Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
Gesetz über die Information und den Datenschutz (Informations- und Datenschutzgesetz, IDG)	**Gesetz über die Information und den Datenschutz** (Informations- und Datenschutzgesetz, IDG)	
Vom 10. Februar 2011 (Stand 1. Januar 2018)	Änderung vom …	*Revisionsanlass: Anpassung des basellandschaftlichen Informations- und Datenschutzgesetzes (IDG) an die geänderten Vorgaben des europäischen Datenschutzrechts[1].* *Als Wegleitung für die kantonalen Rechtsetzungsarbeiten stellte die Konferenz der Kantonsregierungen (KdK) den Kantonen einen Leitfaden zur Verfügung[2]. Dieses von ausgewiesenen Datenschutzfachleuten kompetent verfasste Hilfsmittel entstand in der KdK-Arbeitsgruppe Datenschutz unter massgeblicher Mitwirkung von Vertretungen der kantonalen Datenschutz-Aufsichtsstellen, einschliesslich der Baselbieter Aufsichtsstelle Datenschutz.*
§ 1 Gegenstand und Zweck [2] Es bezweckt: b. die Grundrechte von Personen zu schützen, über welche die öffentlichen Organe Personendaten bearbeiten.	**§ 1 Gegenstand und Zweck** [2] Es bezweckt: b. die Grundrechte von *natürlichen* Personen zu schützen, über welche die öffentlichen Organe Personendaten bearbeiten.	*Siehe unten die Bemerkungen zu § 3 Absatz 3.*

[1] • 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 (nachfolgend EU-Richtlinie 2016/680)
• Entwurf 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) (nachfolgend E-Übereinkommen SEV 108)

[2] Leitfaden der Konferenz der Kantonsregierungen [KdK] zum Anpassungsbedarf bei den kantonalen Datenschutzgesetzen (nachfolgend KdK-Leitfaden)

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
§ 2 Geltungsbereich	**§ 2 Geltungsbereich**	
[2] Es findet keine Anwendung:	[2] Es findet keine Anwendung:	
a. soweit ein öffentliches Organ am wirtschaftlichen Wettbewerb teilnimmt und dabei privatrechtlich handelt;	a. [unverändert, neues Satzzeichen am Ende].	
b. in hängigen Verfahren der Zivilrechts- und Strafrechtspflege;	b. *Aufgehoben.*	
c. in hängigen Verfahren der Verfassungs- und Verwaltungsgerichtsbarkeit.	c. *Aufgehoben.*	
[Absatz 2bis des Revisionsentwurfs ist neu.]	*[2bis] Die Rechte und Ansprüche der betroffenen Person während hängigen Verfahren der Zivilrechts- und Strafrechtspflege, der Verfassungs- und Verwaltungsgerichtsbarkeit sowie während hängigen Rechtshilfeverfahren richten sich ausschliesslich nach dem anwendbaren Verfahrensrecht.*	*Der neue Absatz 2bis ersetzt die bisherigen Buchstaben b und c. Sein Wortlaut entspricht dem Vorschlag im KdK-Leitfaden[3], ergänzt mit der Erwähnung der Rechtshilfeverfahren analog den Datenschutzgesetzen von Bund und anderen Kantonen. Die Neuformulierung ist nötig, weil nach den europarechtlichen Vorgaben[4] für hängige Gerichtsverfahren keine generellen Geltungsbereich-Ausnahmen in der Datenschutzgesetzgebung mehr vorgesehen werden dürfen.* *Die spezifischen Verfahrensgesetze wie etwa die Schweizerische Strafprozessordnung (StPO)[5] und die Schweizerische Zivilprozessordnung (ZPO)[6] behalten als bereichsspezifisches Datenschutzrecht weiterhin ihre Gültigkeit. Dies gilt auch für die Grundsätze unseres Informations- und Datenschutzgesetzes IDG, beispielsweise über die verantwortliche Behörde oder über den Umgang mit Informationen usw.*

[3] Seite 2 / Ziffer 2.3 KdK-Leitfaden (vollständiger Titel mit Link in Fussnote 2)
[4] Artikel 2 EU-Richtlinie 2016/680 / Artikel 3 E-Übereinkommen SEV 108 (vollständige Titel mit Links in Fussnote 1)
[5] SR 312
[6] SR 272

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
§ 3 Begriffe [3] Personendaten sind Informationen, die sich auf eine bestimmte oder bestimmbare natürliche oder juristische Person beziehen.	**§ 3 Begriffe** [3] Personendaten sind Informationen, die sich auf eine bestimmte oder bestimmbare natürliche ~~*oder juristische*~~ Person beziehen.	*Absatz 3: Anders als die internationalen Vorgaben (und die meisten europäischen Staaten) schützen die schweizerischen Datenschutzgesetze bisher nicht nur natürliche, sondern auch juristische Personen. Der Bundesrat will nun bei der Revision des Bundes-Datenschutzgesetzes auf den Einbezug der juristischen Personen verzichten. Die Kantone sind zwar nicht verpflichtet, diese bundesrechtliche Anpassung nachzuvollziehen. Allerdings erscheint – in Übereinstimmung mit dem KdK-Leitfaden[7] – eine abweichende kantonale Regelung nicht sinnvoll. Deshalb soll bei der Begriffsdefinition «Personendaten» in § 3 Absatz 3 die Erwähnung der juristischen Personen entfallen. Als Folge davon ist auch § 1 Absatz 2 Buchstabe b anzupassen (siehe oben).* *Für juristische Personen bleibt ein umfassender Schutz bestehen, wie er durch die Artikel 28 ff. des Schweizerischen Zivilgesetzbuchs ZGB (Persönlichkeitsverletzungen wie beispielsweise Rufschädigung), das Bundesgesetz über das Urheberrecht und verwandte Schutzrechte URG, das Bundesgesetz gegen den unlauteren Wettbewerb UWG oder durch die Bestimmungen zum Schutz von Berufs-, Geschäfts- und Fabrikationsgeheimnissen sowie Artikel 13 "Schutz der Privatsphäre" der Bundesverfassung gewährleistet wird.*

[7] Seite 3 / Ziffer 3.2 des KdK-Leitfadens (vollständiger Titel mit Link in Fussnote 2), Artikel 3 Ziffer 1 EU-Richtlinie 2016/680 / Artikel 2 Buchstabe a E-Übereinkommen SEV 108 (vollständige Titel mit Links in Fussnote 1)

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
(§ 3 Begriffe) [4] Besondere Personendaten sind: a. Personendaten, bei deren Bearbeitung eine besondere Gefahr der Grundrechtsverletzung besteht, insbesondere Angaben über: 1. die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten, 2. die Gesundheit, das Erbgut, die Intimsphäre oder die Rassenzugehörigkeit, 3. Massnahmen der sozialen Hilfe, 4. administrative oder strafrechtliche Verfolgungen und Sanktionen. b. Zusammenstellungen von Informationen, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlauben (Persönlichkeitsprofil).	(§ 3 Begriffe) [4] Besondere Personendaten sind: a. [unverändert] 1. [unverändert], 2. die Gesundheit, das Erbgut (*genetische Daten*), die Intimsphäre oder die *ethnische Herkunft*, *2.[bis] Behinderungen,* 3. [unverändert], 4. [unverändert, neues Satzzeichen am Ende], *5. 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).* b. [unverändert]	*Ziffer 2: Gemäss Empfehlung des KdK-Leitfadens wird der Begriff «Erbgut» mit dem Klammervermerk «genetische Daten» ergänzt[8] und der Begriff «Rassenzugehörigkeit» durch «ethnische Herkunft» ersetzt[9]. Ferner ist zur Klarstellung festzuhalten, dass unter die «Intimsphäre» auch Angaben über das Sexualleben oder die sexuelle Orientierung fallen, weshalb sie nicht gesondert erwähnt werden müssen[10].* *Ziffer 2[bis]: Personendaten über Behinderungen werden grundsätzlich der Gesundheit (siehe Ziffer 2) zugerechnet, was nicht ohne weiteres mit einem modernen Begriff der Behinderung als interaktiv hervorgerufener Nachteil vereinbar erscheint. Im Sinn einer Klarstellung und Präzisierung soll § 3 Absatz 4 mit dem Begriff «Behinderungen» ergänzt werden. Ausschlaggebend für die Qualifizierung als besondere Personendaten nach kantonalem Recht ist die Vermutung des Bestehens einer «besonderen Gefahr der Grundrechtsverletzung» durch Datenbearbeitung.* *Die neue Ziffer 5 übernimmt einen Formulierungsvorschlag im KdK-Leitfaden[11]. In die Kategorie der besonderen Personendaten (= besonders schützenswerte Personendaten) fallen vor allem auch biometrische Daten, da sie die eindeutige Identifizierung einer Person ermöglichen oder bestätigen. Dazu zählen Gesichtsbilder, d.h. mit Gesichtserkennungsprogrammen gewonnene Daten (also nicht jede Fotografie eines Gesichts), daktyloskopische Daten, Stimmmuster, Iris-Muster.*

