenen Person besteht, kann beispielsweise auf folgende Kriterien abgestützt werden: Qualität der Daten (besonders schützenswerte Daten, Persönlichkeitsprofile, Profiles), besonderes Schädigungspotenzial für die betroffene Person (Bankdaten, Kreditkarteninformationen, Zugangsdaten, Passwörter oder Daten, die einem Berufsgeheimnis unterliegen) oder anderweitige erhebliche Risiken.[31] Wie erwähnt, muss sich jedoch eine konstante Praxis im Rahmen der Rechtsanwendung und Rechtsprechung erst noch herausbilden.

4.2.6 Archivierung und Vernichtung von Personendaten

Art. 10 regelt wie bisher die Archivierung und Vernichtung von Personendaten. Zum Begriff der Vernichtung von Personendaten ist an dieser Stelle festzuhalten, dass damit eine endgültige Vernichtung (im Sinn von unwiederbringlich) gemeint ist. Erforderlich ist neu aufgrund des übergeordneten Rechts[32] mindestens eine Regelung für die Löschung (oder Anonymisierung) jener Personendaten, die zur Aufgabenerfüllung nicht mehr benötigt werden, sofern sie nicht nach Archivrecht zu archivieren sind. Für das Angebot an das zuständige Archiv sieht die Regierung vor, dass dieses innert angemessener Frist zu erfolgen hat. Es ist möglich, dass öffentliche Organe die Frist mit dem Staatsarchiv vereinbaren. Die Frist beginnt mit der Erfüllung des Zwecks der Aufgabe zu laufen, zu der die Personendaten benötigt wurden. Die sinnvolle Kontrolle der Einhaltung obliegt der Fachstelle für Datenschutz. Selbstverständlich geht auch hier das entsprechende Prozessgesetz als lex specialis vor (siehe die Ausführungen zu Art. 2).

Schliesslich wird der offensichtliche Druckfehler «Personaldaten» anstatt «Personendaten» in Art. 10 Abs. 1 korrigiert. Dieser ist entstanden, als das Gesetz über Aktenführung und Archivierung vom 19. April 2011 (sGS 147.1; abgekürzt GAA) erlassen wurde.

4.2.7 Bearbeitung durch Justizbehörden und Polizei

Art. 10a (neu): Die Richtlinie (EU) 2016/680 sieht eine Pflicht zur Führung eines Verzeichnisses über Datenbearbeitungstätigkeiten vor.[33] Im Rahmen der Umsetzung des Schengen-Rechts wird diese Pflicht somit für Justizbehörden und Polizei eingeführt.[34] Unter dem Begriff Polizei wird die kantonale und kommunale Polizei im Sinn des Polizeigesetzes (sGS 451.1) verstanden. Im DSG wird neu festgehalten, dass die Justizbehörden und die Polizei ein Verzeichnis ihrer Bearbeitungstätigkeiten führen (Abs. 1). Das Verzeichnis enthält mindestens die Identität der Behörde, den Bearbeitungszweck, eine Beschreibung der Kategorien betroffener Personen und der Kategorien bearbeiteter Personendaten, die Kategorien der Empfängerinnen und Empfänger, wenn möglich die Aufbewahrungsdauer der Personendaten oder die Kriterien zur Festlegung dieser Dauer sowie, wenn möglich, eine allgemeine Beschreibung der Massnahmen zur Gewährleistung der Datensicherheit und, falls die Daten ins Ausland bekanntgegeben werden, die Angabe des Staates und die Garantien bei der Bekanntgabe von Personendaten ins Ausland nach dem Datenschutzrecht des Bundes. Befinden sich die Empfängerinnen und Empfänger im Ausland, muss daher aus dem Verzeichnis hervorgehen, ob grundsätzlich die Voraussetzungen für die Bekanntgabe ins Ausland erfüllt sind.[35] Abs. 3 dieses Artikels regelt den Inhalt des Verzeichnisses bei der Bearbeitung von Personendaten im Auftrag. Abs. 4 hält fest, dass das öffentliche Organ das Ver-

---

31 Vgl. J. Kleiner, Meldepflicht bei Datenschutzverletzungen, digma 2017, S. 170 ff.

32 Art. 5 RL 2016/680.

33 Art. 24 RL 2016/680.

34 Die Ausweitung dieser Pflicht auf weitere Behörden ist für den Kanton St.Gallen nicht notwendig.

35 Vgl. dazu Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, Ziff. 9.1.3.1, BBl 2017, 7019 ff.

zeichnis der zuständigen Fachstelle für Datenschutz melden muss. Das Verzeichnis ist als generelles Verzeichnis über mehrere Personen ausgestaltet (beispielsweise eine Dolmetscherliste). Abschliessend ist zu erwähnen, dass die Verantwortlichkeit im Sinn des DSG nicht delegiert werden kann (beispielsweise an die Konferenz der Gerichte). Verantwortlich bleibt das einzelne öffentliche Organ, das die Daten bearbeitet.

4.3 Bekanntgabe von Personendaten

Art. 13: Aufgrund des übergeordneten Rechts[36] werden der Begriff «Profile» in beiden Absätzen ergänzt und der Artikeltitel angepasst. Der Artikel regelt nun die Bekanntgabe von besonders schützenswerten Personendaten, Persönlichkeitsprofilen sowie die Bekanntgabe von Profiles (soweit dies technisch möglich ist).

4.4 Rechte der betroffenen Person

Das Recht jeder Person, Auskunft zu erhalten, ob und wenn ja, welche Daten über sie von einem öffentlichen Organ bearbeitet werden, und zwar unabhängig davon, ob das öffentliche Organ die Daten selber bearbeitet oder bearbeiten lässt, ist einer der Kernpunkte des Datenschutzrechts und stellt den Ausgangspunkt für die weiteren Rechte und Ansprüche der betroffenen Person dar. Der Wortlaut von *Art. 17 DSG* bleibt im Wesentlichen unverändert. Ergänzt wird Abs. 1 damit, dass ein Gesuch in der Regel schriftlich sein muss. Ein solches Gesuch ist unverzichtbar, um bei Gesuchen von externen Personen die Identität feststellen zu können. Zudem wird ein Gesuchsteller auch aus Gründen der Beweislast üblicherweise ein schriftliches Gesuch einreichen. Ist aufgrund spezieller Umstände die Identität und die Berechtigung einer Person klar oder ist diese ohnehin bekannt (z.B. bei internen Mitarbeitenden), kann auf die Schriftlichkeit verzichtet werden. Dies erscheint zweckmässig, um unnötige bürokratische Hürden zu vermeiden.

Art. 18 DSG regelt die Beschränkung der Auskunft und Einsicht. Diese Bestimmung wird mit der Formulierung «oder ein Gesetz in formellen Sinn dies vorsieht» ergänzt bzw. präzisiert. Somit kann ein öffentliches Organ Auskunft und Einsicht ablehnen, einschränken oder mit Auflagen verbinden, soweit öffentliche oder schutzwürdige private Interessen Dritter überwiegen oder ein Gesetz im formellen Sinn dies vorsieht.

Art. 20 bleibt im Wesentlichen unverändert. Der Artikel wird aber aufgrund des übergeordneten Rechts[37] dahingehend ergänzt, dass die Berichtigung kostenlos zu erfolgen hat.[38] Dass die Berichtigung innert angemessener Frist und in beförderlicher Art und Weise zu erfolgen hat, ist dabei selbstverständlich. Stellt ein öffentliches Organ einen Fehler selber fest, hat die Berichtigung von Amtes wegen zu erfolgen. Grundsätzlich trägt das öffentliche Organ die Beweislast für die Richtigkeit der Daten, nicht die betroffene Person diejenige für die Unrichtigkeit. Ansonsten gilt die übliche Beweislastregel von Art. 8 des Schweizerischen Zivilgesetzbuches (SR 210), da dieser allgemeine Rechtsgrundsatz auch im öffentlichen Recht gilt.[39] Kann weder die Richtigkeit noch die Unrichtigkeit bewiesen werden, hat das öffentliche Organ einen Bestreitungsvermerk anzubringen und darüber hinaus die Bearbeitung der entsprechenden Personendaten einzuschränken. Werden die Daten weitergegeben, hat dies zusammen mit dem Bestreitungsvermerk zu erfolgen. Ergänzend ist festzuhalten, dass Personendaten grundsätzlich richtig sein müssen (vgl. Art. 4 Abs. 2 DSG). Stellen sich Personendaten nachträglich als unrichtig heraus, dann sind

36 Art. 10 RL 2016/680, Art. 6 Ziff. 1 E-Konv 108.

37 Art. 16 RL 2016/680 sowie Art. 12 RL 2016/680 für die Modalitäten, Art. 8 Ziff. 1 Bst. e E-Konv 108.

38 Der Leitfaden der KdK führt aus, dass unter Umständen von der Natur der Daten her weder die Richtigkeit noch die Unrichtigkeit von Personendaten bewiesen werden kann (S. 13). Auf die Formulierung «Natur der Daten» wurde vorliegend aufgrund des unklaren Begriffs und des weiten Interpretationsspielraums verzichtet.

