Appenzell Ausserrhoden

Regierungsrat

Regierungsgebäude
9102 Herisau
Tel. 071 353 61 11
Fax. 071 353 68 64
kantonskanzlei@ar.ch
www.ar.ch

Herisau, 28. April 2020

Kantonales Datenschutzgesetz, Teilrevision

Erläuternder Bericht zum Vernehmlassungsentwurf

A. Ausgangslage

1. Entwicklung auf internationaler Ebene

Auf internationaler Ebene wird dem Datenschutz immer grössere Beachtung geschenkt. So hat die Europäische Union am 27. April 2016 ihre Datenschutzgesetzgebung revidiert. Diese umfasst zwei Rechtsakte: Zum einen die Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (nachfolgend: Datenschutz-Grundverordnung [DSGVO]) und zum anderen die Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten im Bereich des Strafrechts (nachfolgend: Richtlinie (EU) 2016/680). Die Datenschutz-Grundverordnung ist am 25. Mai 2016 und die Richtlinie (EU) 2016/680 am 5. Mai 2016 in Kraft getreten.

Die Schweiz ist gemäss Artikel 2 Absatz 3 des Schengen-Assoziierungsabkommens grundsätzlich verpflichtet, jede Weiterentwicklung des Schengen-Besitzstands zu akzeptieren, umzusetzen und anzuwenden. Nur die Richtlinie (EU) 2016/680 ist Teil des Schengen-Besitzstands. Die Datenschutz-Grundverordnung ist in der Schweiz nicht direkt anwendbar, jedoch ist sie insofern von Bedeutung, als dass die Europäische Kommission gestützt darauf entscheidet, ob Drittstaaten – wie die Schweiz – ein angemessenes Datenschutzniveau vorweisen können.

Der Europarat wiederum hat einen Entwurf für eine Revision der Konvention SEV 108 zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten ausgearbeitet. Die revidierte Konvention SEV 108 wurde am 18. Mai 2018 vom Ministerkomitee des Europarats verabschiedet. Inzwischen liegt sie mit Datum vom 10. Oktober 2018 als SEV 223 in der deutschen Endfassung vor. Da die Schweiz bereits Vertragspartei der Vorgänger-Konvention von 1981 ist, beabsichtigt der Bundesrat, dem Parlament auch das Änderungsprotokoll der Konvention zur Genehmigung vorzulegen. Bevor die revidierte Konvention ratifiziert werden kann, muss das schweizerische Recht den neuen Bestimmungen entsprechend angepasst werden.

Auf Bundesebene war der Datenschutz in den vergangenen Jahren vermehrt Gegenstand zahlreicher parlamentarischer Interventionen. Da der politische Wille besteht, die Bundesgesetzgebung in diesem Bereich zu stärken, unterzieht der Bund derzeit das Bundesgesetz über den Datenschutz (DSG-Bund) einer Totalrevision. Die bundesrechtlichen Gesetzgebungsarbeiten beruhen auf einem Bundesratsbeschluss, wonach eine Vorlage mit zwei Zielsetzungen ausgearbeitet werden soll: Einerseits sollen die Schwächen des Datenschutzgesetzes behoben werden, die aufgrund der rasanten technologischen Entwicklung entstanden sind. Andererseits soll den Entwicklungen auf der Ebene des Europarats und der EU Rechnung getragen werden.

Die künftige Gesetzgebung soll die Anforderungen der Richtlinie (EU) 2016/680 übernehmen, damit die Schweiz auch in Zukunft ihren Schengen-Verpflichtungen nachkommen kann. Darüber hinaus soll die Vorlage mit der SEV 223 vereinbar sein, damit die Schweiz das revidierte Übereinkommen so rasch als möglich ratifizieren kann. Zudem werden die Empfehlungen umgesetzt, welche die EU der Schweiz im Jahr 2014 im Rahmen der Schengen-Evaluation zukommen liess. Dabei wurde insbesondere empfohlen, die Kompetenzen des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) auszubauen. Schliesslich soll sich die schweizerische Datenschutzgesetzgebung insgesamt den Anforderungen der Datenschutz-Grundverordnung annähern. Diese Annäherung bildet – zusammen mit der Ratifizierung der revidierten Konvention SEV 223 – die zentrale Voraussetzung dafür, dass die Europäische Kommission der Schweiz in einem Angemessenheitsbeschluss weiterhin bestätigt, dass die schweizerische Gesetzgebung einem angemessenen Datenschutzniveau entspricht.

Im Sommer 2018 hat sich der Nationalrat für eine Etappierung der Revision des DSG-Bund ausgesprochen. Der Ständerat ist diesem Anliegen in der Herbstsession gefolgt. Bereits am 28. September 2018 hat der Bund ein Bundesgesetz über die Umsetzung der Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung (Weiterentwicklung des Schengen-Besitzstands) sowie darin enthalten (Anhang Ziff. 1^{bis}) das umfassende Bundesgesetz über den Datenschutz im Rahmen der Anwendung des Schengen-Besitzstands in Strafsachen (Schengen-Datenschutzgesetz, SDSG) verabschiedet. Mit diesem Vorgehen wird sichergestellt, dass die Schengen-Anforderungen (Richtlinie [EU] 2016/680) schnellstmöglich eingehalten werden. Zwischenzeitlich ist die Referendumsfrist des SDSG unbenutzt abgelaufen. Der Bundesrat hat das neue Bundesgesetz auf den 1. März 2019 in Kraft gesetzt.