[8] Seite 4 / Ziffer 3.5 KdK-Leitfaden (vollständiger Titel mit Link in Fussnote 2), Artikel 3 Ziffern 12 f. und Artikel 10 EU-Richtlinie 2016/680 / Artikel 6 Ziffer 1 E-Übereinkommen SEV 108 (vollständige Titel mit Links in Fussnote 1)

[9] Seite 4 / Ziffer 3.3 KdK-Leitfaden (vollständiger Titel mit Link in Fussnote 2), Artikel 3 und 10 EU-Richtlinie 2016/680 / Artikel 6 E-Übereinkommen SEV 108 (vollständige Titel mit Links in Fussnote 1)

[10] Seite 4 / Ziffer 3.4 KdK-Leitfaden (vollständiger Titel mit Link in Fussnote 2), Artikel 10 EU-Richtlinie 2016/680 / Artikel 6 Absatz 1 E-Übereinkommen SEV 108 (vollständige Titel mit Links in Fussnote 1)

[11] Seite 4 / Ziffer 3.6 KdK-Leitfaden (vollständiger Titel mit Link in Fussnote 2), Artikel 3 Ziffer 13 und Artikel 10 EU-Richtlinie 2016/680 / Artikel 6 Ziffer 1 E-Übereinkommen SEV 108 (vollständige Titel mit Links in Fussnote 1)

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
(§ 3 Begriffe) 5 Bearbeiten ist jeder Umgang mit Informationen wie das Beschaffen, Aufbewahren, Verwenden, Verändern, Bekanntgeben oder Vernichten, unabhängig von den angewandten Mitteln und Verfahren.	(§ 3 Begriffe) 5 Bearbeiten ist jeder Umgang mit Informationen, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, ~~Verwenden~~ *Lesen*, Verändern, Bekanntgeben, *Archivieren, Löschen* oder Vernichten *sowie das Durchführen logischer und/oder rechnerischer Operationen mit diesen Informationen*.	*Absatz 5 ergänzt und präzisiert gemäss KdK-Leitfaden[12] die bisherige Umschreibung des Begriffs «Bearbeiten» im Sinn des massgebenden Europarechts[13]. Zudem wird ohne inhaltliche Änderung der bisherige Begriff «Verwenden» durch den Begriff «Lesen» ersetzt, um klar zu stellen, dass auch die passive Kenntnisnahme von Informationen eine Bearbeitungsart im Sinn des Gesetzes darstellt.*
[Absatz 7 des Revisionsentwurfs ist neu.]	*7 Profiling ist jede Auswertung von Informationen, um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen, insbesondere bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, Intimsphäre oder Mobilität.*	*Absatz 7: Die EU-Richtlinie 2016/680[14] regelt neu das sogenannte «Profiling» als besondere, 'gefährliche' Art des Bearbeitens von Personendaten. Das Profiling muss denselben Anforderungen genügen wie das Bearbeiten von besonders schützenswerten Personendaten, erfordert also eine Grundlage in einem formellen Gesetz (= § 9 Absatz 2 IDG). Im Interesse der einfachen Formulierung und Verständlichkeit ist «Profiling» in die Begriffsdefinitionen aufzunehmen. Der Wortlaut von Absatz 7 entspricht dem Vorschlag im KdK-Leitfaden[15].*
[Absatz 8 des Revisionsentwurfs ist neu.]	*8 Auftragsdatenbearbeiterin oder Auftragsdatenbearbeiter ist die private Person oder das öffentliche Organ, die oder das Informationen im Auftrag des öffentlichen Organs bearbeitet, welches für die Bearbeitung verantwortlich ist.*	*Absatz 8: Der vom übergeordneten Recht[16] definierte Begriff des «Auftragsbearbeiters» wird in das kantonale Gesetz eingeführt. Da es hier aber nicht um die Bearbeitung eines Auftrags, sondern um eine Datenbearbeitung im Auftrag geht, muss der Begriff korrekt Auftragsdatenbearbeiterin / Auftragsdatenbearbeiter lauten. Der Wortlaut der Bestimmung orientiert sich am Vorschlag im KdK-Leitfaden[17].*

12 Seite 5 / Ziffer 3.7 KdK-Leitfaden (vollständiger Titel mit Link in Fussnote 2)
13 Artikel 3 Ziffer 2 EU-Richtlinie 2016/680 / Artikel 2 Buchstabe b E-Übereinkommen SEV 108 (vollständige Titel mit Links in Fussnote 1)
14 Artikel 3 Ziffer 4 EU-Richtlinie 2016/680 (vollständiger Titel mit Link in Fussnote 1)
15 Seite 5 / Ziffer 3.8 KdK-Leitfaden (vollständiger Titel mit Link in Fussnote 2)
16 Artikel 3 Ziffer 9 EU-Richtlinie 2016/680 / Artikel 2 Buchstabe f E-Übereinkommen SEV 108 (vollständige Titel mit Links in Fussnote 1)
17 Seite 6 / Ziffer 3.10 KdK-Leitfaden (vollständiger Titel mit Link in Fussnote 2)

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
§ 6 Verantwortung [1] Die Verantwortung für den Umgang mit Informationen trägt dasjenige öffentliche Organ, das die Informationen zur Erfüllung seiner gesetzlichen Aufgaben bearbeitet. [2] Bearbeiten mehrere öffentliche Organe einen gemeinsamen Informationsbestand, regeln sie die Verantwortung untereinander.	**§ 6 Verantwortung** [1] [unverändert] [2] Bearbeiten mehrere öffentliche Organe einen gemeinsamen Informationsbestand, regeln sie die Verantwortung untereinander *und legen fest, welches öffentliche Organ die Gesamtverantwortung trägt.*	*Absatz 2: Bereits das geltende Recht legt fest, dass in Fällen, in denen mehrere öffentliche Organe gemeinsam einen Datenbestand bearbeiten, die Verantwortung für die Datenbearbeitung geregelt werden muss. Der Revisionsentwurf präzisiert die heutige Regelung, indem die Gesamtverantwortung für den Umgang mit Informationen einer einzigen Stelle zuzuordnen ist. Dies betrifft insbesondere* *– die Festlegung des Schutzbedarfs für das Gesamtsystem,* *– die Durchführung einer Risikoanalyse sowie* *– die Verantwortung für das Restrisiko und die angemessene Sicherheit für das Gesamtsystem.* *Bearbeiten also mehrere öffentliche Organe gemeinsam einen Datenbestand, ist dasjenige öffentliche Organ zu bestimmen, dem die Gesamtverantwortung zukommt. Zwar können den einzelnen beteiligten Organen durchaus Teilverantwortlichkeiten zugewiesen werden. Allerdings obliegt die Verantwortung für alles, was nicht in eine solche Teilverantwortlichkeit fällt, dem Organ, das die Gesamtverantwortung trägt. Dies wird mit der Ergänzung des bisherigen Wortlauts klargestellt. Die gleiche Lösung sehen die Kantone BS[18], AG[19] und ZH[20] vor.* *Kriterien für die Zuteilung der Gesamtverantwortung an eines der beteiligten Organe sind beispielsweise:* *- das betreffende öffentliche Organ hat die Möglichkeit, über den Inhalt und den Zweck des Datenbestands zu entscheiden;* *- das betreffende öffentliche Organ verfügt über die nötigen personellen und finanziellen Ressourcen,*

