

Leitfaden der Konferenz der Kantonsregierungen (KdK-Leitfaden)

EU-Datenschutzreform/Modernisierung der Europarats-Konvention 108: Anpassungsbedarf bei den kantonalen (Informations- und) Datenschutzgesetzen

Neue Rechtsquellen:

- E-Konv108** Übereinkommen (des Europarates) zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten; konsolidierter Wortlaut der Vorschläge zur Modernisierung des Übereinkommens 108 im Anschluss an die Sitzung des CAHDATA (15./16. Juni 2016) (https://www.admin.ch/ch/d/gg/pc/documents/2826/Totalrevision-des-Datenschutzgesetzes_Uebereinkommen_de.pdf)
- RL 2016/680** 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, ABI L119 vom 4.5.2016, 89 ff.
- VE-DSG** Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz (Vernehmlassung eröffnet am 21.12.2016) (https://www.admin.ch/ch/d/gg/pc/documents/2826/Totalrevision-des-Datenschutzgesetzes_Entwurf-DSB_de.pdf)

Abkürzung:

WL Konferenz der Kantonsregierungen (KdK), Umsetzung Schengen/Dublin in den Kantonen: Datenschutz, Wegleitung, 2006 (https://ius.unibas.ch/uploads/publics/7600/20100219145130_4b7e9762a9a59.pdf).

Anpassungsbedarf:

Kein Anpassungsbedarf

Anpassungsbedarf prüfen

Anpassungsbedarf

Ausgangslage

Es wird für die Darlegung des aktuellen Anpassungsbedarfs davon ausgegangen, dass Anpassungen, die aufgrund der Schengen-Assoziierung (Anpassungsbedarf gemäss Wegleitung 2006 und späterer Anpassungsbedarf aufgrund der Übernahme des Rahmenbeschlusses 2008/977) schon bisher erforderlich waren, vorgenommen worden sind. Sollte das in einem Kanton partiell nicht der Fall sein, sind die nicht erfolgten Anpassungen zusätzlich vorzunehmen.

	Thema	Rechtsgrundlage	Umschreibung	Mögliche Lösungen	Erfüllt, wenn ...
1	Rechtsform: Gesetz				
1.1	Rechtsform (WL Ziff. 1) Kein Anpassungsbedarf	Art. 4 Ziff. 1 E-Konv108 Art. 63 Abs. 1 RL 2016/680	Jeder Kanton muss selber für die nötigen Datenschutzregelungen sorgen, da dem Bund mangels einer verfassungsrechtlichen Kompetenz keine Regelungsbefugnis für das Datenbearbeiten durch kantonale und kommunale Organe zukommt.	Datenschutzgesetz, Informations- und Datenschutzgesetz	... ein kantonales Datenschutzgesetz (Informations- und Datenschutzgesetz o.ä.) existiert, das die inhaltlichen Anforderungen gemäss Ziff. 2-8 erfüllt.

	Thema	Rechtsgrundlage	Umschreibung	Mögliche Lösungen	Erfüllt, wenn ...
2	Geltungsbereich des Gesetzes				
2.1	Geltungsbereich (WL Ziff. 2.1) (nur automatisiertes Datenbearbeiten?)	Art. 2 Abs. 1 VE-DSG Art. 3 E-Konv108 Art. 2 RL 2016/680 Keine Einschränkung mehr in der E-Konv108	Die gesetzliche Regelung muss für alle Datenbearbeitungen durch kantonale und kommunale Organe gelten mit höchstens den folgenden Ausnahmen (Ziff. 2.2-2.5): Es ist unzulässig, den Geltungsbereich auf das automatisierte Bearbeiten von Personendaten einzuschränken.	«gilt für jedes Bearbeiten von Personendaten durch (kantonale und kommunale) öffentliche (Organe), unabhängig von den angewandten Mitteln und Verfahren»	... der Geltungsbereich entsprechend umschrieben ist und keine weiteren als die in Ziff. 2.2–2.5 umschriebenen Ausnahmen vorgesehen sind.
2.2	Ausnahmen vom Geltungsbereich (WL Ziff. 2.2) Anpassungsbedarf	Art. 33 Abs. 1 VE-DSG	Es ist zulässig, für das Datenbearbeiten privatrechtlich handelnder öffentlicher Organe die Regeln des Bundesdatenschutzgesetzes für privates Datenbearbeiten anwendbar zu erklären. Da solche kantonalen öffentlichen Organe nicht Private werden, sondern nur wie Private handeln, bleibt – analog zur Regelung im Bund (Art. 23 Abs. 2 DSG und Art. 32 Abs. 2 VE-DSG) – die kantonale Aufsichtsbehörde zuständig.	«Soweit ein öffentliches Organ am wirtschaftlichen Wettbewerb teilnimmt und dabei privatrechtlich handelt, sind auf sein diesbezügliches Datenbearbeiten die entsprechenden Regeln des Bundesgesetzes über den Datenschutz anwendbar; die Aufsicht richtet sich nach dem vorliegenden Gesetz.»	... die Ausnahme nicht weiter gehend umschrieben ist.
2.3	Nicht mehr für zivil- und strafgerichtliche Verfahren (WL Ziff. 2.3) Anpassungsbedarf	Art. 2 Abs. 3 VE-DSG Keine Ausnahme in Art. 3 E-Konv108 (und Art. 12^{bis} Ziff. 9 K108 [09.16]: Unzuständigkeit der Aufsichtsbehörde in gerichtlichen Verfahren) Keine Ausnahme in Art. 2 RL 2016/680	Änderung gegenüber der bisherigen Ausgangslage: Es dürfen keine generelle Geltungsbereich-Ausnahmen mehr vorgesehen werden für hängige zivil- und strafgerichtliche Verfahren. Das bedeutet aber keineswegs, dass die Prozessordnungen nicht mehr gelten: Sie behalten als bereichsspezifisches Datenschutzrecht (wie die anderen Fachgesetze, z.B. das Polizeigesetz, das Schulgesetz oder das Bundesgesetz über den Allgemeinen Teil des Sozialversicherungsrechts) ohnehin weiter ihre Gültigkeit (vgl. dazu BEAT RUDIN, Überholte Ausnahmen beim Geltungsbereich, digma 2016, 122 ff.). Das heisst: Die Regelungen z.B. der Strafprozessordnung gelten weiterhin – aber auch die Grundsätze des (Informations- und) Datenschutzgesetzes (z.B. die Regeln zur verantwortlichen Behörde, zur Informationssicherheit usw.). Zwei Bereiche sind aber zusätzlich zu regeln: - Um Kollisionen zwischen den verfahrensrechtlichen und den datenschutzrechtlichen Informationsansprüchen der Parteien/der betroffenen Personen zu vermeiden, sollte aber vorgesehen werden, dass sich die Rechte und Ansprüche der betroffenen Personen während hängigen Verfahren der Zivil- und Strafrechtspflege ausschliesslich nach dem anwendbaren Verfahrensrecht richten. - Ausserdem sollte (und darf) vorgesehen werden, dass Datenbearbeitungen in hängigen gerichtlichen Verfahren nicht der Aufsicht der oder des Datenschutzbeauftragten unterstehen (→ Ziff. 8.2.). Mit der Formulierung «Verfahren der Strafrechtspflege» sind	«Die Rechte und Ansprüche der betroffenen Personen während hängigen Verfahren der Zivil- und Strafrechtspflege (... [→ Ziff. 2.4]) richten sich ausschliesslich nach dem anwendbaren Verfahrensrecht.»	... die Ausnahme nicht weiter gehend umschrieben ist.

	Thema	Rechtsgrundlage	Umschreibung	Mögliche Lösungen	Erfüllt, wenn ...
			nicht nur die Verfahren vor dem Strafgericht erfasst; es beginnt mit der Eröffnung einer Strafuntersuchung durch die Staatsanwaltschaft. Die vom Bund im Vernehmlassungsentwurf gewählte Lösung ist nicht konventionskonform, soweit sie den Geltungsbereich des DSG in hängigen gerichtlichen Verfahren einschränkt.		
2.4	Nicht mehr für verwaltungs- und Verfassungsgerichtsbarkeit (WL Ziff. 2.4) Anpassungsbedarf	Art. 2 Abs. 3 VE-DSG Keine Ausnahme in Art. 3 E-Konv108 (und Art. 12^{bis} Ziff. 9 K108 [09.16]: Unzuständigkeit der Aufsichtsbehörde in gerichtlichen Verfahren) Keine Ausnahme in Art. 2 RL 2016/680	Dasselbe (→ Ziff. 2.3) gilt für hängige Verfahren der Verwaltungs- (und, sofern im Kanton gegeben, der Verfassungs-)gerichtsbarkeit.	«Die Rechte und Ansprüche der betroffenen Personen während hängigen (... [→ Ziff. 2.3]) Verfahren der Verwaltungs- und Verfassungsgerichtsbarkeit richten sich ausschliesslich nach dem anwendbaren Verfahrensrecht».	... die Ausnahme nicht weiter gehend umschrieben ist.
2.5	Bearbeiten zum persönlichen Gebrauch (WL Ziff. 2.5) Anpassungsbedarf prüfen	Art. 2 Abs. 2 lit. a VE-DSG Art. 3 Ziff. 1^{bis} E-Konv108 Keine Ausnahme in der RL 2016/680	Eine Ausnahme für das Bearbeiten von Personendaten zum persönlichen Gebrauch vorzusehen ist problematisch (die im VE-DSG vorgesehene Ausnahme der Datenbearbeitung ausschliesslich zum familiären Gebrauch ist bei öffentlichen Organen ohnehin irrelevant). Es darf keine «Schattendossiers» geben. Einzig Aufzeichnungen im Sinne von Gedankenstützen sind zulässig – sie sollten aber nicht aus dem Geltungsbereich des Datenschutzgesetzes generell ausgenommen werden, sondern es sollte höchstens eine Ausnahme für persönliche Notizen im Sinne von Gedankenstützen vom <i>Recht auf Zugang zu den eigenen Personendaten</i> ausgenommen sein.	<i>Keine generelle Ausnahme beim Geltungsbereich.</i> <i>Allerhöchstens eng umschriebene Ausnahme beim Recht auf Zugang zu den eigenen Personendaten (Recht auf Auskunft, → Ziff. 5.4-5.6)</i>	... die keine Ausnahme vom Geltungsbereich für «persönliche Arbeitsmittel» («Personendaten zum persönlichen Gebrauch») o.ä. vorgesehen ist.
3	Begriffsdefinitionen				
3.1	Begriffsdefinitionen (WL ---)	Art. 3 VE-DSG Art. 2 E-Konv108 Art. 3 RL 2016/680	Neben den bisherigen Begriffsdefinitionen sind die folgenden Änderungen zu beachten:		
3.2	Personendaten (WL ---) Anpassungsbedarf prüfen	Art. 3 lit. a und b VE-DSG («betroffene Person») Art. 2 lit. a E-Konv108 Art. 3 Ziff. 1 RL 2016/680	Anders als die internationalen Vorgaben (und die meisten europäischen Staaten) schützen die schweizerischen Datenschutzgesetze bisher nicht nur natürliche, sondern auch juristische Personen. Der Bundesrat hat angekündigt, diese Spezialität bei der Revision des DSG aufzugeben: Die Kantone sind nicht verpflichtet, diese Anpassung nachzuvollziehen, doch wäre es wohl sinnvoll, dies gleichwohl zu tun. Eine Anpassung erfolgt primär durch die Streichung der juristischen Personen bei der Begriffsdefinition «Personendaten». Allenfalls ist es auch notwendig, die Zweckbestimmung des Gesetzes anzupassen, falls dort bisher die juristischen Personen erwähnt oder miterfasst sind (z.B. bei der Umschreibung, dass die Grundrechte von Personen [also natürlichen und juristischen] geschützt werden sollen, über die öffentliche Organe Daten [Informationen] bearbeiten).	Begriffsbestimmungen: Personendaten sind: «- Angaben über bestimmte oder bestimmbare natürliche Personen» Zweckartikel: <i>Dieses Gesetz bezweckt «die Grundrechte von natürlichen Personen zu schützen, über welche die öffentlichen Organe Personendaten bearbeiten.»</i>	... aus der Begriffsdefinition (und allenfalls auch aus dem Zweckartikel) klar hervorgeht, dass der Schutz nur natürlichen Personen zukommt (falls wie im Bund die juristischen Personen ausgenommen werden sollen).

	Thema	Rechtsgrundlage	Umschreibung	Mögliche Lösungen	Erfüllt, wenn ...
3.3	Besonders schützenswerte (besondere) Personendaten Anpassungsbedarf	Art. 3 lit. c VE-DSG Art. 6 E-Konv108 Art. 3 i.V.m. Art. 10 RL 2016/680	Unter die besonders schützenswerten (besonderen) Personendaten fallen seit jeher Angaben «über die Rasse» oder «über die Rassenzugehörigkeit». «Rasse» ist in Bezug auf die Menschen kein wissenschaftlicher Begriff; geschützt werden soll vielmehr vor dem Rassevorwurf (historisch: «Jude», «Neger»). Modernere Gesetze erfassen deshalb «Angaben über die Ethnie» oder «über die 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. Die K108 erwähnt neu neben der Rasse die Ethnie als Kriterium für besonders schützenswerte (besondere) Daten. Empfohlen wird der Ersatz der «Rasse» durch Ethnie.	<i>Besonders schützenswerte Personendaten (besondere Personendaten) sind:</i> «- Daten über (die Gesundheit, das Erbgut, die persönliche Geheimsphäre oder) die ethnische Herkunft;»	... in der Definition im Gesetz das Kriterium «Ethnie» (ethnische Zugehörigkeit, ethnische Herkunft) enthalten (und das Kriterium «Rasse» möglichst nicht mehr enthalten) ist.
3.4	Daten zum Sexualleben oder zur sexuellen Orientierung (WL ---) Anpassungsbedarf prüfen	Art. 3 lit. c Ziff. 2 VE-DSG Art. 6 Abs. 1 E-Konv108 Art. 10 RL 2016/680	Daten zum Sexualleben oder zur sexuellen Orientierung fallen neu ausdrücklich in die Kategorie der besonders schützenswerten (besonderen) Personendaten. Falls bisher z.B. «die Intimsphäre» oder «die persönliche Geheimsphäre» in der Begriffsdefinition enthalten ist oder die besonders schützenswerten (besonderen) Personendaten nicht abschliessend umschrieben sind (z.B. durch eine «insbesondere»-Aufzählung), dann kann eine Anpassung ausbleiben, wenn sichergestellt ist, dass die Daten zum Sexualleben oder zur sexuellen Orientierung zweifellos mitverstanden werden.	<i>Besonders schützenswerte Personendaten (besondere Personendaten) sind:</i> «- Daten über die Intimsphäre» oder «- Daten über das Sexualleben oder die sexuelle Orientierung»	... die Definition im Gesetz enthalten ist oder (z.B. bei nicht abschliessender Umschreibung der besonders schützenswerten [besonderen] Personendaten) zweifellos mitverstanden wird.
3.5	genetische Daten (WL ---) Anpassungsbedarf prüfen	Art. 3 lit. c Ziff. 3 VE-DSG Art. 6 Ziff. 1 E-Konv108 Art. 3 Ziff. 12 i.V.m. Art. 10 RL 2016/680	«Genetische Daten» fallen neu ausdrücklich in die Kategorie der besonders schützenswerten (besonderen) Personendaten. Falls bisher z.B. «das Erbgut» in der Begriffsdefinition enthalten ist oder die besonders schützenswerten (besonderen) Personendaten nicht abschliessend umschrieben sind (z.B. durch eine «insbesondere»-Aufzählung), dann kann eine Anpassung ausbleiben, wenn sichergestellt ist, dass die genetischen Daten zweifellos mitverstanden werden.	<i>Besonders schützenswerte Personendaten (besondere Personendaten) sind:</i> «- genetische Daten»	... die Definition im Gesetz enthalten ist oder (z.B. bei nicht abschliessender Umschreibung der besonders schützenswerten [besonderen] Personendaten) zweifellos mitverstanden wird.
3.6	biometrische Daten (WL ---) Anpassungsbedarf	Art. 3 lit. c Ziff. 4 VE-DSG Art. 6 Ziff. 1 E-Konv108 Art. 3 Ziff. 13 i.V.m. Art. 10 RL 2016/680	Biometrische Daten, d.h. 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 (wie Gesichtsbilder, d.h. durch Gesichtserkennungsprogramme gewonnene Daten zu einem Gesicht – also nicht jede Foto eines Gesichts! –, daktyloskopische Daten, Stimmuster, Iris-Muster), fallen neu in die Kategorie der besonders schützenswerten (besonderen) Personendaten.	<i>Besonders schützenswerte Personendaten (besondere Personendaten) sind:</i> «- 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 (biometrische Daten)»	... die Definition im Gesetz enthalten ist.