39 Vgl. BGer 2A.669/2005 Erw. 3.5.2; BVGE A-5361/2013 Erw. 3.9.3.

sie nicht unbedingt falsch, wenn der zeitliche Kontext dabei ersichtlich ist bzw. klar ist, dass die Angabe dem damaligen Wissenstand entsprach. Ist dies nicht der Fall, ist eine Berichtigung in jedem Fall vorzunehmen. Betreffend die Löschung unrichtiger Daten nach Abs. 2 Bst. a ist ergänzend zu bemerken, dass die unrichtigen Daten mindestens gelöscht werden müssen. Wenn nur eine Vernichtung der Daten möglich ist (beispielsweise durch das Überschreiben von Datenfeldern), muss auch die Vernichtung zulässig sein (vgl. Terminologie bei Art. 1 Abs. 1 Bst. e DSG).

Weiter gibt es Änderungen bei den Ansprüchen der betroffenen Person.[40] Werden Daten unrechtmässig bearbeitet, kann die betroffene Person folgende Ansprüche geltend machen: Unterlassung der widerrechtlichen Bearbeitung, Löschung der unrichtigen Daten und Sperrung der Bekanntgabe an Dritte, Feststellung der Widerrechtlichkeit der Bearbeitung und Beseitigung der Folgen der widerrechtlichen Bearbeitung (z.B. durch Löschung, Mitteilung an Datenempfänger, Veröffentlichung, Schadenersatz, Genugtuung).

Ob ein schutzwürdiges Interesse vorliegt, ist nur dann zu prüfen, wenn nicht die betroffene Person, sondern eine dritte Person (ohne Vollmacht der betroffenen Person) die Berichtigung verlangt. Bei der betroffenen Person ist dieses Interesse wohl stets gegeben. Der Anspruch auf Löschung kann geltend gemacht werden bei widerrechtlich bearbeiteten Personendaten. Eine Löschung kann jedoch unterbleiben, wenn die Personendaten zu Beweiszwecken aufbewahrt werden müssen. Die Dokumentationspflicht bei staatlichem Handeln kann in vielen Fällen auch mit anonymisierten Daten erfolgen. Der Löschungsanspruch kann allenfalls auch zu bestimmten Zwecken (z.B. Schutz der öffentlichen Sicherheit, Nichtbehinderung behördlicher oder gerichtlicher Untersuchungen u.Ä.) spezialgesetzlich eingeschränkt werden.

Der bisherige Abs. 3 bleibt bestehen. Er wird jedoch dahingehend ergänzt, dass die Information unterbleiben kann, wenn sie nicht oder nur mit unverhältnismässigem Aufwand möglich ist. Dies darf nicht leichthin angenommen werden. Ein Beispiel für einen unverhältnismässigen Aufwand könnte beispielsweise eine Massenberichtigung darstellen. Das öffentliche Organ muss aber mindestens den Versuch unternommen haben und dabei auf konkrete, nur mit erheblichem Einsatz überwindbare Schwierigkeiten gestossen sein.

Der neue *Art. 20a* regelt die Informationspflicht.[41] Verlangt wird eine Information über das Beschaffen von Personendaten durch das öffentliche Organ bei Amtsstellen oder Dritten. Dazu ist festzuhalten, dass eine «Beschaffung» ein aktives Tun[42] des öffentlichen Organs (oder einer für das öffentliche Organ tätigen Person) voraussetzt, d.h. beispielsweise eine Anfrage oder Abklärung. Erhält das öffentliche Organ solche Daten ohne ein solches aktives Zutun, greift die Informationspflicht nicht. Personendaten, die in einer für jedermann zugänglichen Weise (z.B. auf einer Webseite) zur Verfügung gestellt wurden oder notorisch sind, werden nicht im Sinn dieses Artikels beschafft und daher entfällt die Informationspflicht. Das heisst, frei zugängliche Informationen und solche, die dem öffentlichen Organ zugetragen wurden (auf einsichtigem Weg), sind nicht betroffen. Das öffentliche Organ hat jedoch zu klären, ob die Personendaten richtig sind (vgl. auch Art. 12 VRP).

Nach *Art. 20b* kann die umfassende Informationspflicht entfallen[43], wenn:
– die betroffene Person über die Information, die ihr zukommen müsste, bereits verfügt (insbesondere, wenn sie in einer früheren Phase der Beschaffung bereits einmal informiert worden ist oder sie die Informationen selber zur Verfügung gestellt hat),

40 Notwendig aufgrund von Art. 54 RL 2016/680, Art. 8 E-Konv 108.

41 Notwendig aufgrund von Art. 13 RL 2016/680, Art. 7bis E-Konv 108.

42 So auch in B. Rudin, Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Basel-Stadt (IDG), Zürich 2014.

43 Notwendig aufgrund von Art. 7bis Ziff. 1bis E-Konv 108.

– die Bearbeitung der Personendaten gesetzlich ausdrücklich vorgesehen ist (d.h. wenn die betroffenen Personen aus den gesetzlichen Grundlagen mit hinreichender Präzision herauslesen können, welche Daten über sie zu welchem Zweck bearbeitet werden) oder
– die Information der betroffenen Person nicht oder nur mit unverhältnismässigem Aufwand möglich ist.

Als Beispiel für den Ausnahmetatbestand «gesetzlich ausdrücklich vorgesehen» ist das Steuergesetz (sGS 811.1) zu nennen. Für die Steuerbehörde ist die Datenbearbeitung bzw. das Einfordern notwendiger Dokumente steuerpflichtiger Personen gesetzlich vorgesehen. Eine Informationspflicht nach DSG entfällt somit. Ein weiteres Beispiel stellt eine Sachverhaltsermittlung nach Art. 12 VRP dar. Auch diese fällt unter den Ausnahmetatbestand «gesetzlich ausdrücklich vorgesehen» nach Art. 20b DSG. Weiter ist zu diesem Ausnahmetatbestand festzuhalten, dass auch ein Gesetz in Verbindung mit einer ergänzenden, konkretisierenden Verordnung den Tatbestand erfüllt, wenn aus der Verordnung mit hinreichender Präzision herausgelesen werden kann, welche Daten zu welchem Zweck bearbeitet werden. Ein Gesetz im formellen Sinn als Grundnorm ist jedoch im Fall von Bst. b stets notwendig. Im Übrigen werden die Auslegung der Ausnahmetatbestände nach Art. 20b DSG von der Rechtsprechung zu konkretisieren sein. Es kann aber davon ausgegangen werden, dass das DSG als «Grundnorm» Anwendung findet und ein Spezialgesetz, beispielsweise das VRP, als lex specialis dem DSG vorgeht.

Ausserdem kann die Information im gleichen Masse eingeschränkt (d.h. ganz oder teilweise eingeschränkt oder aufgeschoben) werden wie der Zugang zu den eigenen Personendaten (Recht auf Auskunft; Art. 17 DSG). Sobald der Einschränkungsgrund wegfällt, ist die Information nachzuholen.