[18] § 6 IDG-Revisionsentwurf
[19] § 29 Absatz 2 IDAG
[20] § 27 IDV

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
		um die rechtmässige Datenbearbeitung und die Informationssicherheit zu gewährleisten.
(§ 6 Verantwortung) *[Absatz 3 des Revisionsentwurfs ist neu.]*	(§ 6 Verantwortung) *3 Das verantwortliche öffentliche Organ muss gegenüber der Aufsichtsstelle Datenschutz nachweisen können, dass es die Datenschutzbestimmungen einhält.* *4 Der Regierungsrat regelt das Nähere für die kantonale Verwaltung, der Gemeinderat regelt das Nähere für die kommunale Verwaltung. Soweit Gemeinden keine Regelungen erlassen, gelten diejenigen für die kantonale Verwaltung.*	*Absatz 3: Nach den geänderten europäischen Rechtsgrundlagen[21] ist gesetzlich festzuschreiben, dass das verantwortliche öffentliche Organ die Einhaltung der Datenschutzbestimmungen gegenüber der Aufsichtsstelle Datenschutz nachweisen können muss. Der Wortlaut des neuen Absatzes entspricht dem Vorschlag im KdK-Leitfaden[22].* *Wie der Nachweis erbracht werden muss, lässt sich nicht auf Gesetzesstufe festlegen. Es soll kein bürokratischer Leerlauf geschaffen werden. Grössere Systeme können heute schon in verantwortlicher Weise nur mit einem Datenschutz-Managementsystem (DSMS) oder mit einem (um Datenschutzaspekte angereicherten) Informationssicherheits-Managementsystem (ISMS) betrieben werden. Diese Managementsysteme basieren auf den ISO-Standards des Qualitätsmanagements (ISO 9001) und der Informationssicherheit (ISO 27001 usw.). Für die Datenbearbeitungen, bei denen kein solches DSMS (oder angereichertes ISMS) geführt wird, ist festzulegen, welche Dokumente notwendig sind, um den erforderlichen Nachweis erbringen zu können (z.B. Informationssicherheitskonzept, Zugriffskonzept usw.). Hierzu bestehen bereits zahlreiche Hilfsmittel.* *In welchen Fällen ein solches DSMS obligatorisch sein soll, ist auf Verordnungsstufe zu regeln (z.B. nur, wenn besondere Personendaten oder Personendaten, die einem besonderen Amtsgeheimnis unterstehen, bearbeitet werden).*

[21] Artikel 4 Absatz 4 EU-Richtlinie 2016/680: "*Der Verantwortliche ist für die Einhaltung […] (der Vorschriften über die Bearbeitung von Personendaten) verantwortlich und muss deren Einhaltung nachweisen können.*" / Artikel 8bis Ziffer 1 E-Übereinkommen SEV 108 (vollständige Titel mit Links in Fussnote 1)

[22] Seite 9 / Ziffer 4.10 KdK-Leitfaden (vollständiger Titel mit Link in Fussnote 2)

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
§ 7 Bearbeiten im Auftrag [1] Das öffentliche Organ kann das Bearbeiten von Informationen Dritten übertragen, wenn: a. keine rechtliche Bestimmung oder vertragliche Vereinbarung entgegensteht und b. sichergestellt wird, dass die Informationen nur so bearbeitet werden, wie es das öffentliche Organ tun dürfte. [2] Das öffentliche Organ bleibt für den Umgang mit Informationen nach diesem Gesetz verantwortlich. *[Absatz 3 des Revisionsentwurfs ist neu.]*	**§ 7 Bearbeiten im Auftrag** [1] Das öffentliche Organ kann das Bearbeiten von Informationen *einer Auftragsdatenbearbeiterin oder einem Auftragsdatenbearbeiter* übertragen, wenn: a. [unverändert] b. [unverändert] [2] [unverändert] *[3] Die Auftragsdatenbearbeiterin oder der Auftragsdatenbearbeiter darf ohne vorgängige schriftliche Zustimmung des auftraggebenden öffentlichen Organs die Informationsbearbeitung keiner weiteren Auftragsdatenbearbeiterin oder keinem weiteren Auftragsdatenbearbeiter übertragen.*	*Absatz 1: Ersetzung des Begriffs «Dritte» durch den neu eingeführten Begriff «Auftragsdatenbearbeiter/-in» (§ 3 Absatz 8 Revisionsentwurf).* *Neuer Absatz 3: Nach dem geänderten europäischen Recht[23] darf die Datenbearbeitung nur mit schriftlicher Genehmigung des auftraggebenden öffentlichen Organs auf weitere Auftragsdatenbearbeiter/-innen übertragen werden. Der Wortlaut der zusätzlichen Gesetzesbestimmung entspricht dem Vorschlag im KdK-Leitfaden[24].* *Die detaillierten Anforderungen für eine zulässige Übertragung auf weitere Auftragsdatenbearbeiter/-innen sind auf Verordnungsstufe zu regeln.*
§ 9 Voraussetzungen für das Bearbeiten [2] Besondere Personendaten dürfen bearbeitet werden, wenn a. sich die Zulässigkeit ausdrücklich aus einem Gesetz ergibt oder b. dies zur Erfüllung einer im Gesetz ausdrücklich umschriebenen Aufgabe erforderlich ist. *[Absatz 4 des Revisionsentwurfs ist neu.]*	**§ 9 Voraussetzungen für das Bearbeiten** [2] Besondere Personendaten dürfen bearbeitet *und ein Profiling darf nur vorgenommen* werden, wenn: a. [unverändert] b. [unverändert] *[4] Personendaten dürfen nur so lange bearbeitet werden, als es zur Erfüllung der gesetzlichen Aufgabe erforderlich ist.*	*In Absatz 2 ist zusätzlich das sogenannte "Profiling" (siehe die Definition im neuen § 3 Absatz 7) zu erwähnen, weil es denselben Anforderungen genügen muss wie das Bearbeiten von besonders schützenswerten Personendaten.* *Absatz 4: Bereits das verfassungsmässige Verhältnismässigkeitsprinzip verlangt, dass die Personendatenbearbeitung auf die Zweckerreichung zu befristen ist. Zur Verdeutlichung wird dies nun explizit festgeschrieben, womit auch den europarechtlichen Vorgaben entsprochen wird.[25]*

[23] Artikel 22 EU-Richtlinie 2016/680 (vollständiger Titel mit Link in Fussnote 1)

[24] Seite 10 / Ziffer 4.12 KdK-Leitfaden

[25] Artikel 5 der EU-Richtlinie 2016/680 (vollständiger Titel mit Link in Fussnote 1), Seite 8 / Ziffer 4.6 KdK-Leitfaden

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
[§ 9a des Revisionsentwurfs ist neu.]	***§ 9a Voraussetzungen für das Bearbeiten im Rahmen von Pilotversuchen*** *[1] Der Regierungsrat kann, nachdem er im Rahmen einer Vorabkonsultation (§ 12) die Beurteilung der Aufsichtsstelle Datenschutz (§ 35) eingeholt hat, vor dem Inkrafttreten eines Gesetzes die Bearbeitung von besonderen Personendaten bewilligen, wenn:* *a. die Aufgaben, die diese Bearbeitung erforderlich machen, in einem Gesetz geregelt sind, und* *b. ausreichende Massnahmen zur Verhinderung von Persönlichkeitsverletzungen getroffen werden, und* *c. die praktische Umsetzung einer Datenbearbeitung eine Testphase vor dem Inkrafttreten des Gesetzes zwingend erfordert.* *[2] Die praktische Umsetzung einer Datenbearbeitung kann eine Testphase zwingend erfordern, wenn die Erfüllung einer Aufgabe:* *a. technische Neuerungen erfordert, deren Auswirkungen zunächst evaluiert werden müssen, oder* *b. bedeutende organisatorische oder technische Massnahmen erfordert, deren Wirksamkeit zunächst geprüft werden muss, insbesondere bei der Zusammenarbeit mit öffentlichen Organen des Bundes und anderer Kantone und Privaten, oder* *c. die Bekanntgabe von besonderen Personendaten an Dritte mittels eines Abrufverfahrens erfordert.* *[3] Pilotprojekte sind auf maximal fünf Jahre zu befristen.*	*Die überwiesene Motion 2013-085[26] beauftragt den Regierungsrat, dem Landrat eine Gesetzesgrundlage vorzulegen, die Pilotprojekte zur Erprobung des elektronischen Patientendossiers ermöglicht. Seit Ende 2013 enthält das – mit dem basellandschaftlichen Gesetz grossteils gleichlautende – baselstädtische IDG eine detaillierte Regelung für die Datenbearbeitung im Rahmen von Pilotprojekten[27]. Diese Regelung ist allgemein formuliert, so dass sie sowohl im Gesundheitsbereich als auch in weiteren Bereichen angewendet werden kann. Sie entspricht weitgehend einer einschlägigen Bestimmung im Bundes-Datenschutzgesetz[28].* *Mit der Integration der Gesetzesbestimmung des Kantons BS in das basellandschaftliche IDG wird der Motionsauftrag erfüllt. Gestützt auf den neuen § 9a kann der Regierungsrat auf Verordnungsstufe eine Rechtsgrundlage schaffen, damit im Rahmen von zeitlich befristeten Pilotversuchen besondere Personendaten bearbeitet werden können.* *Der neue § 9a lockert das Erfordernis der formellgesetzlichen Grundlage für die Bearbeitung von besonderen Personendaten nicht generell. Durch die Festlegung von strikten Voraussetzungen wird verhindert, dass die Pilotversuchsbestimmung als "Lückenbüsser" in Fällen benutzt wird, in denen zwar schon klar ist, dass und wie besondere Personendaten bearbeitet werden sollen, jedoch festgestellt wird, dass die erforderliche formellgesetzliche Grundlage für diese Form der Datenbearbeitung fehlt. Die neue Bestimmung lässt nur dort, wo tatsächlich eine entsprechende Notwendigkeit besteht, eine «experimentelle*