	Thema	Rechtsgrundlage	Umschreibung	Mögliche Lösungen	Erfüllt, wenn ...
3.7	Bearbeiten (WL ---) Anpassungsbedarf prüfen	Art. 3 lit. d VE-DSG Art. 2 lit. b E-Konv108 Art. 3 Ziff. 2 RL 2016/680	Das Bearbeiten wird beispielhaft präziser umschrieben als bisher. In der Vernehmlassungsvorlage des Bundes und auch in der RL 2016/680 werden die Begriffe «Löschen» und «Vernichten» nebeneinander verwendet, ohne dass das Verhältnis der beiden zueinander geklärt wird. Vernichten hat bisher das endgültige physische «Zerstören» gemeint. Ob Löschen nur das «Entfernen aus dem aktiven Prozess» (ähnlich wie das Löschen von Strafregistereinträgen) meint oder einfach das Vernichten im elektronischen Umfeld, muss vom Kanton festgelegt werden; ob im finalen Gesetzesentwurf des Bundesrates eine Klärung enthalten sein wird, ist ungewiss.	« <i>Bearbeiten: jeder Umgang mit Daten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten sowie das Durchführen logischer und/oder rechnerischer Operationen mit diesen Daten;</i> »	... die präzisere Definition im Gesetz enthalten ist oder alle neu erwähnten Erscheinungsformen zweifellos mitverstanden werden.
3.8	Profiling (WL ---) Anpassungsbedarf	Art. 3 lit. f VE-DSG Art. 3 Ziff. 4 RL 2016/680	Die EU-Richtlinie regelt neu das Profiling (als besondere, «gefährliche» Art des <i>Bearbeitens</i> von Personendaten), das denselben Anforderungen genügen muss wie das Bearbeiten von besonders schützenswerten Personendaten (also i.d.R. nur gestützt auf eine Grundlage in einem Gesetz im formellen Sinn). Dies muss auch in die kantonalen Gesetze übernommen werden. Im Interesse der einfachen Formulierung und Verständlichkeit ist «Profiling» in die Begriffsdefinitionen aufzunehmen. Der in den kantonalen Gesetzen häufig verwendete Begriff des Persönlichkeitsprofils (als praktisch den besonders schützenswerten Personendaten gleichgestellte Kategorie von <i>Daten</i>) kann gestrichen oder beibehalten werden. Zusammengefasst heisst das: - der Begriff des Profilings (als <i>Bearbeitungsart</i>) ist einzufügen, - der Begriff des Persönlichkeitsprofils (als <i>Kategorie von Personendaten</i>) kann gestrichen (wie beim Bund) oder beibehalten werden; die Umschreibung der «Zusammenstellungen von Informationen, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit natürlicher Personen erlauben» als Teil der Umschreibung von besonderen (besonders schützenswerten) Personendaten (ohne den Begriff «Persönlichkeitsprofil») kann auf jeden Fall beibehalten werden; - die entsprechenden Anpassungen bei den Grundsätzen des Datenbearbeitens sind vorzunehmen (→ Ziff. 4.2) und - in den bereichsspezifischen Fachgesetzen sind diese Änderungen ebenfalls nachzuvollziehen.	Einfügung des neuen Begriffs: « <i>Profiling: jede Auswertung von Daten oder Personendaten, um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen, insbesondere bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, Intimsphäre oder Mobilität vorherzusagen</i> »	... wenn die Definition des Profilings im Gesetz enthalten.
3.9	Für die Bearbeitung verantwortliches öffentliches	Art. 3 lit. h VE-DSG Art. 2 lit. d E-Konv108 («Controller»)	Das übergeordnete Recht definiert den Begriff der «für die Bearbeitung verantwortlichen Person». Eine solche Begriffsdefinition kann übernommen werden oder bei der Regelung der	« <i>für die Bearbeitung verantwortliches öffentliches Organ: das öffentliche Organ, das – alleine oder zusammen mit anderen</i>	... wenn die Begriffsdefinition übernommen wird oder der Begriff bei der

	Thema	Rechtsgrundlage	Umschreibung	Mögliche Lösungen	Erfüllt, wenn ...
	ches Organ (WL ---) Anpassungsbedarf prüfen	Art. 3 Ziff. 8 RL 2016/680	Verantwortung sachlich geregelt werden. Ohnehin müsste es auf kantonaler Ebene, wo das Bearbeiten durch Private nicht Regelungsgegenstand ist, der Begriff des «für die Bearbeitung verantwortlichen öffentlichen Organs» (Behörde o.ä.) verwendet werden.	– über den Zweck, die Mittel und den Umfang der Bearbeitung von Daten entscheidet» oder direkte Umsetzung (→ Ziff. 4.9)	Regelung der Verantwortung (→ Ziff. 4.9) geklärt wird.
3.10	Auftragsdatenbearbeiter (WL ---) Anpassungsbedarf prüfen	Art. 3 lit. i VE-DSG Art. 2 lit. f E-Konv108 Art. 3 Ziff. 9 RL 2016/680	Das übergeordnete Recht definiert den Begriff des «Auftragsbearbeiters». Eine solche Begriffsdefinition kann übernommen werden oder bei der Regelung der Verantwortung sachlich geregelt werden. Es wird empfohlen, den Begriff der Auftragsdatenbearbeiterin bzw. des Auftragsdatenbearbeiters (und nicht: Auftragsbearbeitung) zu verwenden: Es geht nicht einfach um die Bearbeitung eines Auftrags, sondern um eine Datenbearbeitung im Auftrag.	«Auftragsdatenbearbeiter: die private Person oder das öffentliche Organ, die oder das im Auftrag des für die Bearbeitung verantwortlichen öffentlichen Organs Daten bearbeitet» oder direkte Umsetzung (→ Ziff. 4.12)	... wenn die Begriffsdefinition übernommen wird oder der Begriff bei der Regelung der Auftragsdatenbearbeitung (→ Ziff. 4.12) geklärt wird.
4	Grundsätze des Bearbeitens				
4.1	Rechtmässigkeit (WL Ziff. 3.1) Kein Anpassungsbedarf	Art. 4 Abs. 1 VE-DSG Art. 5 Ziff. 3 E-Konv108 Art. 4 Abs. 1 lit. a und Art. 8 RL 2016/680	Das Bearbeiten von Personendaten muss rechtmässig sein. Bezüglich des behördlichen Datenbearbeitens heisst das insbesondere, dass Daten nur gestützt auf eine Rechtsgrundlage bearbeitet werden dürfen. Eine solche Rechtsgrundlage kann als ausdrückliche Verpflichtung oder Ermächtigung zu einer bestimmten Datenbearbeitung vorliegen (sog. unmittelbare gesetzliche Grundlage) oder als gesetzliche Aufgabe, zu deren Erfüllung bestimmte Datenbearbeitungen erforderlich sind (sog. mittelbare gesetzliche Grundlage). Im öffentlichrechtlichen (d.h. dem Legalitätsprinzip unterstehenden) Datenschutz ist fraglich, ob eine blosser Einwilligung einer betroffenen Person ein behördliches Datenbearbeiten rechtfertigen kann. Es ist nicht nachvollziehbar, dass beispielsweise die Sozialhilfe allein aufgrund einer Einwilligung Daten über einen Gesuchsteller bearbeiten dürfen soll; es müsste ja mehr sein, als was sie aufgrund einer mittelbaren gesetzlichen Grundlage zur Aufgabenerfüllung ohnehin schon tun darf (also z.B. Daten der Steuerverwaltung beziehen, um die Angaben des Gesuchstellers zu seiner Bedürftigkeit zu überprüfen). Eine «Einwilligung» kann aber allenfalls als Entbindung dienen von einem besonderen Amts- oder Berufsgeheimnis der Stelle oder Person, die der Sozialhilfe Daten bekannt geben soll (z.B. bei einer Ärztin, welche die Arbeitsfähigkeit beurteilen soll) oder von der Vornahme einer Interessenabwägung. Sinnvoll ist die Einwilligung ausserdem als Rechtfertigung bei der Datenbekanntgabe. Zu den qualifizierten Anforderungen an das Bearbeiten von	Beim Datenbearbeiten: z.B. «rechtmässig», «gesetzmässig», «wenn dafür eine (ausdrückliche) gesetzliche Grundlage besteht» (sog. unmittelbare gesetzliche Grundlage) «oder dies zur Erfüllung einer gesetzlichen Aufgabe erforderlich ist» (sog. mittelbare gesetzliche Grundlage) Bei der Datenbekanntgabe: z.B. «gibt Personendaten bekannt, wenn eine gesetzliche Bestimmung dazu verpflichtet oder ermächtigt,» (sog. unmittelbare gesetzliche Grundlage) «oder dies zur Erfüllung einer gesetzlichen Aufgabe erforderlich ist» (sog. mittelbare gesetzliche Grundlage) «oder wenn im Einzelfall die betroffene Person ausdrücklich zugestimmt hat oder, falls sie dazu nicht in der Lage ist, die Bekanntgabe in ihrem Interesse liegt und ihre Zustimmung in guten Treuen vorausgesetzt werden darf».	... das Erfordernis der Rechtmässigkeit (Gesetzmässigkeit) entsprechend im Gesetz festgeschrieben ist.

	Thema	Rechtsgrundlage	Umschreibung	Mögliche Lösungen	Erfüllt, wenn ...
			besonders schützenswerten Personendaten und an das Profiling → Ziff. 4.2		
4.2	Qualifizierte Anforderungen an das Bearbeiten besonders schützenswerter (besonderer) Personendaten und das Profiling (WL Ziff. 3.7) Anpassungsbedarf (Profiling)	Art. 27 Abs. 2 und Art. 29 Abs. 1 VE-DSG Art. 6 Ziff. 1 E-Konv108 Art. 10 RL 2016/680	Die Bearbeitung von Personendaten, die besonders persönlichkeitsnahe sind und ein grosses Stigmatisierungs- und Diskriminierungspotenzial besitzen (sog. besonders schützenswerte, sensitive oder besondere Personendaten), verlangt nach einem qualifizierten Schutz. Üblicherweise wird eine <i>formell-gesetzliche Grundlage</i> verlangt oder es werden an die Erforderlichkeit zur Erfüllung einer Aufgabe <i>höhere Anforderungen</i> gestellt («zwingend notwendig», «unbedingt erforderlich», «unentbehrlich»). Wenn bei der Datenbekanntgabe – im Einzelfall – die Einwilligung der betroffenen Person als Rechtfertigungsgrund dienen soll, muss es sich um einen «informed consent» handeln (Zustimmung in Kenntnis der Sachlage, freiwillig und ohne [offene oder versteckte] Androhung von Nachteilen im Verweigerungsfall). Zu beachten ist ausserdem, dass die Begriffsdefinition « <i>Persönlichkeitsprofil</i> » wegfallen kann, aber dafür hier jeweils das Profiling geregelt werden muss (→ Ziff. 3.8).	<i>Bei der Datenbearbeitung:</i> « <i>Besonders schützenswerte Personendaten dürfen nur bearbeitet oder ein Profiling darf nur vorgenommen werden, wenn ein Gesetz (im formellen Sinn) es ausdrücklich vorsieht</i> » (sog. <i>unmittelbare gesetzliche Grundlage</i>) « <i>oder wenn es für eine in einem Gesetz (im formellen Sinn) klar umschriebene Aufgabe unentbehrlich ist</i> » (sog. <i>mittelbare gesetzliche Grundlage</i>) <i>Bei der Datenbekanntgabe:</i> « <i>gibt besonders schützenswerte Personendaten oder Resultate eines Profilings nur bekannt, wenn ein Gesetz dazu ausdrücklich verpflichtet oder ermächtigt</i> » (sog. <i>unmittelbare gesetzliche Grundlage</i>), « <i>dies zur Erfüllung einer in einem Gesetz klar umschriebenen Aufgabe zwingend notwendig ist</i> » (sog. <i>mittelbare gesetzliche Grundlage</i>) « <i>oder wenn im Einzelfall die betroffene Person ausdrücklich zugestimmt hat oder, falls sie dazu nicht in der Lage ist, die Bekanntgabe in ihrem Interesse liegt und ihre Zustimmung in guten Treuen vorausgesetzt werden darf.</i> »	... die Bearbeitung besonders schützenswerter (sensitiver, besonderer) Personendaten und das Profiling an qualifizierte Voraussetzungen geknüpft werden.
4.3	Treu und Glauben (WL Ziff. 3.2) Kein Anpassungsbedarf	Art. 4 Abs. 2 VE-DSG Art. 5 Ziff. 4 lit. a E-Konv108 Art. 4 Abs. 1 lit. a RL 2016/680	Das Bearbeiten von Personendaten muss nach Treu und Glauben erfolgen. Ausfluss dieses Grundsatzes ist insb. das Verbot der verdeckten Datenerhebung (Erkennbarkeit der Datenerhebung). Das Prinzip verliert aufgrund der Informationspflicht der datenbearbeitenden öffentlichen Organe (→ Ziff. 5.2) an selbständiger Bedeutung.	« <i>hat nach Treu und Glauben zu erfolgen</i> »	... das Erfordernis der Bearbeitung nach Treu und Glauben im Gesetz festgeschrieben ist oder sich zweifelsfrei aus den Verfassungsgrundsätzen ergibt
4.4	Zweckbindung (WL Ziff. 3.3) Kein Anpassungsbedarf	Art. 4 Abs. 3 VE-DSG Art. 5 Ziff. 4 lit. b E-Konv108 Art. 4 Abs. 1 lit. b RL 2016/680	Die Zweckbindung (oder das Zweckänderungsverbot) ist eines der Kernelemente des Datenschutzrechts. Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist, wobei im öffentlich-rechtlichen Bereich die Zweckbestimmung durch das Gesetz im Vordergrund steht.	« <i>Personendaten dürfen nur zu dem Zweck bearbeitet werden, zu dem sie erhoben worden sind, soweit nicht eine gesetzliche Grundlage ausdrücklich eine weitere Verwendung vorsieht oder die betroffene Person im Einzelfall einwilligt.</i> » oder « <i>Personendaten dürfen nur für festgelegte (eindeutige) und rechtmässige Zwecke bearbeitet werden</i> »,	... das Erfordernis der Zweckbindung entsprechend im Gesetz festgeschrieben ist