Die Übernahme der Richtlinie (EU) 2016/680 und die Annahme des Änderungsprotokolls zur Konvention SEV 223 durch die Schweiz sind auch für die Kantone bindend. Diese müssen ihre kantonalen Gesetzgebungen insoweit anpassen, als sie die Anforderungen dieser Instrumente nicht erfüllen.

Betreffend die Übernahme der Richtlinie (EU) 2016/680 gilt für die Schweiz eine Umsetzungsfrist von zwei Jahren ab dem Zeitpunkt der Notifikation durch die Europäische Union. Da diese am 1. August 2016 erfolgte, hätte die Datenschutzreform sowohl vom Bund als auch von den Kantonen bis zum 1. August 2018 umgesetzt werden müssen. Eine fristgerechte Umsetzung war unter Einhaltung des ordentlichen Gesetzgebungsprozesses aber unrealistisch. Eine Inkraftsetzung des revidierten kantonalen Datenschutzgesetzes (kDSG) im Laufe des Jahres 2022 ist realistisch und anzustreben.

2. Handlungsbedarf

2.1 Richtlinie (EU) 2016/680

Die Richtlinie (EU) 2016/680 ist darauf ausgerichtet, personenbezogene Daten zu schützen, die zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschliesslich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, bearbeitet werden. Sie soll ein hohes Schutzniveau für personenbezogene Daten gewährleisten und gleichzeitig aber den Austausch dieser Daten zwischen den zuständigen Behörden der verschiedenen Schengen-Staaten erleichtern. Sie gilt sowohl für grenzüberschreitende Datenbearbeitungen als auch für Datenbearbeitungen, die von den Polizei- und Justizbehörden ausschliesslich auf innerstaatlicher Ebene durchgeführt werden.

Die wichtigsten **Neuerungen** sind:

- Ausnahmen vom Anwendungsbereich sind in der Richtlinie (EU) 2016/680 nicht vorgesehen. Sie gilt für alle Datenbearbeitungen, die von den Polizei- und Justizbehörden durchgeführt werden.
- Die verschiedenen Kategorien betroffener Personen müssen unterschieden sowie Regeln zur Unterscheidung der Daten und zur Überprüfung der Qualität der Daten eingeführt werden.
- Neue Rechte für die betroffene Person sind vorzusehen. So ist die bzw. der Verantwortliche verpflichtet, die Datenbearbeitung einzuschränken, wenn die betroffene Person die Richtigkeit der Daten bestreitet und die Richtigkeit nicht festgestellt werden kann.
- Im Sinne der Pflichten des für die Datenbearbeitung Verantwortlichen und des Auftragsbearbeitenden führt die Richtlinie (EU) 2016/680 in Kapitel IV. die beiden Grundsätze Datenschutz durch Technikgestaltung („privacy by design“) und Datenschutz durch datenschutzfreundliche Voreinstellungen („privacy by default“) ein.
- Die für die Datenbearbeitung Verantwortlichen sind verpflichtet, vor bestimmten Bearbeitungen eine Datenschutz-Folgenabschätzung durchzuführen und gegebenenfalls die Aufsichtsbehörde zu konsultieren.
- Es besteht die Pflicht, in gewissen Fällen der Aufsichtsbehörde eine Verletzung des Datenschutzes zu melden und gegebenenfalls die betroffene Person zu benachrichtigen.
- Die Europäische Kommission prüft das Schutzniveau, das ein Drittland, ein Gebiet oder ein Verarbeitungssektor in einem Drittland bietet. Hat die Europäische Kommission die Angemessenheit des Schutzniveaus in einem Drittstaat nicht durch Beschluss festgestellt, darf die Datenübermittlung nur erfolgen, wenn geeignete Garantien bestehen oder wenn in bestimmten Fällen eine Ausnahme vorliegt.
- Die Schengen-Staaten müssen im Bereich des Datenschutzes unabhängige Aufsichtsbehörden einsetzen. Diese Behörde ist aber nicht für die Aufsicht über Datenbearbeitungen zuständig, die Gerichte im Rahmen ihrer justiziellen Tätigkeit vornehmen. Die Schengen-Staaten können auch eine Ausnahme der Aufsichtsbefugnis für jene Datenbearbeitungen vorsehen, die durch andere unabhängige Justizbehörden im Rahmen ihrer justiziellen Tätigkeit erfolgen.
- Die unabhängige Aufsichtsbehörde muss über wirksame Untersuchungsbefugnisse verfügen, d.h. sie muss zumindest vom Verantwortlichen und vom Auftragsbearbeitenden Zugang zu den bearbeiteten Daten und allen Informationen erhalten, die zur Erfüllung ihrer Aufgaben notwendig sind.
- Die Aufsichtsbehörde soll auch über wirksame Befugnisse verfügen, um gegen rechtswidrige Datenbearbeitungen wirksam vorgehen zu können. Es sind dies beispielsweise die Befugnis zur Verwarnung eines Verantwortlichen oder eines Auftragsbearbeitenden, zur Anordnung von vorschriftsgemässen Bearbeitungen, gegebenenfalls durch Berichtigung oder Löschung der Daten, sowie zur Verhängung einer vorübergehenden oder endgültigen Beschränkung der Bearbeitung, einschliesslich eines Verbots.
- Die betroffene Person hat das Recht auf Beschwerde bei der Aufsichtsbehörde. Die betroffene Person hat auch das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen einen sie betreffenden Entscheid der Aufsichtsbehörde. Da die Richtlinie (EU) 2016/680 sowohl für die Mitgliedstaaten der EU als auch für die Schweiz nicht direkt anwendbar ist, bedarf es einer Umsetzung in das jeweilige nationale Recht. In der Schweiz braucht es zur Umsetzung der Richtlinie (EU) 2016/680 nicht nur Anpassungen des DSG-Bund und verschiedener Bundesgesetze, sondern aufgrund der unterschiedlichen Zuständigkeiten im Bereich der Datenschutzgesetzgebung auch der kantonalen Datenschutzgesetze und verschiedener kantonaler Erlasse.