[26] Vom Landrat stillschweigend (oppositionslos) überwiesen.
[27] § 9a IDG BS (SG 153.260) / Revisionsvorlage BS
[28] Artikel 17a "Automatisierte Datenbearbeitung im Rahmen von Pilotversuchen" (SR 235.1)

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
	(§ 9a Voraussetzungen für das Bearbeiten im Rahmen von Pilotversuchen) [4] *Jedes Pilotprojekt ist zu evaluieren.* [5] *Der Regierungsrat regelt die Modalitäten der Datenbearbeitung in einer Verordnung.*	*Gesetzgebung» zu. Diese ermöglicht, die Auswirkungen einer geplanten Gesetzesregelung zunächst während einer Pilotphase zu überprüfen und exakt zu evaluieren.* *Die Eckpunkte der Gesetzesregelung sind:* *Absatz 1: Der Regierungsrat kann für Pilotprojekte die temporäre Bearbeitung von besonderen Personendaten ohne formellgesetzliche Grundlage bewilligen, falls er vorgängig die Beurteilung (Vorabkonsultation) der Datenschutzaufsichtsstelle eingeholt hat und zusätzlich folgende weitere Voraussetzungen kumulativ erfüllt sind:* *– Die Aufgabe, zu deren Erfüllung das Pilotprojekt dient, muss in einem Gesetz im formellen Sinne festgeschrieben sein (Buchstabe a).* *– Der Regierungsrat hat zudem per Verordnung die nötigen Massnahmen zur Verhinderung von Persönlichkeitsverletzungen festzulegen (Buchstabe b).* *– Schliesslich muss auch nachgewiesen sein, dass der Pilotversuch respektive die Testphase zwingend nötig ist (Buchstabe c).* *Absatz 2 konkretisiert, wann eine Testphase zwingend nötig sein kann (Evaluation von Auswirkungen einer technischen Neuerung, Wirksamkeitsprüfung von organisatorischen oder technischen Massnahmen, Notwendigkeit der Datenübermittlung an Dritte per Abrufverfahren).* *Absatz 3 limitiert die Pilotprojekte auf höchstens 5 Jahre und Absatz 4 schreibt eine zwingende Evaluationspflicht für jedes Pilotprojekt vor.* *Absatz 5: Der Regierungsrat muss das eigentliche Pilotprojekt im Rahmen einer Verordnung präzis regeln, die Bewilligung nach Absatz 1 genügt aus rechtstaatlicher Sicht nicht. Diese Verordnung macht das Manko der formellgesetzlichen Grundlage für*

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
		das Bearbeiten der besonderen Personendaten zumindest ansatzweise wett. Ihre Regelung der Datenbearbeitungsmodalitäten ermöglicht die Festlegung verbindlicher Massnahmen zum Schutz der vom Pilotprojekt betroffenen Personen und schafft auch die nötige Transparenz für eine kritische Diskussion der Projekte.
§ 10 Richtigkeit [1] Personendaten müssen richtig und, soweit es der Verwendungszweck erfordert, vollständig sein.	**§ 10 Richtigkeit** [1] [unverändert]	*Der Grundsatz von Absatz 1 bleibt unverändert. Daraus geht allerdings nicht hervor, was die Anforderung der Richtigkeit konkret bedeutet. In Übereinstimmung mit dem Bundesrecht sollen daher die Handlungspflichten benannt werden.* *Die neuen Absätze 2 und 3 stimmen mit der Regelung im Bundes-Datenschutzgesetz[29] überein und entsprechen den europarechtlichen Vorgaben sowie der Empfehlung des KdK-Leitfadens[30].*
[Absatz 2 des Revisionsentwurfs ist neu]	[2] *Wer Personendaten bearbeitet, hat sich über deren Richtigkeit zu vergewissern.*	*Absatz 2: Das öffentliche Organ, das zur Aufgabenerfüllung Personendaten bearbeitet, muss sich vergewissern, ob die Daten richtig sind. Es geht nicht um einen Beweis, sondern um eine Plausibilisierung der Richtigkeit. Auch handelt es sich nicht um eine zwingende Nachforschungspflicht ohne konkreten Anlass. Stammen die Daten von der betroffenen Person selber, darf das öffentliche Organ – aus datenschutzrechtlicher Sicht – auf die Richtigkeit vertrauen und muss sie nicht zusätzlich prüfen. Eine vertiefte Prüfung kann aber angezeigt sein, wenn mit den Daten, die von der betroffenen Person selber stammen, Anspruch auf eine staatliche Leistung erhoben wird.*

[29] Artikel 5 "Richtigkeit der Daten" (SR 235.1)

[30] Seite 9 / Ziffer 4.7 KdK-Leitfaden (vollständiger Titel mit Link in Fussnote 2), Artikel 4 Absatz 1 Buchstabe d EU-Richtlinie 2016/680 / Artikel 5 Ziffer 4 Buchstabe d E-Übereinkommen SEV 108 (vollständige Titel mit Links in Fussnote 1)

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
		Die vom öffentlichen Organ anzuwendende Sorgfalt bei der Vergewisserung der Richtigkeit von Personendaten hängt vom Risiko einer Persönlichkeitsverletzung ab – je heikler die Daten, umso grösser die Sorgfalt. Die Vergewisserungspflicht hat eine grössere Bedeutung, wenn Daten nach einer längeren Phase des Ruhens wieder bearbeitet werden. Beim Erhalt von neuen Daten dürfte sich die Pflicht in Normalfall auf eine Plausibilisierung beschränken. *Werden unrichtige Personendaten festgestellt, ergibt sich aus dem Grundsatz von Absatz 1 sowie nach dem Rechtsprinzip von Treu und Glauben, dass das öffentliche Organ die Empfänger unrichtiger Personendaten zu informieren hat.*
[Absatz 3 des Revisionsentwurfs ist neu]	3 *Es sind 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.*	*Absatz 3: Stellen sich Personendaten als unrichtig heraus, ist dafür zu sorgen, dass die Korrektur (Berichtigung oder Vernichtung nach § 25 IDG) auch umgesetzt werden kann. Bei Papierdossiers ist dies einfacher zu bewerkstelligen, bei IT-Systemen muss dies mit angemessenen Massnahmen sichergestellt werden. Können beispielsweise bei einem IT-System wegen der Revisionstauglichkeit (unrichtige) Einträge nicht einfach durch die richtigen Einträge ersetzt werden, ist auf andere Weise sicherzustellen, dass die Berichtigung umgesetzt wird, etwa durch spätere Ergänzungen, die mit dem ursprünglichen Eintrag verknüpft werden, wie dies etwa beim Rapportsystem der Polizei der Fall ist.*