	Thema	Rechtsgrundlage	Umschreibung	Mögliche Lösungen	Erfüllt, wenn ...
4.5	Verhältnismässigkeit (WL Ziff. 3.4) Kein Anpassungsbedarf	Art. 4 Abs. 2 VE-DSG Art. 5 Ziff. 1 und Art. 5 Ziff. 4 lit. c E-Konv108 Art. 4 Abs. 1 lit. c RL 2016/680	Das Bearbeiten von Personendaten muss – wie jedes behördliche Handeln – verhältnismässig sein. Die bearbeiteten Daten müssen zur Zweckerreichung geeignet sein; die Datenbearbeitung muss das mildeste Mittel sein, mit welchem der Zweck erreicht werden kann, und Zweck (Aufgabe) und Eingriff in die informationelle Selbstbestimmung (Datenbearbeitung) müssen in einem vernünftigen Verhältnis zueinander stehen (Verhältnismässigkeit i.e.S.). Zur zeitlichen Dimension der Verhältnismässigkeit → Ziff. 4.6. Zu den qualifizierten Anforderungen an die Verhältnismässigkeit beim Bearbeiten von besonders schützenswerten Personendaten und an das Profiling → Ziff. 4.2.	<i>«müssen zur Erreichung des Zwecks, zu dem sie bearbeitet werden, geeignet und erforderlich sein (...)</i> », <i>«dürfen bearbeitet werden, soweit (und solange) sie für die Zweckerreichung geeignet und erforderlich sind</i> », <i>«dürfen bearbeitet werden, soweit sie für die Zweckerreichung geeignet und erforderlich sind, (...)»</i>	... das Erfordernis der Verhältnismässigkeit entsprechend im Gesetz festgeschrieben ist.
4.6	(zeitlich) (WL Ziff. 3.4) Anpassungsbedarf prüfen	Art. 4 Abs. 4 VE-DSG Art. 5 RL 2016/680	Schon bisher gehörte zur Verhältnismässigkeit, dass das Bearbeiten von Personendaten zeitlich befristet sein muss. Neu wird verlangt, dass für die Löschung (oder Anonymisierung) von Personendaten bzw. für eine regelmässige Überprüfung, ob Personendaten zur Aufgabenerfüllung noch erforderlich sind, Fristen vorzusehen sind und dass durch verfahrensrechtliche Vorkehrungen sicherzustellen ist, dass diese Fristen eingehalten werden. Erforderlich ist also mindestens eine Vorgabe für die Löschung (oder Anonymisierung) von Personendaten, die zur Aufgabenerfüllung nicht mehr benötigt werden, sofern sie nicht nach Archivrecht zu archivieren sind. Eine Anbietepflicht in anwendbaren Archivgesetz allein dürfte nicht genügen; hingegen kann eine dort verankerte Frist allenfalls als Auffangfrist dienen, wenn nicht bereichsspezifisch Aufbewahrungs-, Überprüfungs- oder Löschfristen verankert sind. Die Vorkehrungen für die Umsetzung können im Verordnungsrecht umschrieben werden oder in einem DSMS (→ Ziff. 4.10) umgesetzt werden. Zur Verwendung der Begriffe «vernichten» bzw. «löschen» → Erläuterungen in Ziff. 3.7	<i>«(müssen zur Erreichung des Zwecks, zu dem sie bearbeitet werden, geeignet und erforderlich sein) und dürfen nicht länger bearbeitet werden, als es zur Zweckerreichung erforderlich ist</i> », <i>«(dürfen bearbeitet werden, soweit) und solange sie für die Zweckerreichung geeignet und erforderlich sind</i> », <i>«(dürfen bearbeitet werden, soweit sie für die Zweckerreichung geeignet und erforderlich sind,) und müssen vernichtet (oder anonymisiert) werden, sobald sie zur Aufgabenerfüllung nicht mehr erforderlich sind»</i> <i>Als separate Bestimmung: «Nicht mehr benötigte Personendaten, die von der gemäss Archivgesetz zuständigen Stelle als nicht archivwürdig beurteilt werden, sind vom öffentlichen Organ zu vernichten (oder zu anonymisieren).»</i> <i>jeweils kombiniert mit der Festlegung von Fristen im bereichsspezifischen Recht, allenfalls mit einer Frist für das Anbieten ans zuständige Archiv im Sinne einer Auffangfrist.</i>	... das Erfordernis zeitlichen Begrenzung einer Datenbearbeitung als Aspekt der Verhältnismässigkeit im kantonalen Recht (Datenschutzgesetz und/oder bereichsspezifisches Recht) festgeschrieben ist.

	Thema	Rechtsgrundlage	Umschreibung	Mögliche Lösungen	Erfüllt, wenn ...
4.7	Richtigkeit (WL Ziff. 3.5) Kein Anpassungsbedarf	Art. 4 Abs. 5 VE-DSG Art. 5 Ziff. 4 lit. d E-Konv108 Art. 4 Abs. 1 lit. d RL 2016/680	Personendaten, die von öffentlichen Organen bearbeitet werden, müssen richtig sein; erstens weil es das Recht auf informationelle Selbstbestimmung es gebietet, und zweitens, weil die Bearbeitung unrichtiger Daten zur behördlichen Aufgabenerfüllung nicht verhältnismässig sein kann. Dementsprechend muss das Erfordernis der Richtigkeit im Gesetz verankert sein, entweder als Grundsatz der Richtigkeit oder als Pflicht der Datenbearbeiter, sich über die Richtigkeit zu vergewissern oder minimal als Berichtigungsanspruch der betroffenen Person. Es reicht nicht mehr, bloss der betroffenen Person einen Berichtigungsanspruch einzuräumen. Die Vollständigkeit der Daten ist ein Unteraspekt der Richtigkeit. Sie ist nur zu beanstanden, wenn die Unvollständigkeit der Daten zu einer Unrichtigkeit führt. In diesem Sinne muss sie nicht ausdrücklich im Gesetz erwähnt sein.	«Das verantwortliche öffentliche Organ hat sich über die Richtigkeit der bearbeiteten Personendaten zu vergewissern. Er hat alle angemessenen Massnahmen zu treffen, damit Daten berichtigt oder vernichtet werden, die im Hinblick auf den Zweck ihrer Beschaffung oder Bearbeitung unrichtig oder unvollständig sind.»	... das Erfordernis der Richtigkeit in einer der erwähnten Formen im Gesetz festgeschrieben ist.
4.8	Informationssicherheit (WL Ziff. 3.6) Anpassungsbedarf prüfen	Art. 11 VE-DSG Art. 7 E-Konv108 Art. 4 Abs. 1 lit. f und Art. 29 RL 2016/680	Personendaten müssen durch technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten (gegen die zufällige oder unbefugte Zerstörung, gegen zufälligen Verlust sowie unbefugten Zugang, unbefugte Veränderung oder unbefugtes Bekanntgeben) geschützt sein. Besser als der überholte Begriff der Datensicherheit (oder gar der Datensicherung) sollte der Begriff Informationssicherheit verwendet werden.	«müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugte Bearbeiten geschützt werden», «sorgt für ihren Schutz vor Verlust, Entwendung, unbefugter Bearbeitung und Kenntnisnahme» plus konkretisierende Regelungen z.B. auf Verordnungsstufe (z.B. Informationssicherheitsverordnung)	... das Erfordernis der Informationssicherheit entsprechend im Gesetz festgeschrieben ist.
4.9	Verantwortung (WL ---) Anpassungsbedarf prüfen	Art. 26 VE-DSG Art. 8 Ziff. 1 ^{bis} E-Konv108 Art. 19 und 21 RL 2016/680	Die neuen Rechtsgrundlagen betonen die Wichtigkeit, dass die Verantwortung für Datenbearbeitungen klar zuzuordnen ist. Das gilt insbesondere bei gemeinsamen Datenbearbeitungen, wo die Verantwortlichkeiten transparent zu regeln sind (inkl. zentrale Anlaufstelle für die betroffenen Personen).	« ^x Die Verantwortung für das Bearbeiten von Personendaten (für den Umgang mit Informationen) trägt dasjenige öffentliche Organ, das die Personendaten (Informationen) zur Erfüllung seiner gesetzlichen Aufgaben bearbeitet. ^x Bearbeiten mehrere öffentliche Organe einen gemeinsamen Informationsbestand, regeln sie die Verantwortung.»	... die Verantwortungszuordnung (insb. bei gemeinsamen Datenbearbeitungen) im Gesetz festgeschrieben ist.
4.10	Nachweisbarkeit der Einhaltung des DS-Vorschriften (WL ---) Anpassungsbedarf	Art. 10 VE-DSG Art. 19 lit. a VE-DSG (ungenügend, da kein Nachweis der Compliance i.S. von K108 und RL) Art. 8 ^{bis} Ziff. 1 E-Konv108 Art. 4 Abs. 4 RL 2016/680	Mehrfach wird in den neuen Rechtsgrundlagen verlangt, dass das verantwortliche öffentliche Organ oder die Auftragsdatenbearbeiterin/der Auftragsdatenbearbeiter die Einhaltung der Datenschutzbestimmungen einhalten können muss. Dieser Nachweis kann in einem Datenschutzmanagementsystem (DSMS) erbracht werden. DSMS basieren auf den ISO-Standards des Qualitätsmanagements (ISO 9001) und der Informationssicherheit (ISO 27001 usw.). Wird auf eine diesbezügliche Zertifizierung verzichtet, ist festzulegen, welche Dokumente notwendig sind, um diesen Nachweis erbringen zu können (z.B. Informationssicherheitskonzept, Zugriffskonzept usw.). Hierzu bestehen bereits zahlreiche Hilfsmittel. Es ist sinnvollerweise auf Verordnungsstufe festzulegen, in	Zusätzlicher Absatz der Verantwortlichkeitsbestimmung: « ^x Das verantwortliche öffentliche Organ muss nachweisen können, dass es die Datenschutzbestimmungen einhält. Der Regierungsrat regelt das Nähere in der Verordnung.»	... wenn die Nachweispflicht im Gesetz verankert ist.

	Thema	Rechtsgrundlage	Umschreibung	Mögliche Lösungen	Erfüllt, wenn ...
			welchen Fällen ein solches DSMS obligatorisch sein soll (z.B. nur wenn besonders schützenswerte [besondere] Personendaten bearbeitet werden).		
4.11	Datenschutzberater (WL ---) Anpassungsbedarf bereichsspezifisch	Art. 32-34 RL 2016/680	Datenschutzberater schreibt nur die Richtlinie für justizielle und polizeiliche Datenbearbeitungen vor. Es ist nicht notwendig, eine solche Pflicht allgemein im Datenschutzgesetz zu verankern – allenfalls bereichsspezifisch im kantonalen Polizeirecht.	<i>Allenfalls im bereichsspezifischen Recht</i>	
4.12	Auftragsdatenbearbeitung (WL ---) Anpassungsbedarf	Art. 7 VE-DSG Art. 22 f. RL 2016/680	Die neue Richtlinie stellt klarere Voraussetzungen auf für das Bearbeitenlassen von Personendaten durch Dritte. So darf nur mit Auftragsdatenbearbeiterinnen und Auftragsdatenbearbeitern gearbeitet werden, die <i>hinreichende Garantien</i> 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 Datenbearbeitung darf nur <i>mit schriftlicher Genehmigung</i> des auftraggebenden öffentlichen Organs auf weitere Auftragsdatenbearbeiterinnen oder Auftragsdatenbearbeiter übertragen werden. Die Übertragung muss durch <i>Vertrag</i> erfolgen oder durch ein anderes Rechtsinstrument, das die Auftragsdatenbearbeiterin bzw. den Auftragsdatenbearbeiter bindet (z.B. durch Gesetz, Verordnung oder Regierungsratsbeschluss). Darin müssen der Gegenstand und die Dauer der Bearbeitung, die Art der Bearbeitung, die Art der zu bearbeitenden Personendaten, die Kategorien betroffener Personen und die Rechte und Pflichten der Auftragsdatenbearbeiterin bzw. des Auftragsdatenbearbeiters und des auftraggebenden öffentlichen Organ festgelegt werden. Insbesondere muss gewährleistet sein, <ul style="list-style-type: none"> - dass die Auftragsdatenbearbeiterin bzw. der Auftragsdatenbearbeiter nur auf Weisung des auftraggebenden öffentlichen Organs handelt, - dass die zur Auftragsdatenbearbeitung beigezogenen Personen sich zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen, - dass die Rechte der betroffenen Personen uneingeschränkt wahrgenommen werden können, - dass bei Vertragsende die Daten nach Wahl des auftraggebenden öffentlichen Organs vernichtet oder dem auftraggebenden öffentlichen Organ zurückgegeben werden, - dass die Auftragsdatenbearbeiterin bzw. der Auftragsdatenbearbeiter Dienste einer weiteren Auftragsdatenbearbeiterin oder eines weiteren Auftragsdatenbearbeiters nicht 	<p>«Das öffentliche Organ kann das Bearbeiten von Personendaten Dritten übertragen, wenn:</p> <ul style="list-style-type: none"> - keine rechtliche Bestimmung oder vertragliche Vereinbarung entgegensteht und - es wirksam sicherstellt, dass die Personendaten nur so bearbeitet werden, wie es das öffentliche Organ tun dürfte. <p><i>Es bleibt für den Umgang mit Informationen nach diesem Gesetz verantwortlich. Eine Auftragsdatenbearbeiterin beziehungsweise ein Auftragsdatenbearbeiter darf ohne die vorgängige schriftliche Zustimmung des auftraggebenden öffentlichen Organs die Datenbearbeitung keiner weiteren Auftragsdatenbearbeiterin und keinem weiteren Auftragsdatenbearbeiter übertragen.»</i></p> <p><i>Die einzelnen Anforderungen an die Auswahl des Dritten und die Sicherstellung, dass die Personendaten nur so bearbeitet werden, wie es das öffentliche Organ tun dürfte, können auf Verordnungsstufe detailliert geregelt werden (siehe unter «Umschreibung»).</i></p>	... wenn die Voraussetzungen für die Übertragung einer Datenbearbeitung, die Pflicht zur Sicherstellung, dass die Personendaten nur so bearbeitet werden, wie es das öffentliche Organ tun dürfte, den Verbleib der Verantwortung beim auftraggebenden öffentlichen Organ und das Verbot der Unterauftragsdatenbearbeitung ohne vorgängige schriftliche Einwilligung des verantwortlichen öffentlichen Organs im Gesetz festgehalten ist