2.2 Datenschutzkonvention SEV 223

Mit der revidierten SEV 223 wird der Datenschutz auf internationaler Ebene vereinheitlicht und verbessert. Dies verstärkt auch den Schutz der Schweizer Bürgerinnen und Bürger, wenn ihre Personendaten im Ausland bearbeitet werden. Die Bekanntgabe von Daten zwischen den Vertragsparteien wird zudem vereinfacht, wodurch Schweizer Unternehmen einen besseren Zugang zu den Märkten dieser Länder erhalten. Die Unterzeichnung des Änderungsprotokolls zur SEV 223 dürfte zudem eine zentrale Voraussetzung sein, damit die Europäische Union der Schweiz erneut ein angemessenes Datenschutzniveau bestätigt. Nur dadurch bleibt der Zugang zum europäischen Markt weiterhin uneingeschränkt gewährleistet. Die Vertragsparteien müssen die SEV 223 auf alle Datenbearbeitungen in ihrer Rechtsordnung im öffentlichen und privaten Sektor anwenden. Nicht durch diesen Entwurf geregelt werden nur Datenbearbeitungen, die eine Person ausschliesslich im Rahmen von persönlichen oder familiären Tätigkeiten vornimmt.

Der Bundesrat hat in mehreren Antworten auf parlamentarische Vorstösse zum Ausdruck gebracht, dass er die Modernisierung der SEV 223 unterstützt. Die Ratifizierung steht noch aus, denn zusammen mit dieser müssen die erforderlichen Massnahmen zur Umsetzung der Bestimmungen gemäss SEV 223 in Kraft treten.

Die **wesentlichsten Punkte** in der SEV 223 sind:

- Die Vertragsparteien sind verpflichtet, die SEV 223 grundsätzlich auf alle Datenbearbeitungen anzuwenden.
- Die Pflichten des für die Datenbearbeitung Verantwortlichen werden ausgeweitet, indem der zuständigen Aufsichtsbehörde bestimmte Verstösse gegen den Datenschutz zu melden sind. Die Informationspflichten gegenüber der betroffenen Person werden ausgeweitet; so müssen die für die Datenbearbeitung Verantwortlichen zusätzliche Informationen zur Datenbearbeitung als auch zu automatisierten Einzelentscheidungen abgeben. Zudem sind im Vorfeld bestimmter Datenbearbeitungen eine Datenschutz-Folgenabschätzung vorzunehmen und die beiden Grundsätze Datenschutz durch datenschutzfreundliche Technikgestaltung («privacy by design») und Datenschutz durch datenschutzfreundliche Voreinstellungen («privacy by default») anzuwenden.
- Der von der Datenbearbeitung betroffenen Person ist das Recht einzuräumen, nicht einer Entscheidung unterworfen zu sein, die ausschliesslich auf der Grundlage einer automatisierten Bearbeitung ihrer Daten ergeht, ohne dass die betroffene Person ihren Standpunkt geltend machen kann. Das Auskunftsrecht der betroffenen Person wird erweitert und die Bedingungen für deren Einwilligung in die Datenbearbeitung werden klar definiert.
- Die Vertragsparteien sind verpflichtet, ein Sanktionen- und ein Rechtsmittelsystem festzulegen.
- Personendaten dürfen nur in einen Drittstaat übermittelt werden, wenn ein angemessener Schutz gewährleistet ist. Ein angemessenes Datenschutzniveau kann durch Rechtsvorschriften des betreffenden Staates oder der empfangenden internationalen Organisation oder durch bestimmte Sicherheiten gewährleistet werden. Wenn kein angemessenes Schutzniveau garantiert ist, dürfen Daten an einen Drittstaat nur weitergegeben werden, wenn der Betroffene gültig eingewilligt hat oder wenn ein bestimmter Ausnahmefall vorliegt. Schliesslich müssen die Vertragsparteien gemäss der SEV 223 vorsehen, dass die Aufsichtsbehörde vom Organ, welches die Daten weitergibt, den Nachweis über die Wirksamkeit der aufgestellten Sicherheiten verlangen und die Datenweitergabe gegebenenfalls verbieten oder aussetzen kann.

- Die Vertragsparteien sind verpflichtet, eine unabhängige Aufsichtsbehörde zu schaffen. Die Aufsichtsbehörden müssen ermächtigt werden, verbindliche, anfechtbare Entscheidungen zu fällen und verwaltungsrechtliche Sanktionen zu verhängen. Der Aufsichtsbehörde muss auch der Auftrag erteilt werden, die Öffentlichkeit und die für die Bearbeitung Verantwortlichen für den Datenschutz zu sensibilisieren.

2.3 Datenschutz-Grundverordnung

Die Datenschutz-Grundverordnung ist der grundlegende Datenschutzerlass auf Ebene der EU. Sie gehört nicht zum Schengen-Besitzstand. Die Richtlinie (EU) 2016/680 und die Verordnung sehen weitgehend übereinstimmende Regelungen vor. Allerdings ist die Verordnung detaillierter, während die Bestimmungen der Richtlinie (EU) 2016/680 auf die Bedürfnisse der Strafbehörden ausgerichtet sind. Die Datenschutz-Grundverordnung regelt hauptsächlich den Schutz von Personen, deren Daten im Rahmen des Binnenmarkts bearbeitet werden, doch sie gilt auch für den öffentlichen Sektor. Sie enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.