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
[§ 11a des Revisionsentwurfs ist neu.]	***§ 11a Datenschutz-Folgenabschätzung***	*Der neue § 11a basiert auf dem Formulierungsvorschlag des KdK-Leitfadens[31].*
	[1] Das verantwortliche öffentliche Organ prüft bei jedem Vorhaben für eine Personendatenbearbeitung, ob voraussichtlich ein hohes Risiko für die Grundrechte der betroffenen Personen besteht.	*Absätze 1 und 2: Die einschlägigen europarechtlichen Vorgaben[32] verlangen, dass das verantwortliche öffentliche Organ bei Personendatenbearbeitungen mit hohem Risikopotenzial eine Datenschutz-Folgenabschätzung (DSFA) durchführt. Damit lassen sich ungewollte Datenschutzrisiken rechtzeitig erkennen, damit nicht später im Betrieb nachgebessert werden muss.*
	[2] Besteht voraussichtlich ein hohes Risiko, ist eine Datenschutz-Folgenabschätzung durchführen.	*Unter «Vorhaben», bei denen eine DSFA durchzuführen ist, sind nicht einzelne, konkrete Bearbeitungen wie beispielsweise eine Einzelbekanntgabe von Personendaten zu verstehen, sondern die Neueinrichtung und Änderung von Prozessen, Verfahren, Anwendungen u.ä..*
	[3] Die Folgenabschätzung enthält mindestens: *a. eine allgemeine Beschreibung der geplanten Bearbeitungsvorgänge,* *b. eine Bewertung der Risiken für die Grundrechte der betroffenen Personen, sowie* *c. eine Darstellung und Bewertung der geplanten Abhilfemassnahmen, Garantien, Sicherheitsvorkehren und Verfahren, durch die der Schutz der Grundrechte der betroffenen Personen sichergestellt und der Nachweis erbracht werden soll, dass die Datenschutzbestimmungen eingehalten werden.*	*Absatz 3: Im Rahmen der DSFA beschreibt das verantwortliche öffentliche Organ die geplanten Bearbeitungsvorgänge und ermittelt/bewertet die Risiken der Personendatenbearbeitung für die Grundrechte der betroffenen Personen. Zudem sind die geplanten Abhilfemassnahmen, Garantien, Sicherheitsvorkehren und Verfahren darzustellen und zu bewerten, mit denen der Grundrechtsschutz gewährleistet und der Nachweis erbracht werden soll, dass die gesetzlichen Vorschriften eingehalten werden.* *Die DSFA ist im Grunde nichts anderes als die Vorbereitung des verantwortlichen öffentlichen Organs zur Erfüllung der heute schon geltenden Pflicht, «gefährliche» Datenbearbeitungsvorhaben der Datenschutzaufsichtsstelle zur sogenannten Vorabkonsultation zu unterbreiten (§ 12 IDG, §§ 9-11 IDV). Aus-*

[31] Seite 16 / Ziffer 6.2 KdK-Leitfaden (vollständiger Titel mit Link in Fussnote 2)

[32] Artikel 27 EU-Richtlinie 2016/680 / Artikel 8bis Ziffer 2 E-Übereinkommen SEV 108 (vollständige Titel mit Links in Fussnote 1)

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
		serdem ist die kantonale Verwaltung auch aufgrund der gesetzlichen Vorgaben zum Projektmanagement verpflichtet, die entsprechenden Dokumente zu erstellen. Bei grösseren Projekten liefert die vorgeschriebene Projektmethode HERMES methodische Unterstützung. *Die DSFA dient dem öffentlichen Organ auch dazu, die Voraussetzungen zu schaffen, um den Nachweis der Einhaltung der Datenschutzvorschriften erbringen zu können (neuer Absatz 3 zu § 6 IDG).*

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
§ 12 Vorabkontrolle [1] Wenn eine Bearbeitung von Personendaten aufgrund der Art der Bearbeitung oder der zu bearbeitenden Daten geeignet ist, besondere Risiken für die Rechte und die Freiheit der betroffenen Personen mit sich zu bringen, muss diese Bearbeitung vorab der oder dem Datenschutzbeauftragten zur Kontrolle vorgelegt werden.	**§ 12 Vorab*konsultation der Aufsichtsstelle Datenschutz*** *[1] Das verantwortliche öffentliche Organ legt der Aufsichtsstelle Datenschutz (§ 35) frühzeitig zur Vorabkonsultation vor:* *a. Rechtsetzungsprojekte, die die Bearbeitung von Personendaten betreffen, und* *b. Vorhaben zur Bearbeitung von Personendaten, die aufgrund der Art der Bearbeitung oder der zu bearbeitenden Daten voraussichtlich zu einem hohen Risiko für die Grundrechte der betroffenen Personen führen.*	*Der neu redigierte § 12 Absätze 1 und 2 entspricht dem Formulierungsvorschlag des KdK-Leitfadens[33].* *Absatz 1: Nach den europarechtlichen Vorgaben[34] sind gewisse Vorhaben vorab der Aufsichtsstelle Datenschutz zur Konsultation (bisher «Vorabkontrolle») zu unterbreiten. Mit diesem wirksamen Mittel des präventiven Datenschutzes lässt sich verhindern, dass datenschutzrelevante Vorhaben hinterher mit grösserem Aufwand verbessert werden müssen oder gar nicht in Betrieb genommen werden können. Ziel der Vorabkonsultation ist, den Datenschutz rechtzeitig sicherzustellen, insbesondere* *– bei Rechtsetzungsvorhaben dafür zu sorgen, dass die verfassungs- und datenschutzrechtlichen Vorschriften berücksichtigt werden,* *– bei anderen (IT-)Vorhaben die Ermittlung und Bewertung der Risiken und der geplanten Massnahmen zur Risikominderung auf ein zulässiges Mass zu überprüfen und dafür zu sorgen, dass gegebenenfalls mit rechtlichen, organisatorischen oder technischen Massnahmen das Risiko weiter reduziert wird.* *Der Pflicht zur Vorabkonsultation unterliegen:* *– Rechtsetzungsvorhaben zur Bearbeitung von Personendaten,* *– Vorhaben, bei denen in einer Datenschutz-Folgenabschätzung ein hohes Risiko festgestellt wurde,* *– Vorhaben, bei denen die Form der Datenbearbeitung (insbesondere bei Verwendung neuer Technologien, Mechanismen oder Verfahren) voraussichtlich ein hohes Risiko für die Grundrechte der betroffenen Personen bewirkt.*

[33] Seite 16 f. / Ziffer 6.3 KdK-Leitfaden (vollständiger Titel mit Link in Fussnote 2)
[34] Artikel 28 EU-Richtlinie 2016/680 (vollständiger Titel mit Link in Fussnote 1)

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
		Auf Verordnungsstufe[35] ist schon bisher konkretisiert, wann insbesondere von einem hohen Risiko im Sinn von Absatz 1 Buchstabe b auszugehen ist. ***EXKURS 1:*** *Im Vernehmlassungsverfahren warfen die Gemeindeverbände die Frage auf, ob im IDG aufgrund der europarechtlichen Vorgaben die Pflicht zur Vorabkonsultation auf «neu anzulegende Dateisysteme» zu beschränken sei. Die EU-Richtlinie[36] äussert sich nicht, ob mit dem unbestimmten Begriff «neu anzulegendes Dateisystem» einzig ein vollständig neues System gemeint ist oder ob auch der Ausbau / die Änderung eines bereits bestehenden Systems – sprich: ein neu anzulegendes Teilsystem / Ergänzungssystem zu einem bestehenden System – darunter fällt. Nach dem Sinn und Zweck der Datenschutzvorschriften muss jedoch klar letzteres gelten. Die EU-Richtlinie verknüpft die Vorabkonsultation mit dem Ergebnis der Datenschutz-Folgenabschätzung. Ergibt die Folgenabschätzung, dass die geplante Personendatenbearbeitung ein hohes Risiko für die Grundrechte der betroffenen Personen zur Folge hätte, ist vorab die Datenschutzaufsichtsstelle zu konsultieren. Der verfassungsrechtlich garantierte Schutz der betroffenen Personen kann nicht davon abhängen, ob die in Frage stehende Grundrechtsverletzung durch ein völlig neues Gesamt-System, oder durch ein neues Teilsystem zu einem bereits bestehenden System oder aber bei tiefgreifenden datenschutzrelevanten Anpassungen an bestehenden Systemen verursacht wird. Zeigt die vorgängige Datenschutz-Folgenabschätzung (§ 11a), dass die geplante Personendatenbearbeitung ein hohes Risiko für die Grundrechte der betroffenen Personen mit sich bringen kann, soll die fragliche Datenbearbeitung nach dem Sinn und Zweck der Datenschutzgesetzgebung*