4.5 Fachstelle für Datenschutz

Einleitend ist zu bemerken, dass mit Erlass des DSG eine kantonale sowie kommunale Fachstellen für Datenschutz vorgesehen und verlangt wurden. Im Rahmen der Anpassung des DSG an die übergeordneten Rechtsgrundlagen erhält diese Funktion eine qualitative Aufwertung und eine stärkere Überprüfungsbefugnis. Dies gilt sowohl für die kantonale Fachstelle für Datenschutz als auch für die Gemeindefachstellen für Datenschutz. Es ist jedoch darauf hinzuweisen, dass die kantonale Fachstelle für Datenschutz zusätzlich die Befugnis erhalten soll, Verfügungen zu erlassen (vgl. den neuen Art. 35a DSG).

An dieser Stelle ist weiter festzuhalten, dass die Leiterin oder der Leiter der jeweiligen Fachstelle für Datenschutz die für die Erfüllung ihrer bzw. seiner Aufgaben und zur Ausübung der entsprechenden Befugnisse erforderliche Qualifikation, Erfahrung und Sachkunde insbesondere im Bereich des Datenschutzes aufweisen muss.[44] Darunter ist eine Person zu verstehen, die über ausgewiesene juristische Kenntnisse verfügt, wie z.B. ein rechtswissenschaftliches Studium und mehrjährige Praxiserfahrung. Dies gilt insbesondere für die Leiterin oder den Leiter der kantonalen Fachstelle für Datenschutz, deren Anforderungsprofil nochmals gesteigert wird. Die Leiterin oder der Leiter der Fachstelle für Datenschutz muss zudem auch die massgeblichen Entwicklungen im Bereich des Datenschutzes[45] im Auge behalten und ihre bzw. seine Tätigkeit darauf ausrichten. Dazu gehören u.a. die Entwicklungen in der Informations- und Kommunikationstechnologie, der Rechtsprechung und der Gesetzgebung. Dies versteht sich jedoch von selbst und wird daher nicht explizit in den Gesetzestext aufgenommen.

44 Notwendig aufgrund von Art. 43 Abs. 2 RL 2016/680.

45 Notwendig aufgrund von Art. 46 Abs. 1 Bst. j RL 2016/680.

4.5.1 Organisation

In *Art. 28 Abs. 1* wird aufgrund des übergeordneten Rechts[46] eine Änderung betreffend die Amtsdauer notwendig. Neu wird die Leiterin oder der Leiter der kantonalen Fachstelle für Datenschutz für eine feste Amtsdauer von vier Jahren gewählt. Es handelt sich somit um ein befristetes Arbeitsverhältnis auf Amtsdauer. Weiter wird Satz 2 dieses Absatzes mit der Formulierung «vor Ablauf der Amtsdauer» ergänzt.

In Abs. 2 wird ergänzt, dass auch die Leiterin oder der Leiter der Gemeindefachstelle für Datenschutz für eine Amtsdauer von vier Jahren ernannt wird.

Der neue Abs. 3bis regelt, dass die Leiterin oder der Leiter der jeweiligen Fachstelle für Datenschutz kein anderes öffentliches Amt, keine leitende Funktion in einer politischen Partei und keine andere Erwerbstätigkeit ausüben darf.[47] Die Regierung, in der Gemeinde der Rat, kann davon absehen, wenn dadurch die Unabhängigkeit und die Ausübung der Funktion nicht beeinträchtigt werden. Die Verantwortung dafür liegt bei der Regierung bzw. in der Gemeinde beim Rat. Die Formulierung entspricht nun im Wesentlichen der Formulierung des Bundes.

Nach Abs. 4 stellt die Leiterin oder der Leiter der Fachstelle für Datenschutz im Rahmen des Voranschlags die Mitarbeitenden an. Dies erfolgt nach den massgeblichen arbeitsrechtlichen Bestimmungen.

Abs. 5 wird im Sinn einer Folgekorrektur zum Erlass des Personalgesetzes (sGS 143.1) dahingehend abgeändert, dass sich das Arbeitsverhältnis der Leiterin oder des Leiters sowie der Mitarbeitenden der kantonalen Fachstelle für Datenschutz nach dem Personalgesetz richten.

Die Einführung einer neuen Geheimhaltungspflicht für das Personal der kantonalen Fachstelle für Datenschutz[48] erachtet die Regierung für entbehrlich. Da diese bereits durch das Amtsgeheimnis sowie Art. 3a des Staatsverwaltungsgesetzes (sGS 140.1) abgedeckt wird, wird auf eine Wiederholung im Datenschutzgesetz verzichtet.

4.5.2 Zuständigkeit / Aufgaben

Art. 30 Abs. 1 Bst. a wird mit der Möglichkeit einer anlassfreien Überprüfung der Einhaltung der Bestimmungen über den Datenschutz durch die jeweilige Fachstelle für Datenschutz ergänzt.[49] Zu der bereits bisher bestehenden Anzeige ist anzumerken, dass hiermit jede Person unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs die Möglichkeit einer datenschutzrechtlichen Anzeige bei der Fachstelle für Datenschutz hat, wenn sie der Ansicht ist, dass die Bearbeitung der sie betreffenden Personendaten gegen die datenschutzgesetzlichen Vorschriften verstosse.[50] Die anzeigende Person hat dabei nicht die Rechte einer Partei. Selbstverständlich sind rechtsmissbräuchliche Anzeigen wie bis anhin unzulässig. Die Fachstelle für Datenschutz hat sich mit dieser Anzeige zu befassen und der sich beschwerenden Person innert drei Monaten die Art der Erledigung mitzuteilen (Satz 2). Kommt die Fachstelle für Datenschutz dieser Pflicht nicht oder nicht rechtzeitig nach, besteht die Möglichkeit eines Rechtsmittels[51] (Rechtsverweigerungsbeschwerde). Dieses richtet sich wie üblich nach dem VRP. Das VRP wird entsprechend in Art. 89 Abs. 1 mit dem neuen Bst. c^{bis} dahingehend ergänzt, als dass neu für Rechtsverweigerungsbeschwerden gegen die kantonale Fachstelle für Datenschutz die Verwaltungsrekurskommission zuständig ist.

---

46 Art. 43 Abs. 3 RL 2016/680.

47 Notwendig aufgrund von Art. 42 Abs. 3 RL 2016/680.

48 Notwendig aufgrund von Art. 44 Abs. 2 RL 2016/680; Art. 12bis Ziff. 5ter E-Konv 108.

49 Notwendig aufgrund von Art. 46 Abs. 1 Bst. a RL 2016/680.

50 Notwendig aufgrund von Art. 52 f. RL 2016/680; Art. 12bis Ziff. 3 E-Konv 108.

51 Notwendig aufgrund von Art. 53 Abs. 2 RL 2016/680.

In der Vernehmlassung wurde die Befürchtung geäussert, dass Mitarbeitende durch die Anforderungen des neuen DSG überfordert sein könnten und sich dadurch rechtlichen Risiken aussetzen würden. Dazu ist auszuführen, dass die Fachstelle für Datenschutz wie bereits bisher die öffentlichen Organe in Fragen des Datenschutzes berät. Mitarbeitende eines öffentlichen Organs können und sollen sich bei Fragen und Unklarheiten an die Fachstelle für Datenschutz wenden. Die Regierung ist der Ansicht, dass durch diese Entlastungsmöglichkeit die Bedenken entschärft werden können.

Weiter wird der Aufgabenkatalog der Fachstellen für Datenschutz mit Bst. f[52] und g[53] erweitert. Neu gehört zu den Aufgaben der Fachstelle für Datenschutz die Sensibilisierung der verantwortlichen öffentlichen Organe für ihre datenschutzrechtlichen Pflichten und der Öffentlichkeit für die Anliegen des Datenschutzes (z.B. auch im Hinblick auf die Eigenverantwortung der betroffenen Personen) sowie die Zusammenarbeit der Fachstelle für Datenschutz mit den Organen der anderen Kantone, des Bundes und des Auslands, welche die gleichen Aufgaben erfüllen. Damit wird die Amtshilfe neu ausdrücklich ins DSG aufgenommen. Zudem wird in Art. 30 aufgrund des übergeordneten Rechts[54] ein neuer Abs. 1bis eingefügt. Demnach unterstehen Kantonsrat und Regierung sowie Gemeindeparlament und Rat (Bst. a) sowie als «Gegenstück» zur Anwendbarkeit des Datenschutzgesetzes in hängigen Verfahren der Zivil-, der Straf- und der gerichtlichen Verwaltungsrechtspflege sowie in hängigen Rechtshilfeverfahren die Datenbearbeitungen in diesen Verfahren (Bst. b) nicht der Aufsicht der Fachstelle für Datenschutz. Dennoch bleiben das DSG und dessen Grundsätze gültig. Bei hängigen Verfahren liegt die Aufsicht bei der zuständigen Verfahrensaufsicht. Im Fall von rechtskräftig abgeschlossenen Verfahren liegt die Zuständigkeit hingegen bei der Fachstelle für Datenschutz. Zu Bst. a ist zu ergänzen, dass das DSG auch die Kommissionen des Kantonsrates und der Gemeindeparlamente von der Aufsicht ausnimmt.