Für die Schweiz sind die Bestimmungen der Datenschutz-Grundverordnung mangels Schengenrelevanz nicht verbindlich. Der Geltungsbereich ist sehr weit gefasst, indem sich die Verordnung gleichermassen an Unionsbehörden wie Private richtet. Damit setzt sie verbindliche Minimal-Standards, die bei der Anwendung der beiden anderen Rechtserlasse im öffentlich-rechtlichen wie auch privatrechtlichen (wirtschaftlichen) Bereich (Binnenmarkt) zu beachten sind. Demnach ist sie auch für die Schweiz von Bedeutung. Gemäss Beschluss der Europäischen Kommission vom 26. Juli 2000 besteht in der Schweiz ein angemessenes Datenschutzniveau. Dieser Beschluss kann jedoch jederzeit widerrufen werden. Wenn die Schweiz erneut einen Angemessenheitsbeschluss der Europäischen Union erlangen will, muss sie ihre Gesetzgebung an die europäischen Anforderungen anpassen. Die in der Datenschutz-Grundverordnung festgelegten Kriterien sind künftig massgebend für die Beurteilung, ob die schweizerische Gesetzgebung einen angemessenen Datenschutz gewährleistet. Das kantonale Datenschutzrecht soll daher auch ein angemessenes Schutzniveau im Sinn der Verordnung garantieren.

2.4 Fazit

Die gesetzgeberischen Tätigkeiten und die Rechtsprechung auf europäischer Ebene wirken sich sowohl auf das Bundesrecht als auch auf kantonales Recht aus. In verschiedenen Bereichen liegt dabei die Rechtsetzungszuständigkeit beim Bund. Er hat die notwendigen Änderungen des DSG-Bund, das die Datenbearbeitungen durch Private und öffentliche Organe des Bundes regelt, und der bundesrechtlichen Spezialgesetzgebung (z.B. Migrationsrecht, Zivilrecht etc.) vorzunehmen. Bei der Bearbeitung von Personendaten durch kantonale und kommunale öffentliche Organe gelten die kantonalen Datenschutzbestimmungen. Im Kanton Appenzell Ausserrhoden steht die Anpassung des Datenschutzgesetzes, das die Bearbeitung von Personendaten durch kantonale und kommunale Organe regelt, aus. Insbesondere durch die Erweiterung des Anwendungsbereichs, die Einführung von neuen Begrifflichkeiten und der Erhöhung des Detaillierungsgrads der Bestimmungen im Datenschutz-Reformpaket der EU und des Europarats müssen Ergänzungen und Präzisierungen vorgenommen werden.

3. Umsetzung

3.1 Bund

Auf Bundesebene ist, wie erwähnt, zur schnellstmöglichen Einhaltung der Schengen-Anforderungen bislang insbesondere das umfangreiche SDSG erlassen worden. Die Referendumsfrist für das SDSG ist am 17. Januar 2019 unbenutzt abgelaufen. Im nächsten Schritt wird das Datenschutzgesetz des Bundes totalrevidiert.

3.2 Kanton Appenzell Ausserrhoden

Der unmittelbare Handlungsbedarf wurde eruiert und gestützt darauf wurde in enger Zusammenarbeit mit dem Datenschutzkontrollorgan die vorliegende Teilrevision ausgearbeitet, welche sich auf das Notwendigste beschränkt, um die Kontinuität der Rechtsordnung möglichst weitgehend zu wahren. Dabei orientiert sich die Vorlage am Anpassungsbedarf, der sich aufgrund der EU-Datenschutzreform und den Änderungen der Konvention SEV 223 des Europarates ergibt. Ein nennenswerter Spielraum bei der nun gewählten Form der Beschränkung der Teilrevision des kantonalen Datenschutzgesetzes auf die Umsetzung der EU-Datenschutzreform und die Änderungen der Konvention SEV 223 des Europarates besteht darum nicht.

Der Revisionsentwurf modernisiert die verwendete Terminologie, um die Vereinbarkeit mit dem europäischen Recht zu verbessern. So werden gewisse Begriffe aus dem europäischen Recht übernommen. Der Begriff „Persönlichkeitsprofil“, der eine schweizerische Besonderheit darstellt, wird beibehalten; zusätzlich wird der Begriff des „Profiling“ aufgenommen. Der Begriff „besonders schützenswerte Personendaten“ wird um „die ethnische Herkunft sowie genetische oder biometrische Daten“ erweitert.

Um Kollisionen zwischen den verfahrensrechtlichen und den datenschutzrechtlichen Informationsansprüchen der Parteien bzw. der betroffenen Personen zu vermeiden, ist festzustellen, dass sich die Rechte und Ansprüche der betroffenen Personen in Verfahren nach dem anwendbaren Verfahrensrecht richten.

Die Pflichten der verantwortlichen Organe werden präzisiert und stärker auf den Schutz der betroffenen Person ausgerichtet. So wird die Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung neu ausdrücklich im Gesetz festgehalten. Zudem sollen sie mit technischen Vorkehrungen („privacy by design“) und Voreinstellungen („privacy by default“) für eine datenschutzfreundliche Ausgestaltung der Systeme sorgen. Diese Anforderungen werden ebenfalls in das Datenschutzgesetz aufgenommen.

Die zwingenden Vorgaben des EU-Rechts (insbesondere auch der Europaratskonvention SEV 223) verlangen zudem eine Stärkung der Kontrolle durch die Datenschutzstelle. Diese Aufwertung der Position des Datenschutz-Kontrollorgans ist in Art. 27b Abs. 1 statuiert.