	Thema	Rechtsgrundlage	Umschreibung	Mögliche Lösungen	Erfüllt, wenn ...
			oder nur mit vorgängiger schriftlicher Genehmigung durch das auftraggebende öffentliche Organ in Anspruch nimmt. Es wird empfohlen, den Begriff der Auftragsdatenbearbeitung (und nicht: Auftragsbearbeitung) zu verwenden: Es geht nicht einfach um die Bearbeitung eines Auftrags, sondern um eine Datenbearbeitung im Auftrag.		
5	Rechte der betroffenen Personen				
5.1	Transparenz über Datenbearbeitungen (WL Ziff. 4.1) Anpassungsbedarf prüfen	Art. 13, 20 und 36 VE-DSG Art. 5 Ziff. 4 lit. a E-Konv108 Art. 13 f. RL 2016/680 Art. 24 RL 2016/680	Transparenz bezüglich der Bearbeitung von Personendaten ist eines der Kernanliegen des Datenschutzrechts. Das Transparenzgebot verlangt: - die Pflicht der öffentlichen Organe (im Polizei- und Justizbereich), ein Verzeichnis der «Datenbearbeitungstätigkeiten» (der Verfahren, bei denen Personendaten bearbeitet werden) zu führen und zugänglich zu machen (→ Ziff. 6.7); - eine Pflicht der öffentlichen Organe, die betroffenen Personen über die Beschaffung von Personendaten zu informieren (→ Ziff. 5.2-5.3); - das Recht jeder Person zu erfahren, ob und, wenn ja, welche Daten über sie von einem öffentlichen Organ bearbeitet werden (Recht auf Zugang zu den eigenen Personendaten) (Recht auf Auskunft) (→ Ziff. 5.4-5.6).		... der Transparenzanspruch in seinen verschiedenen Ausformungen (Ziff. 5.2-5.6) im Gesetz festgeschrieben ist
5.2	Informationspflicht (WL ---) Anpassungsbedarf	Art. 13 VE-DSG Art. 7 ^{bis} E-Konv108 Art. 13 RL 2016/680	Verlangt wird eine (aktive) Information über das Beschaffen von Personendaten – <i>nicht mehr nur beim Bearbeiten von besonders schützenswerten (besonderen) Personendaten</i> . Zu informieren ist insbesondere über: - das verantwortliche öffentliche Organ (samt Kontaktdaten); - Rechtsgrundlage der Datenbearbeitung; - Zweck der Datenbearbeitung; - die bearbeiteten Daten oder die Kategorien der bearbeiteten Daten; - die Datenempfänger oder die Kategorien der Datenempfänger (wenn die Daten weitergegeben werden); - die Rechte der betroffenen Person. Werden die Daten systematisch erhoben (z.B. auf einem Anmelde- oder Gesuchsformular, auf Papier oder online), dann werden diese Angaben geschickterweise gleich auf diesem Formular angebracht. Bei einer anderen Datenbeschaffung sind die betroffenen Personen individuell zu informieren, sofern und soweit nicht eine Einschränkung zulässig ist (→ sogleich Ziff. 5.3).	<i>Informationspflicht bei der Beschaffung von Daten</i> <i>Das verantwortliche öffentliche Organ informiert über jede Beschaffung von Daten die betroffene Person; diese Informationspflicht gilt auch, wenn die Daten bei Dritten beschafft werden.</i> <i>Die Information umfasst insbesondere Angaben über:</i> - <i>das verantwortliche öffentliche Organ samt Kontaktdaten,</i> - <i>die bearbeiteten Daten oder die Kategorien der bearbeiteten Daten,</i> - <i>die Rechtsgrundlage und der Zweck des Bearbeitens,</i> - <i>die Datenempfänger oder die Kategorien der Datenempfänger, falls die Daten Dritten bekannt gegeben werden, und</i> - <i>die Rechte der betroffenen Person.</i>	... wenn die Informationspflicht samt Angaben über den Mindestinhalt im Gesetz verankert ist.
5.3	Einschränkung der Informationspflicht	Art. 14 VE-DSG Art. 7 ^{bis} Ziff. 1 ^{bis} E-Konv108	Die Informationspflicht entfällt, wenn - die betroffene Person über die Information, die ihr zukommen müsste, bereits verfügt (insbesondere also, wenn sie	<i>Die Informationspflicht entfällt, wenn</i> - <i>die betroffene Person bereits über die Informationen nach § ■■ [→ Ziff. 5.2]</i>	... wenn im Gesetz die Einschränkung der Informationspflicht nicht wei-

	Thema	Rechtsgrundlage	Umschreibung	Mögliche Lösungen	Erfüllt, wenn ...
	(WL ---) Anpassungsbedarf		<p>in einer früheren Phase der Beschaffung bereits einmal informiert worden ist);</p> <ul style="list-style-type: none"> - wenn die Beschaffung oder Bekanntgabe der Daten 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 - wenn die Information der betroffenen Person nicht oder nur mit unverhältnismässigem Aufwand möglich ist. <p>Ausserdem kann die Information im gleichen Masse eingeschränkt (ganz oder teilweise eingeschränkt oder aufgeschoben) werden wie der Zugang zu den eigenen Personendaten (Recht auf Auskunft) (→ Ziff. 5.6). Sobald der Einschränkungsground wegfällt, ist die Information nachzuholen.</p>	<p>verfügt,</p> <ul style="list-style-type: none"> - wenn das Bearbeiten der Personendaten gesetzlich ausdrücklich vorgesehen ist oder - die Information nicht oder nur mit unverhältnismässigem Aufwand möglich ist. <p>Die Übermittlung der Informationen kann unter denselben Voraussetzungen eingeschränkt werden wie der Zugang zu den eigenen Personendaten.</p>	tergehend vorgesehen ist.
5.4	Recht auf Auskunft, ob und welche Daten über einen bearbeitet werden (Zugang zu den eigenen Personendaten) (WL Ziff. 4.2) Anpassungsbedarf prüfen	Art. 20 VE-DSG Art. 8 Ziff. 1 lit. b E-Konv108 Art. 14 RL 2016/680 Art. 12 RL 2016/680 für die Modalitäten	<p>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. Es ist der Ausgangspunkt für die weiteren Rechte und Ansprüche der betroffenen Person. Zu regeln sind neben dem Anspruch auch bestimmte Modalitäten (Initiierung durch ein Begehren der betroffenen Person, Form der Auskunfterteilung). Es ist – zur Vereinfachung des Verfahrens – zulässig vorzusehen, dass auf Begehren der betroffenen Person auch direkt Einsicht in die relevanten Daten gewährt werden kann.</p> <p>Die Auskunft umfasst die Angaben, die bei der Informationspflicht gemacht werden müssen (→ Ziff. 5.2) und zusätzlich Angaben über:</p> <ul style="list-style-type: none"> - die Aufbewahrungsdauer der Personendaten und - die Herkunft der Daten. <p>Wie der Zugang zu den eigenen Personendaten gewährt wird, kann auf Verordnungsstufe konkretisiert werden (in der Regel schriftlich, im Einverständnis mit der gesuchstellenden Person auch durch Einsichtgewährung oder mündliche Mitteilung).</p>	<p>«Jede Person hat Anspruch darauf zu wissen, ob bei einem öffentlichen Organ Personendaten über sie vorhanden sind, und gegebenenfalls auf Zugang zu diesen eigenen Personendaten.</p> <p>Die Auskunft umfasst:</p> <ul style="list-style-type: none"> - die Angaben nach § ■■ [→ Ziff. 5.2], - Angaben über die Aufbewahrungsdauer der Personendaten und - Angaben über die Herkunft der Personendaten.» 	... das Recht auf Auskunft (Zugang zu den eigenen Personendaten) entsprechend im Gesetz festgeschrieben ist.
5.5	(Kosten) (WL Ziff. 4.3) Anpassungsbedarf prüfen	Art. 20 Abs. 1 VE-DSG Art. 8 Ziff. 1 lit. b E-Konv108 Art. 12 Abs. 4 RL 2016/680	<p>Das Recht auf Auskunft (und Einsicht) ist einer der wichtigsten Ausflüsse des verfassungsrechtlichen Persönlichkeitsschutzes. Grundsätzlich ist die Auskunfterteilung (der Zugang zu den eigenen Personendaten) kostenlos. Eine Ausnahme ist zulässig, wenn das Gesuch exzessiven Charakter hat.</p>	<p>«Die Auskunft wird kostenlos erteilt.» (evtl. Ausnahme bei Gesuchstellung mit exzessivem Charakter, wenn innert einer kurzen Frist [z.B. innert eines Jahres] ohne schutzwürdiges Interesse erneut ein Gesuch gestellt wird; ein schutzwürdiges Interesse ist etwa gegeben, wenn die Daten ohne Information der betroffenen Person verändert worden sind).</p>	... im Gesetz festgehalten wird, dass die Auskunft kostenlos zu erteilen ist (evtl. mit einer Ausnahme bei Gesuchstellung mit exzessivem Charakter)
5.6	Ausnahmen vom	Art. 21 VE-DSG	Die Auskunfterteilung (Einsichtgewährung) darf nicht ohne	«darf nur eingeschränkt, verweigert oder	... die Zulässigkeit der

	Thema	Rechtsgrundlage	Umschreibung	Mögliche Lösungen	Erfüllt, wenn ...
	Feststellung (WL Ziff. 4.6) Anpassungsbedarf (Anspruch auf Löschung)	spruch auf gerichtlichen Rechtsbehelf)	<p>Löschung, Sperrung der Bekanntgabe), die Beseitigung der Folgen der widerrechtlichen Bearbeitung (z.B. durch Löschung, Mitteilung an Datenempfänger, Veröffentlichung, Schadenersatz, Genugtuung) und die Feststellung der Widerrechtlichkeit der Bearbeitung.</p> <p>Ob ein schutzwürdiges Interesse vorliegt, ist höchstens 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 aufgrund des Persönlichkeitsrechts immer gegeben.</p> <p>Allenfalls kann ein Feststellungsanspruch an das Vorliegen eines schutzwürdigen Interesses geknüpft werden; bei den anderen Ansprüchen muss die Gefahr einer weiteren Bearbeitung oder Weitergabe zur Begründung genügen.</p> <p>Neu ist der <i>Anspruch auf Löschung</i> vorzusehen; er kann geltend gemacht werden bei widerrechtlich bearbeiteten Personendaten.</p> <p>Eine Löschung kann nur unterbleiben, wenn die <i>Personendaten</i> zu <i>Beweis Zwecken</i> aufbewahrt werden <i>müssen</i>. Die Dokumentationspflicht bei staatlichem Handeln kann in vielen Fällen auch mit anonymisierten Daten erfolgen; vgl. dazu Urteil des Verwaltungsgericht des Kantons Bern vom 15.04.2014 (100.2013.156U); SANDRA HUSI, Widerrechtlich bearbeitete Daten ins Archiv?, digma 2015, 24 ff.</p> <p>Der Lösungsanspruch kann allenfalls zu <i>bestimmten Zwecken</i> (Art. 16 Abs. 4 RL 2016/680, z.B. Schutz der öffentlichen Sicherheit, Nichtbehinderung behördlicher oder gerichtlicher Untersuchungen u.ä.; ähnlich Art. 9 E-Konv108) <i>spezialgesetzlich</i> eingeschränkt werden.</p> <p>Zur Verwendung der Begriffe «vernichten» bzw. «löschen» → Erläuterungen in Ziff. 3.7</p>	<i>Personendaten unterlassen wird,</i> - <i>die Folgen eines widerrechtlichen Bearbeitens beseitigt werden,</i> - <i>die Widerrechtlichkeit einer Bearbeitung festgestellt wird.</i> <i>Die Person kann insbesondere verlangen, dass sie betreffende Daten gelöscht werden oder ihre Bekanntgabe an Dritte gesperrt wird.»</i>	rechtlichen Bearbeitung, auf Beseitigung der Folgen einer widerrechtlichen Bearbeitung (inkl. Anspruch auf Löschung) und auf Feststellung der Widerrechtlichkeit einer Bearbeitung im Gesetz festgehalten ist.
5.9	Anspruch auf Sperrung der Bekanntgabe (WL Ziff. 4.7) Kein Anpassungsbedarf	Art. 30 VE-DSG Art. 8 Abs. 1 lit. d K108	Die von behördlicher Datenbearbeitung betroffene Person kann vom verantwortlichen öffentlichen Organ verlangen, dass es die Bekanntgabe von bestimmten Personendaten (an Private) sperrt. Das Recht ist voraussetzungslos zu gewähren oder darf höchstens von der Glaubhaftmachung eines schutzwürdigen Interesses abhängig gemacht werden. Das Gesetz hat auch festzulegen, unter welchen Voraussetzungen die Sperrung durchbrochen werden darf (z.B. wenn ein Gesetz die Bekanntgabe vorschreibt oder wenn durch die Sperrung die Erfüllung der gesetzlichen Aufgabe des verantwortlichen Organs verunmöglicht wird oder zur Durchsetzung von Rechtsansprüchen).	« <i>die betroffene Person(, die ein schutzwürdiges Interesse glaubhaft macht,) kann vom verantwortlichen Organ verlangen, dass es die Bekanntgabe von bestimmten Personendaten sperrt,</i> « <i>Die Bekanntgabe ist trotz Sperrung zulässig, wenn</i> - <i>das öffentliche Organ zur Bekanntgabe gesetzlich verpflichtet ist oder</i> - <i>die Bekanntgabe zur Erfüllung einer gesetzlichen Aufgabe zwingend notwendig ist oder</i> - <i>die um Bekanntgabe ersuchende Person glaubhaft macht, dass die Per-</i>	... das Recht auf Sperrung mit höchstens den erwähnten Durchbrechungsmöglichkeiten im Gesetz festgehalten ist.