Der neue *Art. 30a* regelt die Kosten.[55] Er legt fest, dass die Erfüllung der Aufgaben der Fachstelle für Datenschutz für die betroffenen Personen in der Regel unentgeltlich ist. Bei offenkundig unbegründeten oder – besonders wegen Wiederholung – unverhältnismässig häufigen Anträgen kann die Fachstelle eine angemessene Gebühr auf der Grundlage des Gebührentarifs für die Kantons- und Gemeindeverwaltung (sGS 821.5)[56] verlangen oder sich weigern, aufgrund des Antrags tätig zu werden.

Im Rahmen der Gesetzesrevision wird *Art. 31* dahingehend präzisiert, dass die Fachstelle für Datenschutz berechtigt ist, die für die Erfüllung ihrer Aufgaben unentbehrlichen Daten einschliesslich besonders schützenswerten Personendaten, Persönlichkeitsprofilen und Profiles aus den Datensammlungen des öffentlichen Organs einzusehen. Dabei wird eine formelle Änderung vorgenommen: Der Begriff «besonders geschützte Personendaten» wird ersetzt durch den Begriff «besonders schützenswerte Personendaten», um die einheitliche Begriffsverwendung im gesamten Erlass sicherzustellen. Für die Einsichtnahme innerhalb der Verwaltung (Kanton und Gemeinden) werden keine Kosten erhoben.

Mit dem neuen *Art. 35a*[57] soll der kantonalen Fachstelle für Datenschutz neu die Befugnis zukommen, bei Verstössen gegen das Datenschutzrecht verbindliche Anordnungen (in Form einer Verfügung) zu treffen (z.B. ein widerrechtliches Datenbearbeiten einzustellen oder auf eine wider-

52 Notwendig aufgrund von Art. 46 Abs. 1 Bst. b und d RL 2016/680; Art. 12bis Ziff. 2 Bst. e E-Konv 108.

53 Notwendig aufgrund von Art. 46 Abs. 1 Bst. h RL 2016/680.

54 Art. 45 Abs. 2 RL 2016/680; Art. 12bis Ziff. 9 E-Konv 108.

55 Notwendig aufgrund von Art. 46 Abs. 3 RL 2016/680.

56 Zu denken wäre etwa an die Position 20.12: Verfügung in einem Verwaltungsverfahren, soweit keine andere Gebühr festgelegt ist.

57 Notwendig aufgrund von Art. 47 Abs. 2 Bst. b und c RL 2016/680; Art. 12bis Ziff. 2 Bst. c und Art. 12bis Ziff. 6 E-Konv 108.

rechtliche Datenbekanntgabe zu verzichten). Diese Befugnis kommt ausdrücklich nur der kantonalen Fachstelle für Datenschutz zu. Damit soll sichergestellt werden, dass eine einheitliche Überprüfung bzw. Praxis durch ein einziges Organ erfolgt. Dies hält die Regierung auch im Hinblick auf die Ressourcenthematik für angezeigt. Entsprechend gibt es neu zwei Möglichkeiten: Die Fachstelle für Datenschutz kann wie bisher nach Art. 34 DSG die Anordnung von Massnahmen beantragen, wenn ein öffentliches Organ ihre Empfehlungen nicht oder nur teilweise umsetzen will oder innert angemessener Frist keine Stellungnahme abgibt. Sie kann aber auch neu bei erheblichen Datenschutzverletzungen, in denen ein schnelleres Handeln nötig ist, eine eigene Verfügung erlassen, wenn absehbar ist, dass das öffentliche Organ eine Empfehlung ablehnen oder ihr keine Folge leisten wird (oder das öffentliche Organ erklärt, der Empfehlung nicht folgen zu wollen oder der Empfehlung tatsächlich nicht folgt). Das öffentliche Organ kann Verfügungen nach Art. 35a DSG mit Rekurs anfechten. Da Verfügungen nach diesem Artikel Datenschutzverletzungen eines öffentlichen Organs betreffen, ist auch nur das öffentliche Organ rekursberechtigt. Es handelt sich um ein Verhältnis zwischen der kantonalen Fachstelle für Datenschutz und dem öffentlichen Organ. Da die betroffene Person diesem Verhältnis nicht zugehört, ist sie auch nicht rekursberechtigt. Als Rekursinstanz ist die Verwaltungsrekurskommission vorgesehen. Die Verwaltungsrekurskommission ist eine gerichtliche Instanz und verfügt über volle Kognition, d.h. sie kann den Verstoss gegen wesentliche Form- und Verfahrensvorschriften, die unrichtige oder unvollständige Feststellung des Sachverhalts sowie die Rechtswidrigkeit oder die Unangemessenheit des Inhalts der Verfügung überprüfen (vgl. Art. 46 VRP). Gegen den Entscheid der Verwaltungsrekurskommission kann beim Verwaltungsgericht Beschwerde erhoben werden (Art. 59 VRP). Der vorliegende Rechtsmittelweg entspricht der Tradition der st.gallischen Verwaltungsrechtspflege, die von einem zweistufigen Rechtsmittelweg geprägt ist.

Die kantonale Fachstelle für Datenschutz ist gehalten, auch vorsorgliche Massnahmen in Form einer Verfügung zu treffen.[58] Falls schutzwürdige Interessen offensichtlich gefährdet oder verletzt werden, muss die kantonale Fachstelle für Datenschutz die Befugnis haben, vorsorglich eine Datenbearbeitung einzuschränken oder zu untersagen. Da die vorsorgliche Massnahme in Art. 18 VRP bereits allgemein geregelt ist, kann auf eine entsprechende Bestimmung in diesem Gesetz verzichtet werden. Das öffentliche Organ kann hier gegen die Verfügung der Fachstelle für Datenschutz innert fünf Tagen Rekurs (analog zum VRP; vgl. Art. 47 Abs. 2 VRP) bei der Verwaltungsrekurskommission erheben.

Ferner ist aufgrund des übergeordneten Rechts[59] die Möglichkeit einer allgemeinen aufsichtsrechtlichen Anzeige an die vorgesetzte Behörde des gegen das Datenschutzrecht verstossenden öffentlichen Organs vorzusehen. Diese ist zu unterscheiden von der in Art. 30 Abs. 1 Bst. a DSG geregelten Anzeige an die Fachstelle für Datenschutz. Eine Aufsichtsbeschwerde («Anzeige») ist jedoch kein Rechtsmittel im eigentlichen Sinn, sondern ein Rechtsbehelf. Die Grundlage für die Aufsichtsbeschwerde bilden einerseits der Grundsatz der Gesetzmässigkeit und anderseits der hierarchische Aufbau der Verwaltung mit den damit verbundenen Aufsichtsbefugnissen der übergeordneten Behörde. Für eine Anzeige ist daher keine ausdrückliche gesetzliche Grundlage erforderlich.[60] Deshalb wird vorliegend auf eine Regelung im DSG verzichtet.

4.6 Änderung anderer Erlasse

Aufgrund der vorliegenden Teilrevision ist es notwendig, Art. 23 Abs. 2 GAA dahingehend abzuändern, dass kein Zugang zu Archivgut besteht, dass nach dem vorliegenden Gesetz besonders

58 Notwendig aufgrund von Art. 47 Abs. 2 Bst. c RL 2016/680.

59 Art. 47 Abs. 5 RL 2016/680; Art. 12bis Ziff. 2 Bst. d E-Konv 108.

60 Cavelti / Vögeli, Verwaltungsgerichtsbarkeit im Kanton St.Gallen – dargestellt an den Verfahren vor dem Verwaltungsgericht, 2. Aufl., St.Gallen 2003, § 48 N 1218.

schützenswerte Personendaten, Persönlichkeitsprofile oder Profiles enthält, ausgenommen bei Vorliegen eines überwiegenden öffentlichen Interesses oder bei Zustimmung der betroffenen Person.