B. Erläuterungen zur Teilrevision des kantonalen Datenschutzgesetzes

Art. 2 Begriffe

In Art. 2 des kantonalen Datenschutzgesetzes werden die Begriffe umschrieben. Das kantonale Datenschutzgesetz ist anwendbar, wenn ein öffentliches Organ öffentliche Aufgaben erfüllt. Umgekehrt ist damit klargestellt, dass das Bundesgesetz über den Datenschutz zur Anwendung kommt, wenn ein öffentliches Organ am wirtschaftlichen Wettbewerb teilnimmt und folglich privatrechtlich handelt.

Anpassungen sind in Abs. 3 nötig. In lit. b von Abs. 3 ist der Bereich der besonders schützenswerten Personendaten umschrieben. Lit. b in der bisherigen Fassung ordnete u.a. die „Rassenzugehörigkeit“ diesen besonders geschützten Daten zu. Dieser Ausdruck wird abgelöst durch den umfassenderen Begriff der „ethnischen Herkunft“. Neu werden auch „die genetischen und biometrischen Daten“ diesem besonders geschützten Bereich zugewiesen. Genetische Daten können eindeutige Informationen über das Aussehen oder die Gesundheit einer Person liefern. Soweit sich solche Daten auf bestimmte oder bestimmbare Personen beziehen, sollen sie besonders schützenswerte Personendaten im Sinne des Gesetzes sein. Biometrische Daten sind mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer Person, welche die eindeutige Identifizierung ermöglichen oder bestätigen. Dabei gilt es festzuhalten, dass keineswegs jedes Foto unter die Definition im Sinne des Gesetzes fällt.

In lit. c sind die heute aktuellen Begriffe zu verwenden, also statt der fürsorgerischen bzw. vormundschaftlichen die Verfahren und Massnahmen des Kindes- und Erwachsenenschutzes, ebenso diejenigen der Sozialhilfe.

In Abs. 5^{bis} wird neu das „Profiling“ als besondere Art des Bearbeitens von Personendaten definiert: Profiling ist jede Art der automatisierten Verarbeitung von Personendaten, die darin besteht, dass diese Daten verwendet werden, um bestimmte persönliche Aspekte einer Person zu bewerten. Insbesondere kann Profiling dazu dienen, die Arbeitsleistung, die wirtschaftlichen Verhältnisse, die Gesundheit, die persönlichen Vorlieben und Interessen, das Verhalten (z.B. das Bewegungsverhalten) oder der Aufenthaltsort einer bestimmten natürlichen Person zu analysieren oder vorherzusagen. Als automatisierte Auswertung gilt jede Auswertung mit Hilfe computergestützter Analysetechniken, mit oder ohne Algorithmen. Das Profiling stellt einen besonderen Datenbearbeitungsvorgang dar: Aus dem "Datenbild" einer Person wird eine Schlussfolgerung mit Bezug auf persönliche Aspekte einer Person gezogen. Soweit die aufgrund eines Profiling entstandenen Daten Personendaten oder besonders schützenswerte Personendaten sind, gelangt das Datenschutzgesetz zur Anwendung; dient es zur Erzeugung von anonymen Daten, sind die Resultate des Profiling nicht datenschutzrelevant.

Art. 3 Geltungsbereich

Art. 3 Abs. 1 ist anzupassen. Neu wird statuiert, dass dieses Gesetz gilt, soweit nicht eidgenössisches (wie bisher) oder besonderes kantonales Recht vorgeht. Hierbei ist zu beachten, dass mittlerweile neben dem allgemeinen Datenschutzgesetz zahlreiche bereichsspezifische Normen den Umgang mit Daten und Informationen regeln (zum Beispiel im Polizeigesetz (bGS 521.1) oder im Bereich des Gesundheitswesens).

Zudem wird der Vorbehalt in Abs. 2 auch auf den mit dieser Teilrevision ergänzten Art. 15 ausgedehnt.

Art. 4 Zulässigkeit der Bearbeitung
Die Präzisierung in Art. 4 Abs. 1 ist nötig, um klarzustellen, dass die Datenbearbeitung nicht nur inhaltlich, sondern auch zeitlich nur solange zulässig ist, wie dies für die Erfüllung einer gesetzlichen Aufgabe erforderlich ist und nicht länger. Zudem wird in Abs. 2 statuiert, dass für jedes Profiling ein Gesetz im formellen Sinn notwendig ist.

Art. 7 Informationspflicht
Die Marginalie von Art. 7 wird umbenannt. Ging es bei der aktuellen Bestimmung um die Beschaffung und Bearbeitung von Daten und die Erkennbarkeit der Beschaffung für die betroffenen Personen, wird neu der Spiess umgekehrt und die Organe sind verpflichtet, die betroffenen Personen grundsätzlich aktiv zu informieren (Marginalie und Abs. 1). Verlangt wird vom Europäischen Recht eine aktive Information nicht mehr nur beim Bearbeiten von besonders schützenwerten Personendaten, sondern über das Beschaffen von Personendaten allgemein.

Abs. 2 setzt den „Mindeststandard" der die Informationspflicht umfassenden Angaben fest. Diese ergeben sich u.a. aus Art. 13 der Richtlinie (EU) 2016/680.