	Thema	Rechtsgrundlage	Umschreibung	Mögliche Lösungen	Erfüllt, wenn ...
				<i>sonendaten zur Durchsetzung ihrer Rechtsansprüche erforderlich sind.»</i>	
5.10	«Beschwerde» an die Datenschutzaufsichtsbehörde (WL ---) Anpassungsbedarf	Art. 41 Abs. 5 VE-DSG (unge-nügend) Art. 12^{bis} Ziff. 3 E-Konv108 Art. 52 f. RL 2016/680 Art. 17 RL 2016/680	<p>Es ist vorzusehen, dass jede betroffene Person unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs das «Recht auf Beschwerde» bei der oder dem Datenschutzbeauftragten hat, wenn sie der Ansicht ist, dass die Bearbeitung der sie betreffenden Personendaten gegen die datenschutzgesetzlichen Vorschriften verstösst.</p> <p>Es dürfte sich wohl verwaltungsrechtlich um eine «Aufsichtsbeschwerde» («aufsichtsrechtliche Anzeige») handeln. Die/der Datenschutzbeauftragte hat sich mit dieser Anzeige zu befassen und hat der sich beschwerenden Person innert drei Monaten das Ergebnis der Abklärungen mitzuteilen. Bei Unzuständigkeit ist die Anzeige unverzüglich an die zuständige Datenschutzbeauftragte/den zuständigen Datenschutzbeauftragten weiterzuleiten. Befasst sich die Aufsichtsbehörde, an welche die Anzeige gerichtet wurde, nicht mit ihr, dann ist die Möglichkeit eines Rechtsmittels (wohl ebenfalls eine aufsichtsrechtliche Anzeige) gegen die säumige Aufsichtsstelle vorzusehen (Art. 53 Abs. 2 RL 2016/680).</p> <p>Die Wahrnehmung der Rechte der betroffenen Personen durch die oder den Datenschutzbeauftragte(n) im Sinne von Art. 17 RL 2016/680 (mit Verweis auf die Fälle nach Art. 13 Abs. 3, Art. 15 Abs. 3 und Art. 16 Abs. 4 RL 2016/680) kann bereichsspezifisch geregelt werden (wie es z.B. der Bund bisher in Art. 18 Abs. 3-5 BWIS getan hat).</p>	<p><i>Möglichkeit der aufsichtsrechtlichen Anzeige an die Datenschutzaufsichtsbehörde; falls nicht generell im Verwaltungsverfahrensrecht vorgesehen):</i> <i>(Die oder der Datenschutzbeauftragte)</i> <i>«- behandelt Eingaben von Betroffenen betreffend die Missachtung von Vorschriften dieses Gesetzes als aufsichtsrechtliche Anzeigen und informiert innerhalb von höchstens drei Monaten über das Ergebnis oder den Stand der Abklärungen;»</i> <i>Ausserdem ist sicherzustellen, dass die dafür nötigen Ressourcen vorhanden sind.</i></p>	<p>... die Pflicht der/des Datenschutzbeauftragten, Anzeigen («Beschwerden») von betroffenen Personen innert angemessener Frist (spätestens innert dreier Monate) zu behandeln, in einem Gesetz festgehalten ist und die/der Datenschutzbeauftragte mit den dafür notwendigen Ressourcen ausgestattet ist.</p>
6	Spezielle Regelungen				
6.1	Automatisierte Einzelentscheidungen (WL Ziff. 5.1) Anpassungsbedarf	Art. 15 und 20 Abs. 3 VE-DSG Art. 8 Abs. 1 lit. a und Abs. 2 E-Konv108 Art. 11 RL 2016/680	<p>Nach der K108 hat jede Person das Recht, nicht einer Entscheidung unterworfen zu sein, die sie erheblich beeinträchtigt und aufgrund eines ausschliesslich automatisierten Bearbeitens entstanden ist, ohne dass ihr Standpunkt berücksichtigt wird. Daraus kann als Minimallösung die Pflicht abgeleitet werden, dass</p> <ul style="list-style-type: none"> - die betroffene Person zu informieren ist, wenn eine automatisierte Einzelentscheidung erfolgt und diese rechtliche Wirkungen oder erhebliche Auswirkungen auf die betroffene Person hat, und - ihr die Möglichkeit gegeben wird, sich zur automatisierten Einzelentscheidung und zu den bearbeiteten Daten zu äussern. <p>Von Bedeutung ist diese Regelung v.a. im Privatrecht. Einzelentscheidungen mit rechtlichen Wirkungen ergehen im öffentlichen Recht in aller Regel in Form der Verfügung. Weil diese eröffnet werden müssen, ist die Information der betroffenen</p>	<p><i>Keine Regelung nötig, wenn sichergestellt ist, dass bei automatisierten Einzelentscheidungen die betroffene Person informiert wird (z.B. durch Eröffnung der entsprechenden Verfügung) und sie die Möglichkeit hat, sich zur Einzelentscheidung zu äussern (z.B. aufgrund des Anspruchs auf rechtliches Gehör).</i></p>	<p>... wenn keine Regelung geschaffen wird, weil sichergestellt ist, dass bei automatisierten Einzelentscheidungen die betroffene Person informiert wird (z.B. durch Eröffnung der entsprechenden Verfügung) und sie die Möglichkeit hat, sich zur Einzelentscheidung zu äussern (z.B. aufgrund des Anspruchs auf rechtliches Gehör).</p>

	Thema	Rechtsgrundlage	Umschreibung	Mögliche Lösungen	Erfüllt, wenn ...
			<p>Personen sichergestellt. Weil den betroffenen Personen im Vorfeld des Erlasses von Verfügungen ein Anspruch auf rechtliches Gehör zukommt, ist auch sichergestellt, dass die betroffenen Personen sich zur Einzelentscheidung äussern können. Aus diesem Grund ist davon auszugehen, dass es keine spezifische Regelung in den kantonalen (Informations- und) Datenschutzgesetzen braucht.</p> <p>Sollten in Zukunft bereichsspezifisch automatisierter Einzelentscheidungen eingeführt werden, die nicht zum Erlass einer Verfügung führen, aber trotzdem rechtliche Wirkungen oder erhebliche Auswirkungen auf die betroffene Person haben, dann ist darauf zu achten, dass im entsprechenden Fachgesetz eine ausdrückliche und klare formellgesetzliche Grundlage dafür geschaffen und dabei sichergestellt ist, dass den betroffenen Personen die Möglichkeit gegeben wird, sich zur automatisierten Einzelentscheidung und zu den bearbeiteten Daten zu äussern.</p>		
6.2	<p>Datenschutz-Folgenabschätzung (WL ---)</p> <p>Anpassungsbedarf</p>	<p>Art. 16 Abs. 1 und 2 VE-DSG Art. 8^{bis} Ziff. 2 E-Konv108 Art. 27 RL 2016/680</p>	<p>Neu verlangen die übergeordneten Rechtsgrundlagen eine Datenschutz-Folgenabschätzung durch das verantwortliche öffentliche Organ. Diese Abschätzung enthält zumindest 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, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz der Grundrechte der betroffenen Personen sichergestellt und der Nachweis erbracht werden soll, dass dieses Gesetz eingehalten wird.</p> <p>Diese Datenschutz-Folgenabschätzung ist im Grunde genommen nichts anderes als die Vorbereitung des verantwortlichen öffentlichen Organs, damit es die Voraussetzungen für den Nachweis der Einhaltung der Datenschutzvorschriften (→ Ziff. 4.10) erbringen kann. Ausserdem beschlägt sie dieselben Punkte, die bei Vorhaben, die voraussichtlich zu einem hohen Risiko für die Grundrechte der betroffenen Personen führen, für eine Vorabkonsultation (→ Ziff. 6.3) erarbeitet werden müssen.</p>	<p>«Das verantwortliche öffentliche Organ muss bei jedem Vorhaben für eine Personendatenbearbeitung eine Datenschutz-Folgenabschätzung durchführen.» «Die Folgenabschätzung enthält mindestens:</p> <ul style="list-style-type: none"> - 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, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz der Grundrechte der betroffenen Personen sichergestellt und der Nachweis erbracht werden soll, dass dieses Gesetz eingehalten wird.» <p>Die Inhaltsumschreibung (und weitere Konkretisierungen) können auch auf Verordnungsstufe geregelt werden.</p>	<p>... wenn die Pflicht des verantwortlichen öffentlichen Organs, bei vorgesehenen Personendatenbearbeitungen eine Datenschutz-Folgenabschätzung durchzuführen, im Gesetz verankert ist.</p>
6.3	<p>Vorabkonsultation (WL Ziff. 5.2, «Vorabkontrolle»)</p> <p>Anpassungsbedarf</p>	<p>Art. 16 Abs. 3 und 4 VE-DSG Art. 28 RL 2016/680 («Vorherige Konsultation der Aufsichtsbehörde»)</p>	<p>Die Richtlinie 2016/680 (wie auch die Datenschutz-Grundverordnung) sehen vor, dass bestimmte Vorhaben der oder dem Datenschutzbeauftragten vorab zur Konsultation (nach dem früheren Recht: «Vorabkontrolle») zu unterbreiten sind:</p> <ul style="list-style-type: none"> - Vorhaben, bei denen in einer Datenschutz-Folgenabschätzung 	<p>«Vorabkonsultation der oder des Datenschutzbeauftragten Das verantwortliche öffentliche Organ legt der oder dem Datenschutzbeauftragten frühzeitig zur Vorabkonsultation vor:</p> <ul style="list-style-type: none"> - Rechtsetzungsprojekte, die den Daten- 	<p>... die Pflicht zur Vorabkonsultation bei Rechtsetzungsvorhaben und bei Vorhaben zur Bearbeitung von Personendaten, die zu einem hohen Risiko für die</p>

	Thema	Rechtsgrundlage	Umschreibung	Mögliche Lösungen	Erfüllt, wenn ...
			<p>zung ein hohes Risiko festgestellt wurde,</p> <ul style="list-style-type: none"> - Vorhaben, bei denen die Form der Datenbearbeitung (insbesondere bei Verwendung neuer Technologien, Mechanismen oder Verfahren) ein hohes Risiko für die Grundrechte der betroffenen Person, - Rechtsetzungsvorhaben, welche das Bearbeiten von Personendaten betreffen. <p>Die oder der Datenschutzbeauftragten 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, die Sensitivität der Daten usw. sein (Art. 28 Abs. 3 RL 2016/680).</p> <p>Ziel dieser Vorabkonsultation ist es, den Datenschutz rechtzeitig sicherzustellen, insbesondere:</p> <ul style="list-style-type: none"> - bei Rechtsetzungsvorhaben dafür zu sorgen, dass die verfassungs- und datenschutzrechtlichen Vorgaben berücksichtigt werden, - bei anderen (IT-)Vorhaben die Ermittlung und Bewertung der Risiken und der geplanten Massnahmen, um die Risiken auf ein zulässiges Mass zu reduzieren, zu überprüfen und dafür zu sorgen, dass gegebenenfalls mit rechtlichen, organisatorischen oder technischen Massnahmen das Risiko weiter reduziert wird. <p>Die oder der Datenschutzbeauftragte kann bei Rechtsetzungsvorhaben Stellung nehmen.</p> <p>Bei anderen Vorhaben kann die oder der Datenschutzbeauftragte Empfehlungen (→ Ziff. 8.5b) abgeben, wenn die geplante Datenbearbeitung gegen Datenschutzbestimmungen verstossen würde, insbesondere weil das verantwortliche öffentliche Organ die Risiken für die Grundrechte der betroffenen Personen nicht hinreichend ermittelt oder nicht hinreichend eingedämmt hat.</p> <p>Sobald alle erforderlichen Unterlagen vorliegen, hat die oder der Datenschutzbeauftragte innert sechs Wochen (verlängerbar um einen Monat) seine Beurteilung (Empfehlung) abgeben und/oder seine Befugnisse ausüben (→ Ziff. 8.5). Eine fixe Frist ist nur beschränkt tauglich. Kleine Vorabkonsultationen sollen viel rascher erledigt werden können – bei grossen Projekten findet eine Vorabkonsultation ohnehin in verschiedenen Projektphasen gestaffelt statt. Im Gesetz könnte – wenn eine Frist genannt werden soll – «innert angemessener Frist» stehen.</p> <p>Die vom Bund in der Vernehmlassungsvorlage vorgeschlagene Regelung setzt die Vorgabe der RL 2016/680 nur ungenü-</p>	<p><i>schutz betreffen, und</i></p> <ul style="list-style-type: none"> - <i>Vorhaben zur Bearbeitung von Personendaten, die (aufgrund der Art der Bearbeitung oder der zu bearbeitenden Daten) zu einem hohen Risiko für die Grundrechte der betroffenen Personen führen.</i> <p><i>Die oder der Datenschutzbeauftragte kann eine Liste der Bearbeitungsvorgänge erstellen, die vorab zur Konsultation zu unterbreiten sind.»</i></p>	<p>Grundrechte der betroffenen Personen führen, im Gesetz festgehalten ist</p>

	Thema	Rechtsgrundlage	Umschreibung	Mögliche Lösungen	Erfüllt, wenn ...
			gend um. Die Vorabkonsultation ist ein wirksames Mittel des präventiven Datenschutzes und verhindert, dass Vorhaben hinterher mit grösserem Aufwand verbessert werden müssen oder gar nicht in Betrieb genommen werden können.		
6.4	Meldepflichten bei Datenschutzverletzungen (WL ---) Anpassungsbedarf (Begriffsdefinition) (WL ---) Anpassungsbedarf	Art. 17 VE-DSG Art. 7 Ziff. 2 E-Konv108 Art. 30 RL 2016/680 (an Aufsichtsbehörde) Art. 31 RL 2016/680 (an betroffene Personen)	Verletzungen des Datenschutzes (Begriffsdefinition → nächste Tabellenzeile) sind unverzüglich der oder dem Datenschutzbeauftragten zu melden. Diese Meldung kann ausbleiben, wenn die Verletzung voraussichtlich zu keinem Risiko für die Grundrechte der betroffenen Person führt. Der Inhalt der Meldung (Beschreibung der Verletzung, der wahrscheinlichsten Folgen der Verletzung sowie der ergriffenen und vorgesehenen Massnahmen zur Wiederherstellung des Schutzes bzw. zur Abmilderung der Folgen der Verletzung) kann auf Verordnungsstufe umschrieben werden. Das verantwortliche öffentliche Organ informiert ausserdem die betroffenen Personen, wenn die Umstände es erfordern oder die oder der Datenschutzbeauftragte es verlangen. Die Benachrichtigung hat insbesondere zu erfolgen, wenn die betroffenen Personen zur Abwendung des Schadens Massnahmen ergreifen können. Die Benachrichtigung kann unterbleiben, wenn durch nachträgliche Vorkehrungen sichergestellt werden konnte, dass das hohe Risiko für die Grundrechte der betroffenen Personen aller Wahrscheinlichkeit nach nicht mehr besteht. Die Benachrichtigung der betroffenen Personen kann ausserdem ganz oder teilweise eingeschränkt oder aufgeschoben werden, wenn öffentliche oder private Geheimhaltungsinteressen überwiegen. Bei Auftragsdatenbearbeitung: Falls die Verletzung bei einer Auftragsdatenbearbeitung geschieht, hat die Auftragsdatenbearbeiterin bzw. der Auftragsdatenbearbeiter unverzüglich das auftraggebende öffentliche Organ zu benachrichtigen, das dann die Verletzung der oder dem Datenschutzbeauftragten meldet (Regelung hier oder im Zusammenhang mit der Auftragsdatenbearbeitung → Ziff. 4.12). Was eine «Datenschutzverletzung» ist, muss definiert werden. Die Umschreibung in Art. 17 VE-DSG («unbefugte Datenbearbeitung») ist zu weit; somit würden auch geringfügige «Verletzungen» zu einer Meldepflicht führen.	Meldung von Datenschutzverletzungen « ^x Das verantwortliche öffentliche Organ meldet der oder dem Datenschutzbeauftragten ohne unangemessene Verzögerung eine Datenschutzverletzung. ^x Eine Datenschutzverletzung liegt vor» [→ unten in diesem Tabellenfeld] « ^x Eine Meldepflicht besteht nicht, wenn die Datenschutzverletzung voraussichtlich nicht zu einem Risiko für die Grundrechte der betroffenen Person führt. ^x Das öffentliche Organ informiert ausserdem die betroffenen Personen, wenn die Umstände dies erfordern oder der oder die Datenschutzbeauftragte es verlangt. ^x Die Benachrichtigung der betroffenen Personen kann ausserdem ganz oder teilweise eingeschränkt oder aufgeschoben werden, wenn öffentliche oder private Geheimhaltungsinteressen überwiegen» (oder Verweis auf eine entsprechende generelle Einschränkungsregelung). Bei Auftragsdatenbearbeitung regeln oder hier: « ^x Der Auftragsdatenbearbeiter informiert das auftraggebende öffentliche Organ unverzüglich über eine Datenschutzverletzung.» «Eine Datenschutzverletzung liegt vor, wenn die Sicherheit so verletzt wird, dass bearbeitete Personendaten unwiederbringlich vernichtet werden oder verloren gehen, unbeabsichtigt oder unrechtmässig verändert oder offenbart werden oder dass Unbefugte Zugang zu solchen Personendaten erhalten.»	... wenn eine Meldepflicht bei Datenschutzverletzungen (inkl. Begriffsdefinition) im Gesetz verankert ist.
6.5	Mitteilung von	Art. 19 lit. b VE-DSG	Wenn eine Datenbearbeitung nicht (mehr) rechtmässig ist,	Das öffentliche Organ informiert die Emp-	... wenn die Pflicht zu