Zudem wird im Rahmen der vorliegenden Teilrevision auch das VRP geändert. So wird in Art. 41 Abs. 1 Bst. j VRP festgelegt, dass Verfügungen der kantonalen Fachstelle für Datenschutz mit Rekurs bei der Verwaltungsrekurskommission anfechtbar sind. Wie bereits erwähnt, wird Art. 89 Abs. 1 VRP dahingehend ergänzt, dass neu die Verwaltungsrekurskommission (Bst. c^{bis}) auch über Rechtsverweigerungsbeschwerden gegen die Fachstelle für Datenschutz entscheidet.

5 Kostenfolgen

Der genaue finanzielle Aufwand für die Umsetzung dieser Vorlage ist derzeit nicht abschätzbar. Auch die kantonale Fachstelle für Datenschutz konnte die geschätzten finanziellen Auswirkungen nicht beziffern oder zumindest grob abschätzen. Die Regierung ist deshalb der Ansicht, dass es sich rechtfertigt, vorerst mit den vorhandenen Ressourcen weiterzuarbeiten und diese nach einer gewissen Zeit (z.B. einer Amtsdauer) zu evaluieren. Zu diesem Zeitpunkt liegen auch genaue Zahlen zum Arbeitsaufwand der kantonalen Fachstelle für Datenschutz unter dem revidierten DSG vor. Sofern notwendig, könnten dann ressourcenmässige Anpassungen vorgenommen werden. Somit ergeben sich derzeit keine Kostenfolgen für diese Vorlage.

Schliesslich haben aufgrund der gesellschaftlichen und der informationstechnischen Entwicklung der letzten Jahrzehnte sowohl der Stellenwert als auch die rechtliche Bedeutung des Datenschutzes erheblich zugenommen. Entsprechend ist dem Funktionsausbau der neuen Datenschutzgesetzgebung zweifellos angemessen Rechnung zu tragen und sind die notwendigen Ressourcen in angemessener Weise bereitzustellen. Dabei ist zu beachten, dass sich auch der fachliche Fokus verstärkt auf juristisch-forensische Fragestellungen verschoben hat, weshalb sowohl auf kantonaler als auch auf kommunaler Ebene bei den Fachstellen für Datenschutz zwingend Mitarbeitende mit spezialisierter akademischer und praktischer Erfahrung auf dem Gebiet des Datenschutzrechts notwendig sind.

6 Rechtliches

Der Nachtrag zum Datenschutzgesetz untersteht dem fakultativen Gesetzesreferendum nach Art. 49 Abs. 1 Bst. a der Kantonsverfassung (sGS 111.1) und Art. 5 des Gesetzes über Referendum und Initiative (sGS 125.1).

7 Antrag

Wir beantragen Ihnen, Frau Präsidentin, sehr geehrte Damen und Herren, auf den Nachtrag zum Datenschutzgesetz einzutreten.

Im Namen der Regierung

Stefan Kölliker
Präsident

Canisius Braun
Staatssekretär

Nachtrag zum Datenschutzgesetz

Entwurf der Regierung vom 9. Oktober 2018

Der Kantonsrat des Kantons St.Gallen

hat von der Botschaft der Regierung vom 9. Oktober 2018[61] Kenntnis genommen und

erlässt:

I.

Der Erlass «Datenschutzgesetz vom 20. Januar 2009»[62] wird wie folgt geändert:

Art. 1 Begriffe

[1] In diesem Erlass bedeuten:

a) Personendaten: Angaben, die sich auf eine bestimmte oder bestimmbare **natürliche** Person beziehen;

a[bis]) Daten: alle auf einem Datenträger abgelegten Angaben;

b) besonders schützenswerte Personendaten: Angaben über:

1. religiöse, weltanschauliche sowie politische Ansichten und Tätigkeiten. Ausgenommen sind Angaben über die Mitgliedschaft bei einer Religionsgemeinschaft, einer Organisation oder einer politischen Partei, wenn die betroffene Person diese selbst bekannt gegeben hat oder für ein öffentliches Amt kandidiert;
2. Gesundheit, Intimsphäre und ~~Rassenzugehörigkeit~~**ethnische Zugehörigkeit**;

2[bis]. genetische Daten[63];

2[ter]. biometrische Daten: mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, welche die eindeutige Identifizierung dieser Person ermöglichen oder bestätigen;

3. Leistungen und Massnahmen der sozialen Hilfe;
4. strafrechtliche sowie disziplinarische Verfahren und Sanktionen;

c) betroffene Person: natürliche ~~oder juristische~~ Person ~~sowie Personengemeinschaften~~, über die Personendaten bearbeitet werden;

d) Persönlichkeitsprofil: Zusammenstellung von Personendaten, welche die Beurteilung der Persönlichkeit einer natürlichen Person erlaubt;

d[bis]) Profile: Erkenntnisse, die sich aus der Auswertung von Daten ergeben, um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen, insbesondere bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, Intimsphäre oder Mobilität;

---

61 ABl 2018, ●●.

62 sGS 142.1.

63 Gemäss Bundesgesetz über genetische Untersuchungen beim Menschen vom 8. Oktober 2004, SR 810.12.

e) Bearbeitung ~~von Personendaten~~: **jeder** Umgang mit Personendaten, **unabhängig von den angewandten Mitteln und Verfahren,** insbesondere **die** Beschaffung, Aufbewahrung, Verwendung, **Umarbeitung,** Bekanntgabe, **Archivierung,** ~~Veränderung~~**Löschung** oder Vernichtung **von Personendaten sowie die Durchführung logischer oder rechnerischer Operationen mit diesen Personendaten**;

e[bis]) Datenschutzverletzung: unrechtmässige Bearbeitung von Daten, so dass bearbeitete Personendaten vernichtet werden oder verloren gehen, unbeabsichtigt oder unrechtmässig verändert oder offenbart werden oder dass Unbefugte Zugang zu solchen Personendaten erhalten;

f) Bekanntgabe von Personendaten: Zugänglichmachen von Personendaten sowie Gewährung von Einsicht, Weitergabe und Veröffentlichung;

g) Datensammlung: Bestand von Personendaten, der nach Personen erschlossen oder erschliessbar ist;

h) öffentliches Organ: (Dem öffentlichen Organ sind Private gleichgestellt, wenn sie Staatsaufgaben erfüllen.)[64] Organ, Behörde oder Dienststelle von:
   1. Kanton;
   2. selbständiger öffentlich-rechtlicher Anstalt des Kantons;
   3. Gemeinde;
   4. selbständigem öffentlich-rechtlichem Gemeindeunternehmen;
   5. Gemeindeverband und Zweckverband;

i) Empfängerin oder Empfänger: natürliche oder juristische Person, die vom öffentlichen Organ Personendaten erhält;

j) Fachstelle für Datenschutz: von Kanton und Gemeinde eingesetztes Organ für Aufsicht und Beratung im Datenschutz;

k) Rechtsgrundlage: Erlass mit allgemein verbindlichen Bestimmungen, insbesondere Gesetz und Verordnung. Der Verordnung sind vom fakultativen Referendum ausgenommene Vollzugsvorschriften von Gemeinden gleichgestellt;

l) Gesetz: Erlass, der nach Art. 67 der Kantonsverfassung vom 10. Juni 2001[65] von den Stimmberechtigten ausdrücklich oder stillschweigend angenommen wurde, sowie zwischenstaatliche Vereinbarungen, denen nach Massgabe ihres Inhalts Verfassungs- oder Gesetzesrang zukommt. Dem Gesetz sind die Gemeindeordnung sowie das rechtsetzende Reglement und die rechtsetzende Vereinbarung gleichgestellt.

Art. 2 Geltungsbereich
a) Grundsatz

[1] Dieser Erlass regelt ~~die~~**jegliche** Bearbeitung von Personendaten durch öffentliche Organe.