Das geltende Recht sieht in Art. 7 Abs. 3 vor, dass eine Information über die Datenbearbeitung auf Ersuchen der betroffenen Person bekannt gegeben wird. Neu wird eine aktive Information über das Beschaffen von Daten verlangt. Dabei ist nach Abs. 2 das öffentliche Organ als Datenbearbeiter mit den Kontaktdaten zu bezeichnen, die Rechtsgrundlage der Datenbearbeitung, deren Zweck, die Kategorien der zu bearbeitenden Daten sowie der Empfängerkreis zu bezeichnen; ferner sind die Kontaktdaten des Datenschutz-Kontrollorgans bekannt zu geben.

Diese Informationspflicht entfällt gemäss Abs. 3, wenn die betroffenen Personen bereits über die entsprechenden Informationen verfügen oder wenn die Datenbearbeitung in einer Rechtsgrundlage (Gesetz oder Verordnung) vorgesehen ist. Schliesslich entfällt die Informationspflicht auch, wenn die Information der betroffenen Personen nur mit unverhältnismässigem Aufwand möglich wäre oder überwiegende öffentliche Interessen dagegen sprechen.

Art. 7a (neu) Datenschutz-Folgenabschätzung
Die übergeordneten Rechtsgrundlagen der Richtlinie (EU) 2016/680 (Art. 27) und der SEV 223 (Art. 10 Ziff. 2) verlangen eine Datenschutz-Folgenabschätzung durch das verantwortliche öffentliche Organ. Diese Abschätzung enthält mindestens eine allgemeine Beschreibung der geplanten Bearbeitungsvorgänge, eine Bewertung der in Bezug auf die Grundrechte der betroffenen Personen bestehenden Risiken sowie eine Darstellung und Bewertung der geplanten Abhilfemassnahmen, Garantien, Sicherheitsvorkehren und Verfahren; dadurch soll der Schutz der Grundrechte der betroffenen Personen sichergestellt und der Nachweis erbracht werden, dass das Datenschutzgesetz eingehalten wird. Die Datenschutz-Folgenabschätzung ist somit nichts anderes als die Vorbereitung des verantwortlichen Organs, damit es die Voraussetzungen für den Nachweis der Einhaltung der Datenschutzvorschriften erbringen kann. Die Umsetzung dieser Grundsätze wird in Art. 7a Abs. 1 festgehalten.

Art. 28 der Richtlinie (EU) 2016/680 sieht vor, dass bestimmte Vorhaben dem Datenschutzbeauftragten vorab zur Konsultation (oder Vorabkontrolle) zu unterbreiten sind.
Dazu gehören Vorhaben, bei denen in einer Datenschutz-Folgenabschätzung ein hohes Risiko festgestellt wurde, Vorhaben, bei denen die Form der Datenbearbeitung (insbesondere bei Verwendung neuer Technolo-

gien, Mechanismen oder Verfahren) ein hohes Risiko für die Grundrechte der betroffenen Personen darstellen können (vgl. die neue Formulierung in Art. 27 Abs. 1 lit. e kDSG). Das Datenschutz-Kontrollorgan muss eine Liste der Bearbeitungsvorgänge erstellen können, die vorab zur Konsultation zu unterbreiten sind. Kriterien dafür können etwa die Zahl der erfassten Personen, die Zahl der beteiligten öffentlichen Organe oder die Sensitivität der Daten sein (vgl. Art. 28 Abs. 3 der Richtlinie (EU) 2016/680). Dies wird in Art. 7a Abs. 2 festgehalten.

Zweck dieser Vorabkonsultation ist es, den Datenschutz rechtzeitig sicherzustellen. Es soll dafür gesorgt werden, dass die verfassungs- und datenschutzrechtlichen Vorgaben berücksichtigt werden. Bei anderen Vorhaben soll die Ermittlung und Bewertung der Risiken und der geplanten Massnahmen überprüft werden, damit die Risiken auf ein zulässiges Mass reduziert werden können, indem rechtliche, organisatorische oder technische Massnahmen umgesetzt werden. Das Datenschutz-Kontrollorgan soll bei entsprechenden Vorhaben vor der Umsetzung beigezogen werden und Stellung nehmen können. Die Vorabkonsultation ist ein wirksames Mittel des präventiven Datenschutzes und verhindert, dass entsprechende Vorhaben im Nachhinein mit grösserem Aufwand verbessert werden müssen oder gar nicht in Betrieb genommen werden können.

Art. 15 Bearbeitung durch Drittpersonen
Die bestehende Regelung in Art. 15 Abs. 1 für Datenbearbeitungen durch Drittpersonen wird dahingehend ergänzt, dass sichergestellt werden muss, dass die Personendaten nur so bearbeitet werden, wie es das öffentliche Organ tun dürfte.
In Abs. 2 wird statuiert, dass das öffentliche Organ sich vergewissern muss, dass die Drittperson auch in der Lage ist, die Datensicherheit zu gewährleisten. Dies geschieht auch im eigenen Interesse des öffentlichen Organs, es bleibt nämlich für den Umgang mit den Informationen auch nach der Übertragung verantwortlich.
In Abs. 3 wird neu festgehalten, dass die Weiterübertragung einer Datenbearbeitung der vorgängigen schriftlichen Zustimmung des auftragsgebenden öffentlichen Organs bedarf.

Art. 16a Meldung von Verletzungen der Datensicherheit
Eine Verletzung der Datensicherheit ist unverzüglich dem Datenschutz-Kontrollorgan zu melden, sofern es sich nicht um einen leichten Fall handelt. Eine solche Verletzung der Datensicherheit liegt dann vor, wenn bearbeitete Personendaten vernichtet werden, verloren gehen, unrechtmässig verändert oder offenbart werden oder unbefugte Personen Zugang zu solchen Personendaten erhalten. Das verantwortliche Organ benachrichtigt ausserdem in Absprache mit dem Datenschutz-Kontrollorgan die betroffene Person, wenn die Umstände es erfordern, d.h. dies zum Schutz der Person nötig ist. Die Benachrichtigung der betroffenen Person kann ganz oder teilweise eingeschränkt oder auf die Information verzichtet werden, wenn öffentliche oder private Geheimhaltungsinteressen überwiegen.