[35] § 9 Informations- und Datenschutzverordnung (IDV, SGS 162.11)
[36] Artikel 28 EU-Richtlinie 2016/680 (vollständiger Titel mit Link in Fussnote 1)

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
		möglichst frühzeitig der Datenschutzaufsichtsstelle des Kantons zur Konsultation vorgelegt werden. Deren Beurteilung enthält immer auch beratende Aspekte. Auf diese Fachexpertise der Aufsichtsstelle sollten die öffentlichen Organe im eigenen Interesse nicht verzichten. Stellt sich nämlich erst in einem späteren Projektstadium oder gar erst nach der Projektvollendung eine Verletzung der gesetzlichen Datenschutzvorschriften heraus, muss – mit entsprechendem Personal- und Finanzaufwand – nachträglich nachgebessert werden. Nicht ohne Grund beschränken weder der Bund noch die anderen Kantone in ihren revidierten Gesetzen die Vorabkonsultation auf «neu anzulegende Dateisysteme» sprich gänzlich neue Datenbearbeitungssysteme. Die Vorabkontrolle (neu Vorabkonsultation) hat sich unter dem geltenden Recht als wirksames Instrument etabliert. Eine Einschränkung würde den präventiven Datenschutz gegenüber dem heutigen Niveau schwächen. ***EXKURS 2:*** *Die von den Gemeindeverbänden zur Diskussion gestellte Festlegung einer gesetzlichen Frist für die Beurteilung eines Vorhabens durch die Aufsichtsstelle Datenschutz im Rahmen der Vorabkonsultation wäre nicht sachgerecht, handelt es sich doch bei diesem Vorgang in der Praxis oft nicht um ein einmaliges Ereignis. Die Vorabkonsultation ist ein projektbegleitender Prozess, dessen Dauer auch vom Projektplan abhängt. Es findet keine umfassende Prüfung aller für das Projekt relevanten Dokumente zu einem einzigen Zeitpunkt und mit entsprechendem Zeitaufwand statt. Vielmehr erfolgt die Prüfung in mehreren Teilschritten, wobei in jedem Teilschritt nur die in dieser Projektphase anfallenden Dokumente geprüft werden. Die Anzahl Teilschritte hängt von der Komplexität des Projekts ab. Dieses Vorgehen hat mehrere Vorteile: einerseits erfolgt die Prüfung zum aktuellen Zeitpunkt, d.h. das Projekt kann danach in der*

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
(§ 12 Vorabkontrolle)	(§ 12 Vorabkonsultation der Aufsichtsstelle Datenschutz)	*entsprechenden Projektphase fortgesetzt werden; andererseits sinkt der Zeitaufwand für jeden Prüfungsschritt ganz erheblich, so dass diese Teilprüfungen in aller Regel innerhalb von 2–4 Wochen vorgenommen werden können, was die Gefahr eines längeren, nicht planbaren Stopps oder einer längeren Projektverzögerung minimiert.*
[2] Die oder der Datenschutzbeauftragte gibt die Beurteilung in Form einer Empfehlung gemäss § 43 ab.	*[2] Die Aufsichtsstelle Datenschutz kann Kriterien für Bearbeitungsvorgänge festlegen, die ihr zur Vorabkonsultation zu unterbreiten sind.*	*Absatz 2: Die Datenschutzaufsichtsstelle muss Kriterien für die Bearbeitungsvorgänge formulieren können, die ihr vorab zur Konsultation zu unterbreiten sind. Solche Kriterien können etwa die Zahl der betroffenen Personen, die Zahl der beteiligten öffentlichen Organe, die Sensitivität der bearbeiteten Daten usw. sein[37].* *Auf den Inhalt des heutigen Absatzes 2 kann verzichtet werden, weil sich die Möglichkeit der Aufsichtsstelle Datenschutz, aufgrund der Vorabkonsultation eine Empfehlung abzugeben, bereits direkt aus § 43 IDG ergibt. Dass die Datenschutzaufsichtsstelle ihre Beurteilung im Rahmen der Vorabkonsultation stets als Empfehlung im Sinn von § 43 IDG abgibt, passt nicht mehr, weil neu auch Rechtsetzungsvorhaben, die den Umgang mit Informationen betreffen, unter § 12 IDG fallen (Absatz 1 Buchstabe a). In diesen Fällen ist die Stellungnahme der Aufsichtsstelle keine Empfehlung gemäss § 43 IDG.*

[37] Artikel 28 Absatz 3 EU-Richtlinie 2016/680 (vollständiger Titel mit Link in Fussnote 1)

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
§ 14 Erkennbarkeit der Datenbeschaffung [1] Die betroffene Person muss erkennen können, welche Personendaten über sie beschafft und zu welchem Zweck sie bearbeitet werden, soweit und solange dadurch nicht die Erfüllung der gesetzlichen Aufgabe ernsthaft gefährdet wird. [2] Werden Personendaten systematisch, namentlich mit Fragebogen oder Onlineerfassungen, erhoben, müssen Rechtsgrundlage und Zweck der Bearbeitung angegeben sein. [3] Bei der Beschaffung von besonderen Personendaten ist das öffentliche Organ verpflichtet, die betroffene Person über den Zweck der Bearbeitung zu informieren, soweit und solange dadurch nicht die Erfüllung der gesetzlichen Aufgabe ernsthaft gefährdet wird.	**§ 14 *Informationspflicht bei* der Datenbeschaffung** *[1] Das verantwortliche öffentliche Organ informiert über jede Beschaffung von Daten die betroffene Person; diese Informationspflicht gilt auch, wenn die Daten bei Dritten beschafft werden.*	*Der Titel ist redaktionell an die geänderten Absätze 1 und 2 angepasst. Diese übernehmen den Formulierungsvorschlag des KdK-Leitfadens[38] und entsprechen der Regelung auf Bundesebene[39].* *Absatz 1: Das EU-Recht[40] verlangt eine (aktive) Information über jegliches Beschaffen von Personendaten – nicht mehr nur beim Bearbeiten von besonders schützenswerten (besonderen) Personendaten.* *Die Information muss nicht individuell erfolgen, sondern kann auch in allgemeiner Form – etwa auf einer Webseite – erbracht werden. In den meisten Fällen, nämlich überall dort, wo Daten systematisch, beispielsweise auf einem Anmelde- oder Gesuchsformular erhoben werden, reicht es, die entsprechenden Angaben auf dem Formular anzubringen. Wo Personendaten durch Mitarbeitende in einem Gespräch erhoben werden, kann die Information durch die Aushändigung eines Informationsschreibens erfolgen.* *Die «Beschaffung» von Personendaten setzt ein aktives Tun[41] des öffentlichen Organs (oder einer für das öffentliche Organ tätigen Person) voraus, beispielsweise eine Anfrage oder Abklärung. Erhält das öffentliche Organ solche Daten ohne ein solches aktives Zutun, greift die Informationspflicht nicht. Personendaten, die in einer allgemein zugänglichen Weise (etwa auf einer Webseite) zur Verfügung*

[38] Seite 11 / Ziffer 5.2 des KdK-Leitfadens (vollständiger Titel mit Link in Fussnote 2)

[39] Artikel 14 Bundesgesetz über den Datenschutz (DSG; SR 235.1)

[40] Artikel 13 EU-Richtlinie 2016/680 / Artikel 7bis E-Übereinkommen SEV 108 (vollständige Titel mit Links in Fussnote 1). Die europarechtlichen Vorgaben zielen auf eine aktive Informationspflicht des öffentlichen Organs und nicht auf den individuellen Zugang (per Anfrage) der Personen zu ihren Daten ab. Die ins Deutsche übersetzten Formulierungen «zur Verfügung stellen» (EU-Richtlinie) und «Auskunft geben» (E-Übereinkommen SEV 108) sind in proaktivem Sinn zu verstehen. Dies ergibt sich unter anderem aus den Erläuterungen zum Artikel 7bis revidiertes Europarat-Übereinkommen SEV 108 (Ziffer 68): *«… Certain essential information has to be **compulsorily** provided in a **proactive manner** …»* = «… müssen zwingend in proaktiver Weise zur Verfügung gestellt werden.» Entsprechendes gilt für die französischsprachigen Erläuterungen (Ziffer 8): *«… **doit** fournir **impérativement** et de sa **propre initiative** certaines informations essentielles …»* = «… müssen zwingend und aus eigener Initiative zur Verfügung stellen.» Demgemäss sehen sowohl der Bund (siehe Fussnote 39) als auch die anderen Kantone (siehe die kürzlich revidierten Gesetze der Kantone AG, SG, ZH etc.) einhellig eine aktive Informationspflicht vor.