[2] Er wird nicht angewendet:

a) wenn das öffentliche Organ am wirtschaftlichen Wettbewerb teilnimmt und dabei nicht hoheitlich handelt;

b) auf Personendaten, die von einem im Dienst- oder Auftragsverhältnis mit dem öffentlichen Organ stehenden natürlichen Person zum ausschliesslich persönlichen Gebrauch bearbeitet werden und anderen Personen weder ausgehändigt werden noch ihnen zugänglich sind;

c) ~~in hängigen Verfahren der Zivil-, der Straf- und der gerichtlichen Verwaltungsrechtspflege sowie in hängigen Rechtshilfeverfahren;~~

d) auf Personendaten, die das zuständige Archiv von Kanton und Gemeinde dauerhaft aufbewahrt.

---

64 Im ursprünglichen Erlasstext war der in Klammern gesetzte abschliessende Text nach der Aufzählung in Bst. h platziert. Dieser wurde im September 2013 aus technischen Gründen in den Ingress der Aufzählung verschoben.

65 sGS 111.1.

[3] In hängigen Verfahren der Zivil-, der Straf- und der gerichtlichen Verwaltungsrechtspflege sowie in hängigen Rechtshilfeverfahren richten sich die Rechte und Ansprüche nach dem jeweiligen Verfahrensrecht.

Art. 3 Verantwortlichkeit

[1] Wer Personendaten bearbeitet oder bearbeiten lässt, ist für die Einhaltung des Datenschutzes verantwortlich.

[2] Bearbeiten mehrere öffentliche Organe Personendaten einer Datensammlung, bezeichnen sie das für die Einhaltung des Datenschutzes verantwortliche Organ. Bei Uneinigkeit entscheidet die kantonale Fachstelle für Datenschutz.

[3] Das öffentliche Organ ist für die Einhaltung der Datenschutzbestimmungen beweispflichtig.

Art. 5 Voraussetzungen

[1] Die Bearbeitung von Personendaten ist zulässig, wenn eine Rechtsgrundlage besteht oder die Bearbeitung zur Erfüllung einer gesetzlichen Aufgabe erforderlich ist.

[2] Die Bearbeitung von besonders schützenswerten Personendaten**,** ~~und~~ Persönlichkeitsprofilen **und Profiles** ist zulässig, wenn:

a) das Gesetz die Bearbeitung vorsieht oder
b) die Bearbeitung zur Erfüllung einer gesetzlichen Aufgabe unentbehrlich ist oder
c) die betroffene Person:
   1. im Einzelfall ausdrücklich sowie in Kenntnis von Zweck und Art der vorgesehenen Bearbeitung eingewilligt hat oder
   2. ihre Daten allgemein zugänglich gemacht hat.

Art. 8a (neu) Datenschutz-Folgenabschätzung

[1] Das öffentliche Organ nimmt bei Gefahr von Datenschutzverletzungen eine Datenschutz-Folgenabschätzung vor.

[2] Diese enthält wenigstens:

a) eine allgemeine Beschreibung der geplanten Bearbeitungsvorgänge;
b) eine Bewertung der in Bezug auf die Grundrechte der betroffenen Personen bestehenden Risiken sowie
c) eine Darstellung und Bewertung der geplanten Abhilfemassnahmen.

Art. 8b (neu) Vorabkonsultation

[1] Das öffentliche Organ legt der Fachstelle für Datenschutz zur Vorabkonsultation vor:

a) Rechtsetzungsprojekte, die den Datenschutz betreffen;
b) Vorhaben zur Bearbeitung von Personendaten, die zu einer Gefahr von Datenschutzverletzungen für die betroffenen Personen führen.

[2] Die Vorabkonsultation erfolgt in der Regel innert sechs Wochen ab Gesuchseingang, längstens innert zehn Wochen.

[3] Die Fachstelle für Datenschutz kann die Bearbeitungsvorgänge bezeichnen, die ihr vorzulegen sind.

Art. 9 Bearbeitung durch Dritte

[1] Das öffentliche Organ kann die Bearbeitung von Personendaten an Dritte übertragen, wenn die Übertragung nicht durch Gesetz **oder Verordnung** ausgeschlossen ist und die beauftragten Dritten Gewähr für die datenschutzrechtlich einwandfreie Bearbeitung bieten.

[2] Es stellt die Einhaltung des Datenschutzes sicher und legt insbesondere fest, dass die Personendaten:

a) nur so bearbeitet werden, wie das öffentliche Organ es selbst tun dürfte;
b) nach den für das öffentliche Organ geltenden gesetzlichen Bestimmungen bearbeitet werden;
c) vor Verlust und Entwendung sowie unbefugter Kenntnisnahme und unbefugtem Bearbeiten gesichert werden.

[3] Es prüft durch geeignete regelmässige Kontrollen, ob der Datenschutz eingehalten wird. Stellt es die Nichteinhaltung von Auflagen nach Abs. 2 dieser Bestimmung oder Verstösse gegen andere Datenschutzvorschriften fest, macht es die Übertragung rückgängig.

[4] Die Weiterübertragung der Datenbearbeitung bedarf der vorgängigen schriftlichen Zustimmung des auftraggebenden öffentlichen Organs.

Art. 9a (neu) Meldung von Datenschutzverletzungen

[1] Das öffentliche Organ meldet eine Datenschutzverletzung unverzüglich der Fachstelle für Datenschutz, ausser es handelt sich um einen leichten Fall.

[2] Es benachrichtigt die betroffene Person über die Datenschutzverletzung, wenn die Umstände es erfordern oder die Fachstelle für Datenschutz es verlangt.

[3] Wenn öffentliche oder private Geheimhaltungsinteressen überwiegen, kann die Benachrichtigung der betroffenen Person ganz oder teilweise eingeschränkt oder aufgeschoben werden.

[4] Der Dritte, der Personendaten im Auftrag bearbeitet, informiert das auftraggebende öffentliche Organ unverzüglich über eine Datenschutzverletzung.

Art. 10 Archivierung und Vernichtung

[1] Das öffentliche Organ bietet dem zuständigen Archiv von Kanton oder Gemeinde **innert angemessener Frist** die ~~Personaldaten~~**Personendaten** an, die es nicht mehr benötigt. Vorbehalten bleiben besondere Bestimmungen über die Archivierung.

[2] Das öffentliche Organ vernichtet die vom zuständigen Archiv als nicht archivwürdig bezeichneten Personendaten. Ausgenommen sind Personendaten, deren Vernichtung schutzwürdige Interessen der betroffenen Person verletzen könnte.

[3] Auf die Vernichtung kann verzichtet werden, wenn die Personendaten:

a) anonymisiert sind;
b) vom öffentlichen Organ unmittelbar nach Mitteilung des zuständigen Archivs anonymisiert werden.

Art. 10a (neu) ***Bearbeitung durch Justizbehörden und Polizei***

[1] Die Justizbehörden und die Polizei führen ein Verzeichnis ihrer Bearbeitungstätigkeiten.

[2] Das Verzeichnis enthält wenigstens:
a) die Identität des öffentlichen Organs;
b) den Bearbeitungszweck;
c) eine Beschreibung der Kategorien betroffener Personen und der Kategorien bearbeiteter Personendaten;
d) die Kategorien der Empfängerinnen und Empfänger;
e) wenn möglich die Aufbewahrungsdauer der Personendaten oder die Kriterien zur Festlegung dieser Dauer;
f) wenn möglich eine allgemeine Beschreibung der Massnahmen zur Gewährleistung der Datensicherheit;
g) falls die Daten ins Ausland bekanntgegeben werden, die Angabe des Staates und die Garantien bei der Bekanntgabe von Personendaten nach der Bundesgesetzgebung über den Datenschutz.

[3] Bei Bearbeitung von Personendaten im Auftrag enthält das Verzeichnis Angaben zur Identität des Dritten und des auftraggebenden öffentlichen Organs, zu den Kategorien von Bearbeitungen, die im Auftrag des öffentlichen Organs durchgeführt werden, sowie wenn möglich eine allgemeine Beschreibung der Massnahmen zur Gewährleistung der Datensicherheit und falls die Daten ins Ausland bekanntgegeben werden, die Angabe des Staates und die Garantien bei der Bekanntgabe von Personendaten nach der Bundesgesetzgebung über den Datenschutz.