	Thema	Rechtsgrundlage	Umschreibung	Mögliche Lösungen	Erfüllt, wenn ...
	Berichtigungen, Löschungen/Vernichtungen, Datenschutzverletzungen und Einschränkungen der Bearbeitung an die Empfänger der Personendaten (WL ---) Anpassungsbedarf	Art. 16 Abs. 5 RL 2016/680	<p>muss dafür gesorgt werden, dass Stellen und Personen, welche die entsprechenden Personendaten vorgängig empfangen haben, über die Berichtigung, Löschung oder Vernichtung von Daten, über Datenschutzverletzungen (→ Ziff. 6.4) sowie über Einschränkungen der Bearbeitung (→ Ziff. 5.7 am Ende), informiert werden, damit die Daten nicht von den Dritten, an die sie übermittelt wurden, weiter bearbeitet werden, weil sie keine Kenntnis vom entsprechenden Vorgang haben. Von einer Mitteilung darf nur abgesehen werden, wenn sie nicht oder nur mit unverhältnismässigem Aufwand erfolgen kann. Das darf nicht leichthin angenommen werden. Das verantwortliche öffentliche Organ muss mindestens den Versuch unternommen haben und dabei auf konkrete, nur mit erheblichem Einsatz überwindbare Schwierigkeiten gestossen sein.</p>	<p>fängerinnen und Empfänger von Personendaten über jede Berichtigung, Löschung oder Vernichtung von Daten, über Datenschutzverletzungen (→ Ziff. 6.4) sowie über Einschränkungen der Bearbeitung nach Art. 16 (→ Ziff. 5.7 am Ende), es sei denn, eine solche Mitteilung ist nicht oder nur mit unverhältnismässigem Aufwand möglich.</p>	<p>Mitteilung im Gesetz verankert ist.</p>
6.6	Regeln für das Bearbeiten von Personendaten zu nicht personenbezogenen Zwecken (WL Ziff. 5.3) Kein Anpassungsbedarf	Art. 32 VE-DSG Art. 5 Ziff.4 lit. b E-Konv108 Art. 4 Abs. 3 RL 2016/680	<p>Personendaten können zu nicht personenbezogenen Zwecken weiterbearbeitet werden, wenn zwar Daten über bestimmte oder bestimmbare Personen bearbeitet werden, aber die Person als solche nicht im Fokus steht, sondern Statistik, Planung oder Forschung (z.T. auch «wissenschaftliche Zwecke» genannt, obwohl «wissenschaftlich» eigentlich nur die Methode beschreibt). Es ist zulässig, solche Weiter-Bearbeitungen zu privilegieren (z.B. vom Vorliegen einer spezifischen gesetzlichen Grundlage für die Weiter-Bearbeitung oder Bekanntgabe zu befreien), wenn sichergestellt wird, dass die Daten anonymisiert werden, sobald es der Bearbeitungszweck zulässt und die Ergebnisse so veröffentlicht werden, dass es unmöglich ist, auf die betroffenen Personen zurück zu schliessen. Es ist u.U. sinnvoll, für die Bekanntgabe von Personendaten an Empfänger ausserhalb der Verwaltung zusätzliche Auflagen vorzusehen (Garantien, Weitergabeverbot, Verstärkung mit Konventionalstrafe u.ä.). Die <i>erstmalige</i> Erhebung von Personendaten zu nichtpersonenbezogenen Zwecken braucht hingegen eine separate gesetzliche Grundlage und ist in der «Aufgabenerfüllungs-Grundlage» nicht mitenthalten. Allenfalls kann die Bekanntgabe für einen nicht personenbezogenen Zweck mit einer Strafbestimmung verstärkt werden für den Fall, dass die Empfängerin oder der Empfänger die Personendaten, die sie oder er von einem öffentlichen Organ zum Bearbeiten zu nicht personenbezogenen Zwecken erhalten hat, vorsätzlich oder fahrlässig entgegen der Verpflichtung für andere Zwecke bearbeitet oder an Dritte weitergibt.</p>	<p>z.B. zum Bearbeiten zu einem nicht personenbezogenen Zweck (durch das verantwortliche öffentliche Organ selber): <i>«Ein öffentliches Organ darf Personendaten zu einem nicht personenbezogenen Zweck, namentlich für Statistik, Planung oder Forschung, bearbeiten, wenn es</i></p> <ul style="list-style-type: none"> - <i>diese Daten nicht mehr für einen personenbezogenen Zweck verwendet oder weitergibt und</i> - <i>diese Daten anonymisiert oder pseudonymisiert, sobald es der Bearbeitungszweck erlaubt, und</i> - <i>die Ergebnisse der Bearbeitung nur so bekannt gibt, dass keine Rückschlüsse auf betroffene Personen möglich sind.»</i> <p>z.B. zur Bekanntgabe für einen nicht personenbezogenen Zweck: <i>«Das öffentliche Organ kann anderen öffentlichen Organen im Kanton, in anderen Kantonen oder im Bund Personendaten zur Bearbeitung für einen nicht personenbezogenen Zweck, namentlich für Statistik, Planung oder Forschung, bekannt geben, sofern dies nicht durch eine besondere Geheimhaltungsbestimmung ausgeschlossen ist. Die Empfängerin oder der Empfänger hat sich zu verpflichten:</i></p> <ul style="list-style-type: none"> - <i>die Personendaten zu anonymisieren</i> 	<p>... im Gesetz sichergestellt ist, dass die Personendaten, sobald es der nicht personenbezogenen Zweck des Bearbeitens es zulässt, anonymisiert werden und die Resultate nur so veröffentlicht werden, dass es unmöglich ist, auf die betroffenen Personen zurück zu schliessen.</p>

	Thema	Rechtsgrundlage	Umschreibung	Mögliche Lösungen	Erfüllt, wenn ...
				<p>oder zu pseudonymisieren, sobald es der Bearbeitungszweck zulässt, und</p> <ul style="list-style-type: none"> - die Auswertungen nur so bekannt zu geben, dass keine Rückschlüsse auf betroffene Personen möglich sind. <p>Privaten kann das öffentliche Organ Personendaten zur Bearbeitung für Zwecke der Forschung bekannt geben, sofern dies nicht durch eine besondere Geheimhaltungsbestimmung ausgeschlossen ist und sich die Empfängerin oder der Empfänger zusätzlich zu den Anforderungen von Abs. 2 verpflichtet,</p> <ul style="list-style-type: none"> - die Personendaten nicht für andere Zwecke zu bearbeiten und - die Personendaten nicht an Dritte weiterzugeben und - für die Informationssicherheit zu sorgen.» <p>Allenfalls Sicherung mit einer Strafbestimmung: «Wer Personendaten, die sie oder er von einem öffentlichen Organ zum Bearbeiten zu nicht personenbezogenen Zwecken erhalten hat, vorsätzlich oder fahrlässig entgegen der Verpflichtung gemäss § ■■ für andere Zwecke bearbeitet oder an Dritte weitergibt, wird mit Busse bestraft.» (allenfalls Verweis auf das Übertretungsstrafgesetz für die Höhe der Busse, die Bemessungsgrundsätze usw.).</p>	
6.7	<p>Verzeichnis der Datenbearbeitungstätigkeiten (WL Ziff. 5.4)</p> <p>Anpassungsbedarf prüfen</p>	<p>Art. 36 VE-DSG Art. 24 RL 2016/680 (nicht mehr öffentliches Register)</p>	<p>Die Richtlinie 2016/680 sieht eine Pflicht, ein Verzeichnis über die Datenbearbeitungstätigkeiten zu führen, nur für Justiz- und Polizeibehörden vor. Dementsprechend kann eine solche Pflicht bereichsspezifisch umgesetzt werden (z.B. im Polizeigesetz und im Einführungsgesetz zur StPO – der Bund behält die Registrierpflicht für Bundesorgane voraussichtlich im DSG bei, weshalb sie nicht in der StPO – und damit auch für kantonale Justizorgane verbindlich – festgelegt wird).</p> <p>Ein solches Verzeichnis ist nicht identisch mit dem Nachweis, dass die Datenschutzbestimmungen eingehalten sind (→ Ziff. 4.10), sondern höchstens eine Art «Nebenprodukt». Die Kantone können <i>im Sinne der Transparenz</i> z.B. die Führung eines Verzeichnisses der Verfahren, bei denen Personendaten bearbeitet werden, beibehalten (so z.B. § 24</p>	<p>Eine Pflicht zur Führung eines Verzeichnisses der Datenbearbeitungstätigkeiten existiert nur im Anwendungsbereich der Richtlinie 2016/680 (justiziell/ polizeilich) → Verankerung der Verzeichnispflicht bereichsspezifisch im Polizeigesetz und im Einführungsgesetz zur StPO. Allenfalls im Sinne der Transparenz Pflicht zur Führung eines Verzeichnisses der Verfahren, bei denen Personendaten bearbeitet werden (so z.B. § 24 IDG/BS).</p>	<p>... wenn eine Pflicht zur Führung eines Verzeichnisses über die Datenbearbeitungstätigkeiten für Justiz- und Polizeibehörden im entsprechenden Sachrecht verankert ist.</p>

	Thema	Rechtsgrundlage	Umschreibung	Mögliche Lösungen	Erfüllt, wenn ...
			IDG/BS, http://www.staatskanzlei.bs.ch/oeffentlichkeitsprinzip/verfahren.html).		
6.8	Grenzüberschreitender Datenverkehr (WL Ziff. 5.5) Kein Anpassungsbedarf	Art. 5 und 6 VE-DSG Art. 12 E-Konv108 Art. 35-39 RL 2016/680	Für den Fall des grenzüberschreitenden Datenverkehrs ist im Gesetz festzuhalten, dass die grenzüberschreitende Übermittlung von Personendaten an Empfänger, für welche die Europaratskonvention 108 nicht gilt, – zusätzlich zu den allgemeinen Bekanntgabevoraussetzungen – nur dann zulässig ist, wenn beim Empfänger ein adäquates Datenschutzniveau sichergestellt ist (i.S.v. Art. 12 K108). Es ist sinnvoll, (evtl. im Verordnungsrecht) festzuhalten, dass öffentliche Organe sich bei der Frage, ob in einem Staat ein adäquates Datenschutzniveau sichergestellt ist, auf die vom Bundesrat nach Art. 5 Abs. 7 VE-DSG zu erlassende Liste stützen darf.	<i>Festschreiben der Voraussetzungen nach Art. 12 K108 im Gesetz</i>	... im Gesetz festgeschrieben ist, dass eine Datenbekanntgabe ins Ausland nur unter den Voraussetzungen, wie sie Art. 12 K108 umschreibt, zulässig ist.
7	Rechtsbehelfe, Haftung, Sanktionen				
7.1	Rechtsbehelfe (Rechtsweggarantie) (WL Ziff. 6.1) Kein Anpassungsbedarf	Art. 34 Abs. 5 VE-DSG Art. 8 lit. f E-Konv108 Art. 10 E-Konv108 Art. 12^{bis} Ziff. 6 E-Konv108 Art. 53 und 54 RL 2016/680	Die von einer Bearbeitung ihrer Daten betroffenen Personen müssen bei einer dadurch erfolgenden Verletzung ihrer Rechte mit einem Rechtsmittel an eine gerichtliche Instanz gelangen können – allenfalls nach dem verwaltungsinternen Beschwerdeverfahren. (zur Anfechtbarkeit von Entscheidungen des Kontrollorgans siehe unten → Ziff. 8.10)	<i>(im Zusammenhang mit den Rechten und Ansprüchen der betroffenen Personen [oben → Ziff. 5.4 ff.] «Entspricht ein öffentliches Organ einem Begehren aufgrund dieses Gesetzes nicht, erlässt es eine begründete Verfügung» → daraus folgende Anfechtbarkeit aufgrund z.B. des Verwaltungsverfahrensgesetzes oder der Verwaltungsprozessordnung</i>	... im Resultat erreicht wird, dass die betroffene Person (allenfalls nach Ausschöpfung des verwaltungsinternen Beschwerdeweges) mit einem Rechtsmittel an eine gerichtliche Instanz gelangen kann.
7.2	Haftung (WL Ziff. 6.2) Kein Anpassungsbedarf	Art. 10 E-Konv108 Art. 56 RL 2016/680	Entsteht einer Person wegen einer widerrechtlichen Bearbeitung ihrer Personendaten ein Schaden, so ist ihr ein Anspruch auf Schadenersatz einzuräumen.	<i>z.B. Verantwortlichkeitsgesetz, Staatshaftungsgesetz</i>	... eine gesetzliche Grundlage für die Geltendmachung von Schadenersatz bei widerrechtlicher Datenbearbeitung besteht.
7.3	Sanktionen (WL Ziff. 6.3) Kein Anpassungsbedarf	Art. 50 ff. VE-DSG (Strafbestimmungen) Art. 10 E-Konv108 Art. 57 RL 2016/680	Ein Gesetz muss Sanktionen vorsehen, die bei Verstössen gegen das Datenschutzgesetz anzuwenden sind.	<i>z.B. Strafbestimmung für Amtsgeheimnisverletzungen; Strafbestimmung für die auftragswidrige Verwendung oder Bekanntgabe von Personendaten durch die Beauftragten bei einer Datenbearbeitung im Auftrag</i>	... ein Gesetz Sanktionen vorsieht, die bei Verstössen gegen das Datenschutzgesetz anzuwenden sind