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

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
	(§ 14 Informationspflicht bei der Datenbeschaffung)	*gestellt wurden oder notorisch sind, werden nicht im Sinn von Absatz 1 «beschafft», womit hier die Informationspflicht entfällt. Das bedeutet, frei zugängliche Informationen und solche, die dem öffentlichen Organ zugetragen wurden (auf einsichtigem Weg), sind nicht betroffen. Das öffentliche Organ hat jedoch zu klären, ob die Personendaten richtig sind.*
	[2] Die Information umfasst insbesondere Angaben über: *a. das verantwortliche öffentliche Organ samt Kontaktdaten,* *b. die bearbeiteten Daten oder die Kategorien der bearbeiteten Daten,* *c. alle verfügbaren Informationen über die Herkunft der Personendaten, wenn sie nicht bei der betroffenen Person erhoben worden sind,* *d. die Rechtsgrundlage und den Zweck des Bearbeitens,* *e. die Datenempfänger oder die Kategorien der Datenempfänger, falls die Daten Dritten bekanntgegeben werden, und* *f. die Rechte der betroffenen Person.*	*Absatz 2: Die Informationspflicht betrifft insbesondere* *– die Identität des verantwortlichen öffentlichen Organs (Buchstabe a);* *– die vom öffentlichen Organ bearbeiteten Daten (Buchstabe b);* *– falls Daten nicht bei der betroffenen Person selbst erhoben wurden, die verfügbaren Angaben, woher diese Daten stammen (Buchstabe c); auf diesem Weg kann sich die betroffene Person, sollten solche Daten unrichtig sein, mit ihrem Berichtigungsanspruch an die Quelle der Unrichtigkeit wenden;* *– die Rechtsgrundlage und den Zweck der Datenbearbeitung (Buchstabe d);* *– bei Weitergabe der Daten auch deren Empfänger (Buchstabe e) sowie* *– die Aufklärung der betroffenen Person über ihre Rechte (Buchstabe f).*

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
	(§ 14 Informationspflicht bei der Datenbeschaffung) *[3] Die Informationspflicht entfällt, wenn:* *a. die betroffene Person bereits über die Informationen nach Absatz 2 verfügt;* *b. das Bearbeiten der Personendaten gesetzlich ausdrücklich vorgesehen ist, oder* *c. die Information nicht oder nur mit unverhältnismässigem Aufwand möglich ist.* *[4] Die Bekanntgabe der Informationen kann unter denselben Voraussetzungen eingeschränkt werden wie der Zugang zu den eigenen Personendaten.*	(§ 14) *Wie schon nach bisherigem Recht[42] gelten nach Absatz 3 gewisse Ausnahmen von der Informationspflicht. Diese entfällt namentlich, wenn die betroffene Person bereits informiert ist (Buchstabe a), was insbesondere in einer früheren Phase der Datenbeschaffung geschehen sein kann. Keine Informationspflicht besteht auch, wenn die Beschaffung oder Bekanntgabe der Daten gesetzlich ausdrücklich vorgesehen ist Buchstabe b) – d.h. wenn die betroffenen Personen aus den gesetzlichen Grundlagen mit hinreichender Präzision herauslesen können, welche Daten über sie zu welchem Zweck bearbeitet werden. Schliesslich bleibt noch der Ausnahmefall, dass die Information der betroffenen Person gar nicht möglich oder nur mit unverhältnismässigem Aufwand realisierbar ist (Buchstabe c). Ab wann der Aufwand für die Information an die betroffene Person als unverhältnismässig zu beurteilen ist, hängt vom konkreten Fall ab und ist letztlich eine Ermessensfrage. Als Richtschnur kann gelten, dass je grösser der Behördenaufwand wäre und je weniger sensibel die Personendaten sind, um die es geht, die Information entfallen kann.* *Absatz 4: Die Information der von einer Datenbearbeitung betroffenen Person hat ganz oder teilweise zu unterbleiben oder sie ist aufzuschieben, wenn eine besondere gesetzliche Geheimhaltungspflicht oder ein überwiegendes öffentliches oder privates Interesse entgegen steht (§ 27 IDG). Dies deckt sich mit der europarechtlichen Vorgabe[43], wonach Einschränkungen zulässig sind etwa zur*

[42] Heutiger § 14 Absatz 3 IDG BL

[43] Artikel 15 EU-Richtlinie 2016/680 / Artikel 9 E-Übereinkommen SEV 108 (vollständige Titel mit Links in Fussnote 1)

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
		Sicherstellung behördlicher Verfahren (z.B. Strafverfolgung/Strafvollstreckung) oder zum Schutz der öffentlichen Sicherheit oder der nationalen Sicherheit etc.. Sobald der Einschränkungsgrund wegfällt, ist die Information nachzuholen.

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
		EXKURS *Verzicht auf Regelung über automatisierte Einzelentscheidungen* *In Übereinstimmung mit dem KdK-Leitfaden zum Anpassungsbedarf bei den kantonalen Datenschutzgesetzen[44] wird – analog zum Revisionsentwurf des Kantons Basel-Stadt – aus folgenden Gründen auf eine Regelung über die automatisierte Einzelentscheidung verzichtet:* *Nach dem Revisionsentwurf des Europarat-Übereinkommens SEV 108[45] hat jede Person das Recht, nicht einer Entscheidung unterworfen zu sein, die sie erheblich beeinträchtigt und die aufgrund eines ausschliesslich automatisierten Bearbeitens entstanden ist, ohne dass ihr Standpunkt berücksichtigt wird. Daraus kann als Minimallösung die Pflicht abgeleitet werden, dass* *- 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.* *Diese Regelung ist vor allem im Privatrecht von Bedeutung (zum Beispiel bei einem automatisierten Entscheid über die Kreditwürdigkeit einer Person). Nach dem hier massgebenden öffentlichen Recht werden Einzelentscheidungen mit rechtlichen Wirkungen in aller Regel in der Form der Verfügung erlassen. Da Verfügungen formell eröffnet werden*

[44] Seite 15 f. / Ziffer 6.1 des KdK-Leitfadens (vollständiger Titel mit Link in Fussnote 2)

[45] Artikel 8 Absatz 1 Buchstabe a Entwurf 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) (E-Übereinkommen SEV 108)

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
		müssen, ist die Information der betroffenen Personen sichergestellt. Ausserdem haben die betroffenen Personen vor dem Erlass einer Verfügungen ein verfassungsmässiges Anhörungsrecht (Anspruch auf rechtliches Gehör), womit auch sichergestellt ist, dass sich die betroffenen Personen zur Einzelentscheidung äussern können. Aus diesem Grund ist davon auszugehen, dass es für automatisierte Einzelentscheidungen keine spezifische Regelung in den kantonalen Datenschutzgesetzen braucht. *Sollten in Zukunft bereichsspezifisch automatisierte Einzelentscheidungen eingeführt werden, die nicht zum Erlass einer Verfügung führen, aber trotzdem rechtliche Wirkungen oder erhebliche Auswirkungen auf die betroffene Person haben, wird darauf zu achten sein, dass im entsprechenden Spezialgesetz eine ausdrückliche und klare formellgesetzliche Grundlage dafür geschaffen wird und sichergestellt ist, dass den betroffenen Personen die Möglichkeit gegeben wird, sich zur automatisierten Einzelentscheidung und zu den bearbeiteten Daten zu äussern.*