[4] Das öffentliche Organ meldet das Verzeichnis der Fachstelle für Datenschutz.

*Art. 13 Besonders schützenswerte Personendaten**, ~~und~~ Persönlichkeitsprofile* ***und Profiles***

[1] Die Bekanntgabe von besonders schützenswerten Personendaten**,** ~~und~~ Persönlichkeitsprofilen **und Profiles** ist zulässig, wenn:
a) das Gesetz die Bekanntgabe vorsieht oder
b) die betroffene Person eingewilligt hat oder
c) die Bekanntgabe im Interesse der betroffenen Person liegt und deren Einwilligung nicht eingeholt werden kann.

[2] Das öffentliche Organ gibt besonders schützenswerte Personendaten**,** ~~und~~ Persönlichkeitsprofile **und Profiles** einer Behörde des Bundes, eines anderen Kantons oder einem anderen öffentlichen Organ bekannt, wenn die Personendaten für die Empfängerin oder den Empfänger zur Erfüllung einer ihr oder ihm übertragenen gesetzlichen Aufgabe unentbehrlich sind.

Art. 17 Auskunft und Einsicht
a) Grundsatz

[1] Das öffentliche Organ erteilt der betroffenen Person auf **grundsätzlich schriftliches** Gesuch **hin** und gegen Ausweis über die Identität Auskunft, welche Personendaten über sie bearbeitet werden. Die Auskunft erfolgt in der Regel schriftlich.

[2] Es gewährt auf Verlangen der betroffenen Person Einsicht in die Personendaten.

Art. 18 b) Beschränkung

[1] Das öffentliche Organ lehnt Auskunft und Einsicht ab, schränkt sie ein oder verbindet sie mit Auflagen, soweit öffentliche oder schutzwürdige private Interessen Dritter überwiegen **oder ein Gesetz im formellen Sinn dies vorsieht**.

Art. 20 Unrichtige oder widerrechtlich bearbeitete Personendaten

[1] Die betroffene Person hat Anspruch darauf, dass das öffentliche Organ unrichtige Personendaten **kostenlos** berichtigt. Kann weder Richtigkeit noch Unrichtigkeit bewiesen werden, bringt das öffentliche Organ bei den Personendaten einen entsprechenden Vermerk an **und schränkt deren Bearbeitung ein**.

[2] Die betroffene Person hat Anspruch darauf, dass das öffentliche Organ:
a) die widerrechtliche Bearbeitung von Personendaten unterlässt, **unrichtige Daten löscht und deren Bekanntgabe an Dritte sperrt**;
a^{bis}) die Widerrechtlichkeit einer Bearbeitung feststellt;
a^{ter}) die Folgen eines widerrechtlichen Bearbeitens beseitigt;
b) widerrechtlich bearbeitete Personendaten vernichtet.

[3] Das öffentliche Organ informiert Empfängerinnen und Empfänger von unrichtigen oder widerrechtlich bearbeiteten Personendaten über die getroffenen Massnahmen. **Die Information kann unterbleiben, wenn sie nicht oder nur mit unverhältnismässigem Aufwand möglich ist.**

Art. 20a (neu) Informationspflicht bei der Beschaffung von Daten
a) Grundsatz

[1] Das öffentliche Organ informiert die betroffene Person über die Beschaffung von Personendaten bei Amtsstellen oder Dritten.

Art. 20b (neu) b) Beschränkung

[1] Die Informationspflicht entfällt, wenn:
a) die betroffene Person bereits über die Information nach Art. 20a dieses Erlasses verfügt;
b) wenn das Bearbeiten der Personendaten gesetzlich ausdrücklich vorgesehen ist oder
c) die Information nicht oder nur mit unverhältnismässigem Aufwand möglich ist.

[2] Die Übermittlung der Informationen kann unter denselben Voraussetzungen eingeschränkt werden wie das Recht auf Auskunft nach Art. 18 dieses Erlasses.

Art. 28 Personal

[1] Die Regierung wählt die Leiterin oder den Leiter der kantonalen Fachstelle für Datenschutz **für eine Amtsdauer von vier Jahren**. Sie kann ihr oder sein Dienstverhältnis bei Amtspflichtverletzung oder fachlichem Ungenügen **vor Ablauf der Amtsdauer** auflösen. Wahl und Auflösung des Dienstverhältnisses bedürfen der Genehmigung durch das Präsidium des Kantonsrates.

[2] Der Rat ernennt die Leiterin oder den Leiter der Gemeindefachstelle für Datenschutz **für eine Amtsdauer von vier Jahren**. Er kann die Ernennung bei Amtspflichtverletzung oder fachlichem Ungenügen widerrufen. Ernennung und Widerruf bedürfen der Genehmigung durch die Geschäftsprüfungskommission.

[3] Setzen mehrere Gemeinden eine gemeinsame Gemeindefachstelle ein, regeln sie das Verfahren und die Zuständigkeit für die Ernennung der Leiterin oder des Leiters und für den Widerruf sowie die Genehmigung durch ein unabhängiges Organ in der Vereinbarung.

[3bis] Die Leiterin oder der Leiter der Fachstelle für Datenschutz darf kein anderes öffentliches Amt, keine leitende Funktion in einer politischen Partei und keine andere Erwerbstätigkeit ausüben. Die Regierung, in der Gemeinde der Rat, kann davon absehen, wenn dadurch die Unabhängigkeit und die Ausübung der Funktion nicht beeinträchtigt ist.

[4] Die Leiterin oder der Leiter der Fachstelle für Datenschutz stellt im Rahmen des Voranschlags die Mitarbeitenden an ~~und erlässt die das Dienstverhältnis betreffenden Verfügungen~~.

[5] Das Dienstverhältnis der Leiterin oder des Leiters sowie der Mitarbeitenden der kantonalen Fachstelle für Datenschutz richtet sich nach dem ~~Staatsverwaltungsgesetz vom 16. Juni 1994~~[66] **Personalgesetz vom 25. Januar 2011**[67].

Art. 30 Aufgaben

[1] Die Fachstelle für Datenschutz:

a) überprüft auf Anzeige**,** ~~betroffener Personen~~ **von sich aus** ~~und~~**oder** nach dem von ihr aufgestellten Prüfprogramm die Einhaltung der Bestimmungen über den Datenschutz. ~~Kantonsrat und Regierung sowie Gemeindeparlament und Rat sind von der Aufsicht ausgenommen~~; **Der anzeigenden Person ist die Art der Erledigung innert drei Monaten mitzuteilen**;
b) berät öffentliche Organe und betroffene Personen in Fragen des Datenschutzes;
c) kann der Regierung, in Gemeinden dem Rat, den Erlass von Weisungen über technische und organisatorische Massnahmen zur Gewährleistung des Datenschutzes beantragen;
d) nimmt Stellung zum Entwurf von Erlassen, die:
   1. Bestimmungen über den Datenschutz enthalten;
   2. datenschutzerhebliche Sachverhalte regeln;
e) wirkt in Projekten mit, die den Datenschutz betreffen oder Bezüge zum Datenschutz aufweisen~~.~~**;**
f) sensibilisiert die öffentlichen Organe für ihre datenschutzrechtlichen Pflichten und die Öffentlichkeit für die Anliegen des Datenschutzes;
g) arbeitet zur Erfüllung ihrer Aufgaben mit den Organen der anderen Kantone, des Bundes und des Auslands, welche die gleichen Aufgaben erfüllen, zusammen.

[1bis] Von der Aufsicht der Fachstelle für Datenschutz nach Abs. 1 Bst. a dieser Bestimmung sind ausgenommen:
a) Kantonsrat und Regierung sowie Gemeindeparlament und Rat;
b) Datenbearbeitungen in hängigen Verfahren der Zivil-, der Straf- und der gerichtlichen Verwaltungsrechtspflege sowie in hängigen Rechtshilfeverfahren.

[2] Die kantonale Fachstelle für Datenschutz berät die Gemeindefachstellen für Datenschutz.