	Thema	Rechtsgrundlage	Umschreibung	Mögliche Lösungen	Erfüllt, wenn ...
8	Datenschutzbeauftragte				
8.1	Datenschutzbeauftragte(r) (WL Ziff. 7.1) Kein Anpassungsbedarf	Art. 37-49 VE-DSG Art. 12 ^{bis} Ziff. 1 E-Konv108 Art. 44 RL 2016/680	Die behördliche Datenbearbeitung ist durch ein völlig unabhängiges Kontrollorgan zu kontrollieren. Dafür muss das Gesetz ausdrücklich eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten vorsehen. Die Stelle muss sich an den Anforderungen an die Unabhängigkeit (unten Ziff. 8.7 f.) und Wirksamkeit der Kontrolle (unten Ziff. 8.9) messen lassen.		... die Schaffung der Stelle einer oder eines Datenschutzbeauftragten im Gesetz festgeschrieben ist (und die Aufgaben nach Ziff. 8.4, die Befugnisse nach Ziff. 8.5, die Pflichten nach Ziff. 8.6 festgeschrieben sowie die Unabhängigkeit nach Ziff. 8.7 f. und die Wirksamkeit der Kontrolle nach Ziff. 8.9 sichergestellt sind)
8.2	Ausnahmen von der Aufsicht (WL ---)	Art. 2 Abs. 3 und 4 VE-DSG Art. 12 ^{bis} Ziff. 9 E-Konv108 Art. 45 Abs. 2 RL 2016/680	Als «Gegenstück» zur Anwendbarkeit des Datenschutzgesetzes auch in hängigen gerichtlichen Verfahren (→ Ziff. 2.3 und 2.4) sollen Datenbearbeitungen in hängigen gerichtlichen Verfahren nicht der Aufsicht der oder des Datenschutzbeauftragten unterstehen. Dementsprechend ist eine Ausnahme vorzusehen. Allenfalls können aufgrund der Gewaltenteilung auch das kantonale Parlament und die kantonale Exekutive von der Aufsicht durch die Datenschutzbeauftragte oder den Datenschutzbeauftragten ausgenommen werden.	«Der Aufsicht der oder des Datenschutzbeauftragten unterstehen nicht: - Datenbearbeitungen in hängigen Verfahren der Zivil- und Strafrechtspflege; - Datenbearbeitungen in hängigen Verfahren der Verfassungs- und Verwaltungsgerichtsbarkeit»	... wenn Datenbearbeitungen in hängigen gerichtlichen Verfahren von der Aufsicht der oder des Datenschutzbeauftragten ausgenommen sind.
8.3	Qualifikation (WL ---) Anpassungsbedarf	Art. 43 Abs. 2 RL 2016/680	Die oder der Datenschutzbeauftragte muss die für die Erfüllung ihrer/seiner Aufgaben und zur Ausübung ihrer/seiner Befugnisse erforderliche Qualifikation, Erfahrung und Sachkunde insbesondere im Bereich des Datenschutzes verfügen.	Die Aufsichtsstelle «wird von einer in Datenschutzfragen ausgewiesenen Fachperson (der oder dem Beauftragten) geleitet», «zur oder zum Datenschutzbeauftragten gewählt werden kann eine in Datenschutzfragen ausgewiesene Fachperson»	
8.4	Aufgaben (WL Ziff. 7.2) Anpassungsbedarf	Art. 40 Abs. 1, Art. 49 VE-DSG Art. 12 ^{bis} Ziff. 2 lit. b, e, E-Konv108 Art. 12 ^{bis} Ziff. 2 ^{bis} , 3, 5 ^{bis} , 7 K 108 (09.16) Art. 45 RL 2016/680	Die oder der Datenschutzbeauftragte muss mindestens die folgenden Aufgaben zu erfüllen haben:		
8.4a	Kontrolle (WL Ziff. 7.2a) Kein Anpassungsbedarf	Art. 40 Abs. 1 VE-DSG Art. 46 Abs. 1 lit. a RL 2016/680	Kontrolle - unabhängige, anlassfreie Prüfung nach einem durch die Datenschutzbeauftragte/den Datenschutzbeauftragten autonom aufzustellenden Prüfprogramm - anlassbezogene Kontrolle einer konkreten Datenbearbeitung – insbesondere auf «Beschwerde» (aufsichtsrechtliche	Die oder der Datenschutzbeauftragte «überwacht die Umsetzung der Bestimmungen über den Datenschutz», «kontrolliert nach einem autonom aufzustellenden Prüfprogramm die Anwendung der Bestimmungen über den Datenschutz»	... der Kontrollauftrag im Gesetz festgelegt ist

	Thema	Rechtsgrundlage	Umschreibung	Mögliche Lösungen	Erfüllt, wenn ...
			Anzeige) von betroffenen Personen hin	mit Informationen	
8.4b	Beratung (WL Ziff. 7.2b) Kein Anpassungsbedarf	Art. 49 lit. a VE-DSG Art. 12 ^{bis} Ziff. 2 ^{bis} K 108 (09.16) Art. 46 Abs. 1 lit. c und e RL 2016/680	Beratung der öffentlichen Organe - in der Rechtsetzung und - in der Rechtsanwendung und Beratung der betroffenen Personen	Die oder der Datenschutzbeauftragte «nimmt Stellung zu Erlassen, die für den Datenschutz erheblich sind»; «das Kontrollorgan berät die öffentlichen Organe in Fragen des Datenschutzes (und der Informationssicherheit)», «berät die betroffenen Personen über ihre Rechte.»	... der Beratungsauftrag im Gesetz festgelegt ist
8.4c	Sensibilisierung der verantwortlichen öffentlichen Organe und der Bevölkerung (WL ---) Anpassungsbedarf	Art. 49 lit. c VE-DSG Art. 12 ^{bis} Ziff. 2 lit. e K 108 (09.16) Art. 46 Abs. 1 lit. b und d RL 2016/680	Zu den Aufgaben der/des Datenschutzbeauftragten gehört auch die Sensibilisierung der verantwortlichen öffentlichen Organe für ihre Pflichten und der Öffentlichkeit für die Anliegen des Datenschutzes (z.B. auch im Hinblick auf die Eigenverantwortung der betroffenen Personen).	Die oder der Datenschutzbeauftragte «sensibilisiert die öffentlichen Organe für ihre datenschutzrechtlichen Pflichten und die Öffentlichkeit für die Anliegen des Datenschutzes»	... der Sensibilisierungsauftrag im Gesetz festgelegt ist
8.4d	Verfolgen der massgeblichen Entwicklungen (WL ---) Anpassungsbedarf	Art. 46 Abs. 1 lit. j RL 2016/680	Verfolgung der massgeblichen Entwicklungen in der Informations- und Kommunikationstechnologie, soweit sie sich auf den Schutz von Personendaten auswirken	Die oder der Datenschutzbeauftragte «verfolgt die für den Schutz von Personendaten massgeblichen Entwicklungen»	... der Auftrag, die für den Schutz von Personendaten massgeblichen Entwicklungen zu verfolgen, im Gesetz festgelegt ist
8.4e	Zusammenarbeit (WL ---) Anpassungsbedarf prüfen	Art. 49 lit. b VE-DSG Art. 46 Abs. 1 lit. h RL 2016/680	Die Datenschutzaufsichtsbehörden sind zur Zusammenarbeit mit anderen Datenschutzaufsichtsbehörden zusammen; sie gewähren sich gegenseitig Amtshilfe.	Die oder der Datenschutzbeauftragte «arbeitet zur Erfüllung ihrer oder seiner Aufgaben mit den Organen der anderen Kantone, des Bundes und des Auslandes, welche die gleichen Aufgaben erfüllen, zusammen»	... wenn die Pflicht zur Zusammenarbeit im Gesetz festgelegt ist
8.4f	Kosten (WL ---) Anpassungsbedarf prüfen	Art. 46 Abs. 3 RL 2016/680	Die Erfüllung der Aufgaben der oder des Datenschutzbeauftragten ist für die betroffenen Personen unentgeltlich. Bei offenkundig unbegründeten oder — besonders wegen häufiger Wiederholung — exzessiven Anträgen kann die Aufsichtsbehörde eine angemessene Gebühr auf der Grundlage ihrer Verwaltungskosten verlangen oder sich weigern, aufgrund des Antrags tätig zu werden. In diesem Fall trägt die Aufsichtsbehörde die Beweislast dafür, dass der Antrag offensichtlich unbegründet oder exzessiv ist.	Kein Vorsehen einer Kostenüberbindung oder ausdrücklicher Ausschluss: «Für die Aufgabenerfüllung der oder des Datenschutzbeauftragten werden den betroffenen Personen keine Kosten überbunden.» Allenfalls mit einer expliziten Ausnahme (Kostenüberbindung oder Nichtannahme bei offensichtlich unbegründeten oder exzessiven Anträgen)	... aus dem Gesetz hervorgeht, dass für die Aufgabenerfüllung der oder des Datenschutzbeauftragten keine Kosten erhoben werden (evtl. mit einer Ausnahme bei offensichtlich unbegründeten oder exzessiven Anträgen)
8.4g	weitere (WL Ziff. 7.2c) Kein Anpassungsbedarf	Art. 49 lit. f VE-DSG	Es können dem Kontrollorgan weitere Aufgaben übertragen werden, z.B. die Vermittlung zwischen betroffenen Personen und öffentlichen Organen (wenn beide Seiten sich auf den Vermittlungsversuch einlassen). Es ist aber darauf zu achten, dass solche Aufträge nicht die Unabhängigkeit der Kontrolle gefährden.	Die oder der Datenschutzbeauftragte «vermittelt zwischen öffentlichen Organen und betroffenen Personen»	... der oder dem Datenschutzbeauftragten keine weiteren Aufträge erteilt werden, die zu einer Gefährdung der Unabhängigkeit der Kontrolle führen.

	Thema	Rechtsgrundlage	Umschreibung	Mögliche Lösungen	Erfüllt, wenn ...
			Der Vorbehalt einer Genehmigung bestimmter Datenbearbeitungen durch die oder den Datenschutzbeauftragte(n) ist problematisch, wenn bzw. weil dadurch die Verantwortlichkeit (→ Ziff. 4.9) nicht mehr beim datenbearbeitenden öffentlichen Organ liegt. Eine Schlichtungsaufgabe im Zusammenhang mit dem Öffentlichkeitsprinzip kann problematisch sein, weil es im Vorfeld die Beratung des öffentlichen Organs und evtl. der gesuchstellenden Person) praktisch ausschliesst (oder nach der Beratung eine unvoreingenommene Schlichtung nicht mehr möglich ist).		
8.5	Befugnisse (WL Ziff. 7.3)	Art. 12 ^{bis} Ziff. 2 lit. a, b-d E-Konv108 Art. 47 RL 2016/680	Das Kontrollorgan (der/die Datenschutzbeauftragte) muss mindestens die folgenden Befugnisse besitzen:		
8.5a	Untersuchung (WL Ziff. 7.3a) Kein Anpassungsbedarf	Art. 41 VE-DSG Art. 12 ^{bis} Ziff. 2 lit. a K 108 (09.16) Art. 47 Abs. 1 RL 2016/680	Umfassende Untersuchungsbefugnisse: die Befugnis, ungeachtet allfälliger Geheimhaltungspflichten Ermittlungen durchzuführen, alle für die Erfüllung des Kontrollauftrages erforderlichen Informationen über Datenbearbeitungen einzuholen, Einsicht in alle Unterlagen zu nehmen, Besichtigungen durchzuführen und sich Bearbeitungen vorführen zu lassen	<i>Die oder der Datenschutzbeauftragte «ist befugt, ungeachtet allfälliger Geheimhaltungspflichten Ermittlungen durchzuführen, alle für die Erfüllung des Kontrollauftrages erforderlichen Informationen über Datenbearbeitungen einzuholen, Einsicht in alle Unterlagen zu nehmen, Besichtigungen durchzuführen und sich Bearbeitungen vorführen zu lassen»</i>	... der oder dem Datenschutzbeauftragten im Gesetz umfassende Untersuchungsbefugnisse i.S. der Umschreibung – also ungeachtet allfälliger Geheimhaltungspflichten – zuerkannt werden
8.5b	Einwirkung (WL Ziff. 7.3b) Anpassungsbedarf prüfen	Art. 43 VE-DSG Art. 12 ^{bis} Ziff. 2 lit. a K 108 (09.16) Art. 47 Abs. 2 RL 2016/680	Die oder der Datenschutzbeauftragte muss über wirksame Einwirkungsbefugnisse verfügen. Dazu gehört das Recht, sich zu Vorhaben zu äussern (Vorabkonsultation, oben Ziff. 6.3), zu Datenbearbeitungen <i>Hinweise</i> abzugeben, aber auch zu konkreten Datenbearbeitungen (förmliche) <i>Empfehlungen</i> zu erlassen. Das öffentliche Organ, an welches eine Empfehlung gerichtet ist, muss sich dazu äussern: Es muss erklären, ob es ihr folgen will oder nicht.	z.B. <i>«Die oder der Datenschutzbeauftragte kann zum Bearbeiten von Personendaten Empfehlungen abgeben. Das öffentliche Organ, an welches die Empfehlung gerichtet ist, hat gegenüber der oder dem Datenschutzbeauftragten zu erklären, ob es der Empfehlung folgen will.»</i>	... der oder dem Datenschutzbeauftragten im Gesetz wirksame Einwirkungsbefugnisse i.S. der Umschreibung zuerkannt werden.
8.5c	Anordnung (Verfügung) Anpassungsbedarf prüfen	Art. 43 VE-DSG Art. 12 ^{bis} Ziff. 2 lit. c und Art. 12 ^{bis} Ziff. 6 K 108 (09.16) Art. 47 Abs. 2 lit. b und c RL 2016/680	Der Aufsichtsbehörde muss neu die Befugnis zukommen, bei Verstössen gegen das Datenschutzrecht <i>verbindliche Anordnungen</i> (in Form einer Verfügung) treffen zu können (z.B. ein widerrechtliches Datenbearbeiten einzustellen oder auf eine widerrechtliche Datenbekanntgabe zu verzichten). Die Anordnung kann z.B. als «Weisung» bezeichnet werden, wenn dieser Begriff im kantonalen Recht nicht schon anderweitig besetzt ist (z.B. im Kanton Zürich für die Vorlagen an das Parlament, im Bund «Botschaft» genannt). Eine solche verbindliche Anordnung kann nach der Ablehnung einer Empfehlung (→ Ziff. 8.5b) erlassen werden oder direkt, wenn absehbar ist, dass das öffentliche Organ eine Empfehlung ablehnen oder ihr keine Folge leisten wird. Diese verbindliche Anordnung in Form einer Verfügung ist	<i>«Wenn ein öffentliches Organ erklärt, der Empfehlung der oder des Datenschutzbeauftragten nicht folgen zu wollen, oder tatsächlich der Empfehlung nicht folgt, kann die oder der Datenschutzbeauftragte die Empfehlung oder Teile davon als verbindliche Anordnung (als Weisung) in Form einer Verfügung erlassen, wenn das Interesse an der Durchsetzung schwer wiegt. Keine Anordnung (Weisung) kann gegenüber dem Kantonsgericht (Verwaltungsgericht) erlassen werden. Die oder der Datenschutzbeauftragte kann</i>	... wenn der oder dem Datenschutzbeauftragten die Befugnis zukommt, bei Verstössen gegen das Datenschutzrecht verbindliche Anordnungen (Weisung) (in Form einer Verfügung) zu erlassen, die vor einem Gericht angefochten werden können.