Für den Fall der Auftragsdatenbearbeitung ist Folgendes zu berücksichtigen: Falls die Verletzung bei einer Auftragsdatenbearbeitung geschieht, hat der Datenbearbeiter unverzüglich das auftraggebende öffentliche Organ zu benachrichtigen. Dieses meldet die Verletzung dem Datenschutz-Kontrollorgan.

Art. 25 Verfahren
In Abs. 1 erfolgt eine Präzisierung, indem die Gesuche auf die Art. 21 bis Art. 24 (bisher Art. 25) eingeschränkt werden, da Art. 25 ja das Verfahren regelt.
Die bisherigen Abs. 2 bis 4 werden zugunsten eines neuen Abs. 2 aufgehoben. Da das Verwaltungsrechtspflegegesetz aus dem Jahre 2002 stammt und somit jünger ist als das kantonale Datenschutzgesetz, war ein sol-

cher Verweis zum Zeitpunkt der Erarbeitung des kDSG nicht möglich. Mit dem neuen allgemeinen Hinweis auf das Gesetz über die Verwaltungsrechtspflege (bGS 143.1) erübrigen sich die (unvollständigen) Hinweise zum Verfahren. Zusätzlich wird an dieser Stelle statuiert, dass das Datenschutz-Kontrollorgan zur Erhebung von Rechtsmitteln berechtigt ist (bisher Art. 27 Abs. 4).

Art. 26 Datenschutz-Kontrollorgan
Abs. 1 Satz 1 entspricht weitgehend dem bisherigen Recht; ergänzt wird dieser Satz mit dem Hinweis, dass die Wahl nur auf eine ausgewiesene Fachperson fallen kann. Neu wird explizit statuiert, dass die Wahl auf eine Amtsdauer von vier Jahren erfolgt, was praxisgemäss schon bisher der Fall war (neu Satz 2 von Abs. 1). Wiederwahlen sind zulässig.

Aufgrund von Art. 42 Abs. 3 der Richtlinie (EU) 2016/680 wird in Art. 26 Abs. 1^{bis} neu geregelt, dass das Datenschutz-Kontrollorgan keine andere öffentliche oder private Tätigkeit ausüben darf, welche die Unabhängigkeit oder das Ansehen des Amtes beinträchtigen könnte.

Art. 27 Aufgaben des Datenschutz-Kontrollorgans
Abs. 1 lit. a sieht wie bisher vor, dass das Datenschutz-Kontrollorgan die Einhaltung der Vorschriften über den Datenschutz überwacht. Damit ist die unabhängige, anlassfreie Prüfung nach einem durch das Datenschutz-Kontrollorgan autonom aufgestellten Prüfprogramm umschrieben. Erfasst ist damit auch die ohne Anlass durchgeführte Kontrolle einer konkreten Datenbearbeitung, beispielsweise aufgrund einer „Beschwerde“.

Abs. 1 lit. b sieht ebenfalls wie bisher die Beratung der betroffenen Personen über ihre Rechte vor. Neu hinzu kommt die Information der Öffentlichkeit über den Datenschutz als explizite Aufgabe des Datenschutz-Kontrollorgans. Dies ist namentlich im Hinblick auf die zunehmende Eigenverantwortung der betroffenen Personen in einer digitalisierten Welt wichtig.

Das Datenschutz-Kontrollorgan behandelt ferner gemäss Abs. 1 lit. c Anzeigen betreffend die Verletzung von Datenschutzvorschriften. Jede Person hat, unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs, die Möglichkeit einer datenschutzrechtlichen Anzeige beim Datenschutz-Kontrollorgan, wenn sie der Ansicht ist, dass die Bearbeitung der sie betreffenden Personendaten gegen die datenschutzrechtlichen Vorschriften verstösst.

Gemäss Abs. 1 lit. d kann das Datenschutz-Kontrollorgan Empfehlungen abgeben, und es berät wie bisher die öffentlichen Organe in Fragen des Datenschutzes. Gemäss Abs.1 lit. e prüft das Datenschutz-Kontrollorgan Bearbeitungsmethoden vorab, wenn ein hohes Risiko für eine Beeinträchtigung von Grundrechten besteht.

Neu ist die Kompetenz, dass das Datenschutz-Kontrollorgan zu allen Erlassen Stellung nehmen kann, die für den Datenschutz erheblich sind (Abs. 1 lit. e^{bis}). Praxisgemäss wurde dies schon bisher so gehandhabt, nun wird dies auch gesetzlich festgehalten.

Der bisherige Abs. 1 lit. f wird ergänzt mit dem Halbsatz, dass das Datenschutz-Kontrollorgan die für den Schutz von Personendaten massgeblichen technischen und rechtlichen Entwicklungen verfolgt. Dieser Auftrag an das Datenschutz-Kontrollorgan soll explizit im Gesetz festgelegt werden.
Die bisher in den Abs. 2 bis 4 geregelten Befugnisse sind entweder in andere Bestimmungen eingeflossen oder obsolet geworden.