[3] Sie nimmt vor Erteilung der Bewilligung nach Art. 16a dieses Erlasses Stellung zur beabsichtigten automatisierten Bearbeitung von Personendaten im Pilotversuch.[68]

---

66 ~~sGS 140.1.~~

67 sGS 143.1.

68 Abs. 3 ergänzt durch Drittänderung im Rahmen des Gesetzes über E-Government (22.18.05); vom Kantonsrat erlassen am 19. September 2018; Referendumsvorlage: ABl 2018, 3532 ff.; Ablauf der Referendumsfrist: 19. November 2018.

Art. 30a (neu) Kosten

[1] Die Aufgabenerfüllung der Fachstelle für Datenschutz ist für die betroffene Person in der Regel unentgeltlich.

[2] Die Fachstelle für Datenschutz kann in offensichtlich unbegründeten oder unverhältnismässig häufigen Fällen die Kosten der betroffenen Person überbinden oder nicht tätig werden.

Art. 31 Einsicht in Daten

[1] Die Fachstelle für Datenschutz ist berechtigt, die für die Erfüllung ihrer Aufgaben unentbehrlichen Daten einschliesslich besonders ~~geschützter~~**schützenswerten** Personendaten**, Persönlichkeitsprofilen und Profiles** aus den Datensammlungen des öffentlichen Organs einzusehen.

Art. 35a (neu) Anordnungen

[1] Die kantonale Fachstelle für Datenschutz erlässt bei erheblichen Datenschutzverletzungen eine Verfügung, wenn absehbar ist, dass das öffentliche Organ eine Empfehlung ablehnen oder ihr keine Folge leisten wird.

[2] Das öffentliche Organ kann die Verfügung innert vierzehn Tagen mit Rekurs bei der Verwaltungsrekurskommission anfechten.

II.

1. Der Erlass «Gesetz über Aktenführung und Archivierung vom 19. April 2011»[69] wird wie folgt geändert:

Art. 23 c) durch das abliefernde öffentliche Organ

[1] Das zuständige Archiv gewährt dem öffentlichen Organ, das die Unterlage abgeliefert hat, während der Schutzfrist Zugang, wenn die Unterlage benötigt wird.

[2] Kein Zugang besteht für Archivgut, das nach dem Datenschutzgesetz vom 20. Januar 2009[70] besonders schützenswerte Personendaten**,** ~~oder~~ Persönlichkeitsprofile **oder Profiles** enthält, ausgenommen bei Vorliegen eines überwiegenden öffentlichen Interesses oder bei Zustimmung der betroffenen Person.

[3] Das öffentliche Organ verändert das Archivgut nicht.

69 sGS 147.1.

70 sGS 142.1.

2. Der Erlass «Gesetz über die Verwaltungsrechtspflege vom 16. Mai 1965»[71] wird wie folgt geändert:

Art. 41 b) Verwaltungsrekurskommission
1. als ordentliches Rekursgericht

[1] Bei der Verwaltungsrekurskommission können mit Rekurs angefochten werden:
a) …
b) Arbeitnehmerschutz:
   1. Verfügungen der zum Vollzug des eidgenössischen Arbeitsgesetzes zuständigen Stellen betreffend die Anwendbarkeit des Gesetzes, die Arbeits- und Ruhezeit, den Sonderschutz der jugendlichen und weiblichen Arbeitnehmer und die Betriebsordnung;
   2. Verfügungen der zum Vollzug des Bundesgesetzes über die Heimarbeit zuständigen Stelle;
c) Berufsbildung: Verfügungen des Amtes für Berufsbildung gegenüber Lehrbetrieben und Lehrlingen;
d) Landwirtschaft:
   1. Verfügungen und Einspracheentscheide der für den Vollzug des Bundesgesetzes über die landwirtschaftliche Pacht zuständigen Behörde;
   2. Verfügungen nach Art. 80 und 86 des Bundesgesetzes über das bäuerliche Bodenrecht;
   3. Verfügungen der für den Vollzug der Vorschriften über Investitionskredite, Strukturverbesserungsbeiträge und Betriebshilfe in der Landwirtschaft zuständigen Stellen;
   4. Einspracheentscheide der Meliorationskommission nach Art. 47 des Meliorationsgesetzes;
e) Schätzungen:
   1. Entscheide der zuständigen Gemeindebehörde oder der Schätzungskommission im Kostenverlegungsverfahren nach Strassengesetz;
   2. Verfügungen und Entscheide der zuständigen Stelle der Gemeinde oder des Kantons oder der Schätzungskommission im Kostenverlegungsverfahren nach Wasserbaugesetz;
   3. Verfügungen und Entscheide der Schätzungskommission nach dem Gesetz über die Melioration der Rheinebene und die Errichtung eines Arbeitsbeschaffungskontos;
   4. Verfügungen und Entscheide der zuständigen Behörde bei Landumlegung und Grenzbereinigung nach ~~Art. 116 Abs. 3 Bst. b und Art. 122 Abs. 2 des Baugesetzes~~**Art. 51 Abs. 2 Bst. b des Planungs- und Baugesetzes**;
f) …
g) öffentliche Dienstpflichten:
   1. Verfügungen der Feuerschutzkommission betreffend die Feuerwehrdienstpflicht oder die Ersatzsteuerpflicht;
   2. Verfügungen der Feuerschutzkommission betreffend die Wind- und Feuerwachpflicht;
   3. Verfügungen der für die Festlegung der Wasserwehrpflicht zuständigen Behörde;
g[bis]) Strassenverkehr: Verfügungen der für den Vollzug der Vorschriften der Strassenverkehrsgesetzgebung über Fahrzeuge und Fahrzeugführer zuständigen Behörden;
h) Abgaben:
   1. Verfügungen oder, soweit das Einspracheverfahren vorgesehen ist, Einspracheentscheide der Steuerveranlagungsbehörden, einschliesslich Verfügungen bzw. Einspracheentscheide über Steuerausscheidungen;
   2. Einspracheentscheide des kantonalen Steueramtes betreffend Steuerbezug sowie Verzugszinsen;
   3. Entscheide des Gemeinderates betreffend die Veranlagung zum Feuerwehrdienstersatz;

71 sGS 951.1.

4. Einspracheentscheide der Militärpflichtersatzverwaltung;
5. selbständige Verfügungen und Entscheide der obersten Verwaltungsbehörde einer öffentlich-rechtlichen Körperschaft oder einer selbständigen öffentlich-rechtlichen Anstalt über Gebühren, Taxen, Beiträge und andere öffentlich-rechtliche Geldleistungen Privater sowie über öffentlich-rechtliche Sicherheitsleistungen und Rückerstattungen Privater;
6. Verfügungen des zuständigen Departementes über Perimeterbeiträge an das Rheinunternehmen;
7. Verfügungen des zuständigen Departementes über die Beiträge der Gemeinden nach dem Linthgesetz~~.~~**;**

i) …

j) Datenschutz: Verfügungen der kantonalen Fachstelle für Datenschutz.

Art. 89 Instanzen

[1] Über Rechtsverweigerungsbeschwerden gegen:

a) untere Instanzen einer öffentlich-rechtlichen Körperschaft oder Anstalt entscheidet die oberste Verwaltungsbehörde der Körperschaft oder Anstalt;
b) untere Verwaltungsbehörden des Staates oder oberste Verwaltungsbehörden einer öffentlich-rechtlichen Körperschaft oder Anstalt entscheidet das zuständige Departement;
c) Departemente, Verwaltungsrekurskommission oder Versicherungsgericht, soweit dieses nicht als oberes Gericht zuständig ist, entscheidet das Verwaltungsgericht;

c^{bis}) die Fachstelle für Datenschutz entscheidet die Verwaltungsrekurskommission;

d) …

[2] Weitergezogen werden können:

a) der Entscheid nach Abs. 1 Bst. a dieser Bestimmung mit Rekurs an das zuständige Departement;
b) der Entscheid nach Abs. 1 Bst. b und **Bst. c^{bis} sowie** Abs. 2 Bst. a dieser Bestimmung mit Beschwerde an das Verwaltungsgericht.

III.

[keine Aufhebung anderer Erlasse]

IV.

Die Regierung bestimmt den Vollzugsbeginn dieses Erlasses.