	Thema	Rechtsgrundlage	Umschreibung	Mögliche Lösungen	Erfüllt, wenn ...
			anfechtbar (→ Ziff. 8.10). Sinnvollerweise ist der Rechtsweg direkt ans Kantonsgericht (Verwaltungsgericht) festzulegen.	<i>direkt eine Anordnung (Weisung) erlassen, wenn absehbar ist, dass das öffentliche Organ eine Empfehlung ablehnen oder ihr keine Folge leisten wird. Das öffentliche Organ, an welches die Anordnung (Weisung) gerichtet ist, kann sie mit einer Beschwerde (einem Rekurs) nach den allgemeinen Vorschriften beim Kantonsgericht (Verwaltungsgericht) anfechten.»</i>	
8.5d	Vorsorgliche Massnahmen (WL ---) Anpassungsbedarf	Art. 42 VE-DSG Art. 47 Abs. 2 lit. c RL 2016/680	Falls schutzwürdige Interessen offensichtlich gefährdet oder verletzt werden, muss die oder der Datenschutzbeauftragte die Befugnis haben, vorsorglich eine Datenbearbeitung zu untersagen.	<i>«Werden schutzwürdige Interessen offensichtlich gefährdet oder verletzt, so kann die oder der Datenschutzbeauftragte im Sinne einer vorsorglichen Massnahme anordnen, dass das öffentliche Organ die Bearbeitung bis zur erfolgten Überprüfung durch das Kantonsgericht einschränkt oder einstellt.»</i>	... wenn der oder dem Datenschutzbeauftragten die Befugnis zukommt, bei offensichtlichen Gefährdungen oder Verletzungen schutzwürdiger Interessen vorsorgliche Massnahmen (Einschränkung oder Einstellung von Datenbearbeitungen) anzuordnen.
8.5e	Klage, Anzeige (WL Ziff. 7.3c) Anpassungsbedarf prüfen	Art. 45 VE-DSG Art. 12^{bis} Ziff. 2 lit. d K 108 (09.16) Art. 47 Abs. 5 RL 2016/680	Klage-/Anzeigebefugnis: das Recht, bei gerichtlichen Instanzen Klage zu erheben oder eine Anzeige einzureichen bei Verstössen gegen das Datenschutzgesetz. Das Anzeigerecht bei Straftaten ergibt sich aus Art. 301 StPO. Eine Anzeigepflicht (Art. 302 Abs. 2 StPO) ist – mindestens im Bereich der vermittelnden Tätigkeit – nicht festzulegen. Dauert der Verstoß an, ist eine verbindliche Anordnung in Betracht zu ziehen (→ Ziff. 8.5c). Für Fälle, bei denen weder eine Strafanzeige angezeigt ist noch eine Weisung in Betracht zu ziehen ist, muss die Möglichkeit der aufsichtsrechtlichen Anzeige an die vorgesetzte Behörde des gegen das Datenschutzrecht verstossenden öffentlichen Organs bestehen, was sich aus dem allgemeinen Verwaltungsrecht ergeben kann. Andernfalls ist diese Möglichkeit im Datenschutzgesetz vorzusehen.	<i>Falls sich das Recht auf aufsichtsrechtliche Anzeige an die vorgesetzte Behörde eines gegen das Datenschutzrecht verstossenden öffentlichen Organs nicht aus dem allgemeinen Verwaltungsrecht ergibt: «Die oder der Datenschutzbeauftragte kann der vorgesetzten Behörde eines gegen das Datenschutzrecht verstossenden öffentlichen Organs einen solchen Verstoß anzeigen.»</i>	... der oder dem Datenschutzbeauftragten im Gesetz eine Klage-/Beschwerdebefugnis i.S. der Umschreibung zuerkannt wird.
8.5f	Sanktionen (WL ---) Anpassungsbedarf prüfen	Art. 50 ff. VE-DSG Art. 12^{bis} Ziff. 2 lit. c E-Konv108 Art. 57 RL 2016/680	Die Aufsichtsbehörde soll bei Verstössen gegen das Datenschutzrecht administrative Sanktionen verhängen können; gedacht ist etwa an Bussen. Die Sanktionen müssen wirksam, verhältnismässig und abschreckend sein. Bussen innerhalb der Verwaltung, d.h. innerhalb desselben Budgets, machen nur begrenzt Sinn. Jeder Kanton muss sich deshalb überlegen, ob er eine entsprechende Regelung schaffen will.	<i>Falls die oder der Datenschutzbeauftragte gegenüber gegen das Datenschutzrecht verstossenden öffentlichen Organe Bussen verhängen können soll: entsprechende Regelung ausarbeiten (z.B. Bussenrahmen, Zumessungskriterien).</i>	... aus dem Gesetz die Sanktionsbefugnis (mit der notwendigen Detailregelung) zu entnehmen ist, falls der Kanton eine solche schaffen will.
8.6	Pflichten (WL Ziff. 7.4)	div. Art. im VE-DSG Art. 12 Ziff. 3, 5^{bis}, 5^{ter}, 7 E-Konv108	Mindestens die folgenden Pflichten des Kontrollorgans (des/der Datenschutzbeauftragten) müssen im Gesetz ausdrücklich festgelegt werden:		

	Thema	Rechtsgrundlage	Umschreibung	Mögliche Lösungen	Erfüllt, wenn ...
		Art. 44 Abs. 2 sowie Art. 49, 50, 52 RL 2016/680			
8.6a	Behandlung von Eingaben (WL Ziff. 7.4a) Anpassungsbedarf	Art. 12 ^{bis} Ziff. 3 E-Konv108 Art. 52 RL 2016/680	Behandlung von Eingaben: die Pflicht, «Beschwerden» (→ Ziff. 5.10) von Personen in Bezug auf den Schutz ihrer Rechte und grundlegenden Freiheiten hinsichtlich der Bearbeitung von Personendaten anzuhören und zu behandeln.	→ Ziff. 5.10.	→ Ziff. 5.10.
8.6b	Amtshilfe (WL Ziff. 7.4b) Kein Anpassungsbedarf	Art. 46 und 47 VE-DSG Art. 12 ^{bis} Ziff. 7 E-Konv108 Art. 50 RL 2016/680	Amtshilfe: Pflicht, zur Erfüllung ihrer Kontrollaufgaben mit den Kontrollorganen (Datenschutzbeauftragten) der anderen Kantone, des Bundes und des Auslandes zusammenzuarbeiten.	<i>Die oder der Datenschutzbeauftragte «arbeitet zur Erfüllung der Kontrollaufgabe mit den Kontrollorganen der anderen Kantone, des Bundes und des Auslandes zusammen»</i>	... der oder dem Datenschutzbeauftragten im Gesetz die Pflicht zur Zusammenarbeit mit anderen Kontrollorganen auferlegt wird.
8.6c	Geheimhaltungspflicht (WL Ziff. 7.4c) Kein Anpassungsbedarf	Art. 12 ^{bis} Ziff. 5 ^{ter} E-Konv108 Art. 44 Abs. 2 RL 2016/680	Berufsgeheimnis: die Pflicht, dieselben Geheimhaltungsbestimmungen einzuhalten wie die öffentlichen Organe, welche Personendaten bearbeiten, und zwar auch über die Beendigung der Funktion hinaus.	<i>«Die Mitglieder, Mitarbeiterinnen und Mitarbeiter der oder des Datenschutzbeauftragten sind hinsichtlich Personendaten, die sie bei ihrer Tätigkeit zur Kenntnis nehmen, zur gleichen Verschwiegenheit verpflichtet wie das bearbeitende öffentliche Organ» Als «Gegenstück» zur Untersuchungsbefugnis auch bei Geheimhaltungspflichten: « Die oder der Beauftragte und die Mitarbeitenden unterstehen bezüglich der Informationen, die sie bei ihrer Tätigkeit zur Kenntnis nehmen, der gleichen Pflicht zur Verschwiegenheit wie das bearbeitende öffentliche Organ.»</i>	... der oder dem Datenschutzbeauftragten im Gesetz die Pflicht zur Geheimhaltung (auch über die Beendigung der Funktion hinaus) auferlegt wird.
8.6d	Berichterstattung (WL Ziff. 7.4d) Kein Anpassungsbedarf	Art. 48 VE-DSG Art. 12 ^{bis} Ziff. 5 ^{bis} E-Konv108 Art. 49 RL 2016/680	Berichterstattung: die Pflicht, einerseits dem Wahlorgan gegenüber Rechenschaft abzulegen über die Tätigkeit, das finanzielle Gebaren usw., und andererseits das Wahlorgan und die Öffentlichkeit periodisch sowie bei Bedarf über die Resultate der (Kontroll-)Tätigkeit zu informieren, also über wichtige Feststellungen und Beurteilungen sowie über die Wirkung der Datenschutzbestimmungen (Erfolge und Defizite im Datenschutzbereich).	<i>Die oder der Datenschutzbeauftragte «legt dem Wahlorgan gegenüber Rechenschaft über seine Tätigkeit ab und informiert das Wahlorgan und die Öffentlichkeit periodisch und bei Bedarf über wichtige Feststellungen und Beurteilungen sowie über die Wirkung der Datenschutzbestimmungen»</i>	... der oder dem Datenschutzbeauftragten im Gesetz die Pflicht zur Rechenschaftsablage und Berichterstattung im Sinne der Umschreibung auferlegt wird.
8.7	Sicherstellung der völligen Unabhängigkeit (WL Ziff. 7.5 + Anhang)	Art. 37 Abs. 3 VE-DSG Art. 12 ^{bis} Ziff. 4 E-Konv108 Art. 42 und 43 RL 2016/680	Die rechtlichen Vorgaben verlangen ein Kontrollorgan, das seine Aufgabe unabhängig wahrnehmen kann. Das verlangt einerseits, dass die Unabhängigkeit ausdrücklich im Gesetz festgehalten ist. Andererseits muss die Unabhängigkeit auch mit institutionellen Sicherungen garantiert werden (sogleich Ziff. 8.8).	<i>z.B. Verwendung der Begriffe «Unabhängigkeit», «unabhängige Aufsichtsstelle» o.ä. im Paragrafentitel oder Gesetzestext</i>	... die Garantie der Unabhängigkeit ausdrücklich im Gesetz festgehalten ist.
8.8	(institutionelle Garantien für die völlige Unabhängigkeit)	Art. 37-39 VE-DSG Art. 12 ^{bis} Ziff. 4 K 108 (09.16) Art. 42 Abs. 2 RL 2016/680	Neben der ausdrücklichen Festschreibung der völligen Unabhängigkeit des Kontrollorgans braucht es auch institutionelle Garantien dafür.	<i>Weisungsunabhängigkeit: «erfüllt seine Aufgaben weisungsunabhängig»</i>	... die Weisungsunabhängigkeit, die Unvereinbarkeit, das Wahlverfahren,

	Thema	Rechtsgrundlage	Umschreibung	Mögliche Lösungen	Erfüllt, wenn ...
	gigkeit) (WL Ziff. 7.6 + Anhang) Anpassungsbedarf prüfen	(Weisungsunabhängigkeit) Art. 42 Abs. 3 RL 2016/680 (Unvereinbarkeitsregelungen) Art. 42 Abs. 5 RL 2016/680 (Auswahl des eigenen Personals) Art. 42 Abs. 6 RL 2016/680 (Budget) Art. 43 Abs. 1 RL 2016/680 (Wahlverfahren) Art. 43 Abs. 3 RL 2016/680 (Wahl auf Amtszeit) Art. 43 Abs. 4 RL 2016/680 (Amtsenthebung)	Die Garantien müssen mindestens folgende Elemente umfassen: - Weisungsunabhängigkeit - Unvereinbarkeitsregelung: anderes öffentliches Amt, leitende Funktion in politischer Partei, andere Erwerbstätigkeit? - Regelung des Wahlverfahrens (im Sinne der Verhinderung einer «Wahl der Kontrolleure durch die Kontrollierten»: möglichst allein durch das Parlament oder unter Beteiligung des Parlaments [Genehmigung der durch die Exekutive vorgenommenen Wahl, Wahl durch das Parlament auf Antrag der Exekutive usw.]) - Wahl auf eine feste Amtszeit von mindestens vier oder mehr Jahren - Beschränkung der Amtsenthebung: nur bei dauernder Amtsunfähigkeit oder schwerer Amtspflichtverletzung (i.d.R. durch einen Beschluss der Wahlbehörde mit qualifiziertem Mehr) - eigenes Budget - Auswahl des eigenen Personals (im Rahmen des genehmigten Budgets)	<i>Unvereinbarkeiten:</i> «Die oder der Beauftragte darf kein anderes öffentliches Amt, keine leitende Funktion in einer politischen Partei und keine andere Erwerbstätigkeit ausüben. Die Wahlbehörde kann Ausnahmen bewilligen. Versieht die oder der Beauftragte ein Teilpensum der Aufsichtsstelle, so darf die Bewilligung der anderen Erwerbstätigkeit nicht verweigert werden, wenn durch diese Erwerbstätigkeit die Ausübung der Funktion sowie Unabhängigkeit und Ansehen nicht beeinträchtigt werden.» <i>Regelung des Wahlverfahrens (Wahlorgan, Wahlverfahren) und der Amtszeit Amtsenthebung:</i> «Die oder der Datenschutzbeauftragte darf nur des Amtes enthoben werden bei dauernde Amtsunfähigkeit oder bei schwerer Amtspflichtverletzung. Die Enthebung bedarf eines Beschlusses des Wahlorgans mit Zweidrittelsmehr.» <i>Budget:</i> Sicherstellung, dass die Aufsichtsstelle ein eigenes Budget erstellt, über das sie nach der Genehmigung durch das Parlament auch selber verfügt. <i>Anstellung des Personals der Aufsichtsstelle:</i> «Die oder der Beauftragte ist im Rahmen des vom Parlament genehmigten Budgets für die Personalgeschäfte der weiteren Mitarbeitenden der Aufsichtsstelle und für personalrechtliche Massnahmen zuständig».	die Amtszeit, die Möglichkeit der Amtsenthebung, das Budget und die Auswahl des eigenen Personals im Sinne der Umschreibung im Gesetz geregelt sind.
8.9	Sicherstellung einer effektiven Aufgabenerfüllung (WL Ziff. 7.7) Anpassungsbedarf prüfen	Art. 12 ^{bis} Ziff. 5 E-Konv108 Art. 47 Abs. 4 RL 2016/680	Die rechtlichen Vorgaben verlangen eine wirksame aktive Kontrolle. Eine solche aktive Kontrolle muss anlassfrei möglich sein und nach einem aufgrund einer Risikobeurteilung durch die Aufsichtsstelle autonom erstellten Prüfprogramm erfolgen. Das verlangt, - dass das Kontrollorgan erstens die nötigen Befugnisse besitzt (oben Ziff. 8.5), - dass zweitens die erforderlichen personellen und finanziellen Ressourcen zugeteilt erhält, und - dass drittens an das Kontrollorgan (bzw. an seine Leitung)	<i>Zuteilung angemessener Ressourcen, in mittleren und grösseren Kantonen sicher ein Kontrollorgan mit mehreren Stellen (Recht, Informatik[revision]), in kleineren Kantonen wohl mindestens mit 50%-100%-Pensum</i> <i>Alternative Möglichkeit: allenfalls gemeinsame regionale Lösungen verschiedener (kleinerer) Kantone</i>	... wenn durch Zuteilung genügender personeller und finanzieller Ressourcen und durch hohe fachliche Anforderungen sichergestellt ist, dass die Datenschutzkontrolle effektiv ist.

	Thema	Rechtsgrundlage	Umschreibung	Mögliche Lösungen	Erfüllt, wenn ...
			<p>hohe fachliche Anforderungen gestellt werden (Qualifikation → Ziff. 8.3; Weiterbildung).</p> <p>Eine effektive Kontrolle kann beispielsweise in keiner Weise sichergestellt werden, wenn ein kantonales Kontrollorgan aufgrund seines kleinen Pensums (bei kleinen Kantonen z.B. 30-40%) faktisch höchstens reaktiv tätig werden kann, wenn ein Anliegen an es herangetragen wird. Ausserdem wird mit einem nicht vollen Pensum die Frage der Neben(erwerbs)-tätigkeiten (bzw. der Bewilligung solcher Tätigkeiten) aktuell, was im Zusammenhang mit der Unabhängigkeit wiederum Fragen aufwirft.</p>		
8.10	Anfechtbarkeit von Entscheidungen der Aufsichtsbehörde (WL Ziff. 7.8)	<p>Art. 44 VE-DSG</p> <p>Art. 12^{bis} Ziff. 6 E-Konv108</p> <p>Art. 53 RL 2016/680</p>	<p>Entscheidungen des Kontrollorgans müssen vor Gericht angefochten werden können. In dem Ausmass, in welchem seinen Rechtshandlungen (z.B. verbindliche Anordnungen, vorsorgliche Massnahmen; siehe oben Ziff. 8.5c+d) verbindliche Wirkung zukommt, müssen sie einer gerichtlichen Kontrolle unterworfen werden können.</p>	<p><i>Keine explizite Regelung im DSG/IDG, wenn sich aus den geltenden Rechtschutzregeln im Kanton und in der BV die Anfechtbarkeit von Entscheidungen der oder des Datenschutzbeauftragten zweifelsfrei ergibt.</i></p>	<p>... die gerichtliche Anfechtbarkeit von Entscheidungen des Kontrollorgans im Ausmass der Verbindlichkeit sichergestellt ist</p>