Art. 27a Untersuchung
Das Datenschutz-Kontrollorgan wird einerseits tätig und eröffnet eine Untersuchung, wenn es selbst Feststellungen für eine Verletzung von Datenschutzvorschriften ausmacht, andererseits wird es auf Anzeige hin tätig. Das Datenschutz-Kontrollorgan ist gehalten, aufgrund von Art. 47 Abs. 2 lit. c der Richtlinie (EU) 2016/680 auch vorsorgliche Massnahmen zu treffen. Es kann, um einen bestehenden Zustand aufrechtzuerhalten, gefährdete schutzwürdige Interessen zu schützen oder Beweismittel zu sichern, eine Datenbearbeitung vorsorglich untersagen oder einschränken.
Das bisher in Art. 27 Abs. 2 geregelte Auskunfts- und Einsichtsrecht des Datenschutz-Kontrollorgans wird aufgrund des übergeordneten europäischen Rechts verstärkt und neu in Art. 27a Abs. 2 geregelt. Das Datenschutz-Kontrollorgan muss einschneidendere Kontrollbefugnisse haben als bis anhin.
Das Datenschutz-Kontrollorgan informiert – im Falle einer Anzeige – die sich beschwerende Person innert drei Monaten über die Art der Erledigung der Anzeige oder über den aktuellen Stand der Untersuchung (Abs. 3).

Art. 27b Abhilfemassnahmen
Wie in Art. 27a erwähnt, muss das Datenschutz-Kontrollorgan aufgrund des übergeordneten europäischen Rechts stärkere Befugnisse haben als bis anhin. Das bisherige System mit der Abgabe lediglich einer Empfehlung (vgl. Art. 27 Abs. 1 lit. d) genügt deshalb nicht mehr. Das Datenschutz-Kontrollorgan muss bei Verstössen gegen das Datenschutzrecht verbindliche Anordnungen treffen können. Im Sinne der erhöhten Transparenz informiert das Datenschutz-Kontrollorgan die Aufsichtsbehörde des verantwortlichen Organs über allfällige Abhilfemassnahmen (Abs. 2). Der Rechtsschutz gegen Anordnungen des Datenschutz-Kontrollorgans richtet sich nach den allgemeinen Regeln des Gesetzes über die Verwaltungsrechtspflege.

Art. 28 Abs. 1 Kostenpflicht
Im Datenschutz hat sich der Grundsatz durchgesetzt, dass Auskünfte, die Gewährung von Einsicht, die Berichtigung falscher Daten und die Sperrung von Daten grundsätzlich kostenlos erteilt werden. Insofern wird Abs. 1 von Art. 28 ergänzt. Dies geschieht auch vor dem Hintergrund von Art. 46 Abs. 3 der Richtlinie (EU) 2016/680. Aufgrund von offensichtlich unbegründeten oder – besonders wegen Wiederholungen – unverhältnismässig häufigen Anträgen kann das Datenschutz-Kontrollorgan – wie bis anhin schon – eine angemessene Gebühr verlangen.

Art. 29 Regierungsrat
Dieser Artikel wird aufgehoben. Aufgrund der gestärkten institutionellen Unabhängigkeit des Datenschutz-Kontrollorgans ist der Erlass von Weisungen usw. durch den Regierungsrat nicht mehr gerechtfertigt.

Änderungen von kantonalem Recht
Auf kantonaler Ebene sind Anpassungen in zwei Gesetzen notwendig, einerseits im Gesetz über eGovernment und Informatik und andererseits im Polizeigesetz.

Gesetz über eGovernment und Informatik
Art. 18 des Gesetzes über eGovernment und Informatik (EGovG, bGS 142.3) wird mit einem Abs. 3 ergänzt, wonach die Geschäftsleitung der AR Informatik AG (ARI) eine verantwortliche Person für den Datenschutz bezeichnet. Diese dient dem Datenschutz-Kontrollorgan als fachliche Anlaufstelle im Bereich Informatik, der für den Datenschutz immer zentraler wird.

Polizeigesetz
Aufgrund von Art. 47 Abs. 2 lit. c der Richtlinie (EU) 2016/680 wird Art. 31a des Polizeigesetzes angepasst. Dabei geht es um Anpassungen im Zusammenhang mit der Interkantonale Vereinbarung über die computergestützte Zusammenarbeit der Kantone bei der Aufklärung von Gewaltdelikten (ViCLAS-Konkordat), welches von der Kantonspolizei vollzogen wird. Der Kanton Appenzell Ausserrhoden trat dem Konkordat im Jahre 2011 bei. Gegenstand und Zweck der Vereinbarung ist die effiziente Bekämpfung der (seriellen) Gewalt- und Sexualkriminalität durch Unterstützung und Förderung der interkantonalen Zusammenarbeit. Dazu gehört gemäss der kantonsübergreifende Einsatz des Analyseinstruments ViCLAS. Zweck ist die Unterstützung in der Verhinderung bzw. Aufklärung von Delikten gegen die physische und sexuelle Integrität.

C. Auswirkungen

Die Anpassungen des Datenschutzrechts führt voraussichtlich auch beim Kanton Appenzell Ausserrhoden zu personellen und finanziellen Mehraufwänden. Der zu erwartende Mehraufwand ist derzeit indes noch nicht abschätzbar. Die neuen Aufgaben werden sich voraussichtlich schrittweise entwickeln. Sowohl der Bund als auch andere Kantone schlagen vor, vorerst mit den vorhandenen Ressourcen weiterzuarbeiten und diese nach einer gewissen Zeit zu evaluieren und erst dann ressourcenmässige Anpassungen vorzunehmen. Diese Haltung erscheint auch für den Kanton Appenzell Ausserrhoden zielführend.