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
§ 15 Vernichtung 1 Nicht mehr benötigte Personendaten, die von der gemäss Archivierungsgesetz zuständigen Stelle als nicht archivwürdig beurteilt werden, sind vom öffentlichen Organ zu vernichten. *[Absatz 2 des Revisionsentwurfs ist neu.]*	**§ 15 Vernichtung** 1 [unverändert] *2 Für alle Informationsbestände, die Personendaten enthalten, sind Fristen für die Beurteilung festzulegen, ob die Personendaten zur Aufgabenerfüllung noch benötigt werden oder ob sie archiviert oder vernichtet werden sollen.*	*Absatz 2: Nach der europarechtlichen Vorgabe[46] müssen für die Vernichtung (oder Anonymisierung) von Personendaten respektive für eine regelmässige Überprüfung, ob Personendaten zur Aufgabenerfüllung noch benötigt werden, Fristen vorgesehen werden. Erforderlich ist also mindestens eine Regelung für die Vernichtung (oder Anonymisierung) von nicht mehr benötigten Personendaten, sofern sie nicht nach Archivrecht zu archivieren sind. Der KdK-Leitfaden[47] hält fest, dass eine archivierungsrechtliche Anbietepflicht[48] allein nicht genügen dürfte; hingegen könne eine dort verankerte Frist allenfalls als Auffangfrist dienen, wo keine bereichsspezifischen Aufbewahrungs-, Überprüfungs- oder Löschfristen festgelegt seien.* *Die Fristen sind so festzusetzen, dass nach ihrem Ablauf die Daten in der Regel entweder nach den Archivierungsvorschriften archiviert oder vernichtet werden, d.h. nicht mehr beim öffentlichen Organ vorhanden sind. Eine allfällige weitere Verwendung muss dokumentiert und begründet werden.* *Der Zeitpunkt der Vernichtung und jener der Archivierung ist derselbe. In beiden Fällen richtet er sich danach, ob die Daten zur Aufgabenerfüllung noch benötigt werden. Das heisst, auch für archivierungswürdige Daten ist eine Frist festzulegen. Entweder weiss man schon im Voraus, dass die Daten in das Archiv kommen, dann entfällt der Schritt der Beurteilung der Archivierungswürdigkeit. Oder man prüft zu einem festgelegten Zeitpunkt x, ob die Daten in das Archiv abgeliefert oder vernichtet werden. Kriterium ist nicht der Unterschied Archivierung oder Vernichtung der Daten, sondern deren Erforderlichkeit für die Erfüllung einer öffentlichen Aufgabe.*

46 Artikel 5 der EU-Richtlinie 2016/680 (vollständiger Titel mit Link in Fussnote 1)
47 Seite 8 / Ziffer 4.6 KdK-Leitfaden (vollständiger Titel mit Link in Fussnote 2)
48 BL: § 6 Gesetz über die Archivierung (Archivierungsgesetz, SGS 163)

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
[§ 15a des Revisionsentwurfs ist neu.]	***§ 15a Meldung von Datenschutzverletzungen***	*Das EU-Recht[49] gibt vor, dass die Datenschutzaufsichtsstelle baldmöglichst über Verletzungen von Datenschutzvorschriften zu informieren ist. Der neue § 15a entspricht dem Formulierungsvorschlag im KdK-Leitfaden[50].*
	[1] 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.	*Absatz 1 umschreibt den Begriff der Datenschutzverletzung.*
	[2] Das verantwortliche öffentliche Organ meldet der Aufsichtsstelle Datenschutz (§ 35) ohne unangemessene Verzögerung eine Datenschutzverletzung.	*Absatz 2: Meldepflichtig ist das für die Datenbearbeitung verantwortliche öffentliche Organ. Der konkrete Inhalt der Meldung an die Aufsichtsstelle kann auf Verordnungsstufe umschrieben werden (Beschreibung der Datenschutzverletzung und deren wahrscheinlichste Folgen sowie der ergriffenen und vorgesehenen Massnahmen zur Wiederherstellung des Schutzes bzw. zur Abmilderung der Folgen der Verletzung).*
	[3] Die Auftragsdatenbearbeiterin oder der Auftragsdatenbearbeiter informiert das auftraggebende öffentliche Organ unverzüglich über eine Datenschutzverletzung.	*Absatz 3: Geschieht die Datenschutzverletzung im Rahmen einer Auftragsdatenbearbeitung, hat der/die Auftragsdatenbearbeiter/-in unverzüglich das auftraggebende öffentliche Organ zu benachrichtigen, welches die Verletzung seinerseits der Datenschutzaufsichtsstelle meldet.*
	[4] Eine Meldepflicht des öffentlichen Organs besteht nicht, wenn die Datenschutzverletzung voraussichtlich nicht zu einem Risiko für die Grundrechte der betroffenen Person führt. Die Aufsichtsstelle Datenschutz kann Kriterien für Datenschutzverletzungen festlegen, die ihr zu melden sind.	*Nach Absatz 4 kann das öffentliche Organ auf eine Meldung verzichten, wenn die Datenschutzverletzung voraussichtlich zu keinem Risiko für die Grundrechte der betroffenen Person führt. Im Zweifelsfall ist die Aufsichtsstelle Datenschutz beizuziehen. Diese kann Kriterien für die Beurteilung durch die öffentlichen Organe definieren, ob eine Datenschutzverletzung meldepflichtig ist oder nicht.*

[49] Artikel 30 und 31 EU-Richtlinie 2016/680 / Artikel 7 Ziffer 2 E-Übereinkommen SEV 108 (vollständige Titel mit Links in Fussnote 1)

[50] Seite 18, Ziffer 6.4 KdK-Leitfaden (vollständiger Titel mit Link in Fussnote 2)

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
	(§ 15a Meldung von Datenschutzverletzungen)	
	[5] *Das öffentliche Organ informiert die betroffenen Personen, wenn die Umstände dies erfordern oder die Aufsichtsstelle Datenschutz es verlangt.*	*Absatz 5 regelt, wann die von einer Datenschutzverletzung tangierten Personen vom verantwortlichen öffentlichen Organ darüber informiert werden. Die Benachrichtigung erfolgt insbesondere, wenn die betroffenen Personen zur Abwendung des Schadens Massnahmen ergreifen können.*
	[6] *Die Benachrichtigung der betroffenen Personen kann ganz oder teilweise unterbleiben oder aufgeschoben werden, wenn eine Einschränkung gemäss § 27 zulässig ist.*	*Nach Absatz 6 kann das öffentliche Organ die Benachrichtigung der betroffenen Personen ganz oder teilweise unterlassen oder vorerst aufschieben, wenn die Voraussetzungen des analog anwendbaren § 27 Datenschutzgesetz erfüllt sind. Demnach werden die von einer Datenschutzverletzung betroffenen Personen nicht benachrichtigt oder ihre Benachrichtigung wird aufgeschoben, wenn eine besondere gesetzliche Geheimhaltungspflicht oder ein überwiegendes öffentliches oder privates Geheimhaltungsinteresses einer Benachrichtigung entgegen steht.*

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
§ 19 Bekanntgabe von besonderen Personendaten 1 Das öffentliche Organ gibt besondere Personendaten bekannt, wenn	**§ 19 Bekanntgabe von besonderen Personendaten** 1 Das öffentliche Organ gibt besondere Personendaten *oder Resultate eines Profilings* bekannt, wenn*:*	*Absatz 1 wird mit dem sogenannten "Profiling" ergänzt, das neu in § 3 Absatz 7 definiert ist*[51]*.*
§ 22 Verzeichnis der Informationsbestände mit Personendaten 1 Das öffentliche Organ führt ein vollständiges Verzeichnis seiner Informationsbestände, die Personendaten enthalten.	**§ 22 Verzeichnis der *Verfahren, bei denen Personendaten bearbeitet werden*** 1 *Die Strafverfolgungs-, Strafgerichtsbarkeits- und Strafvollzugsorgane führen ein vollständiges Verzeichnis ihrer Verfahren, bei denen Personendaten bearbeitet werden.*	*Die Pflicht zur Führung eines Verzeichnisses wird auf die Organe der Strafverfolgung, des Strafvollzugs und der Strafgerichtsbarkeit fokussiert. Diese Beschränkung ist europarechtlich zulässig, auch andere Kantone machen davon Gebrauch. Damit werden insbesondere auch die Gemeinden künftig von der vor mehreren Jahren eingeführten Verzeichnispflicht entlastet, die ohnehin keine grosse Beachtung fand.* *Mit Hilfe des Verzeichnisses der Verfahren sollen die Betroffenen die Möglichkeit erhalten, festzustellen, in welchen Prozessen beim jeweiligen öffentlichen Organ Personendaten bearbeitet werden. Es geht also um die Transparenz über die Personendatenbearbeitungen. Die Registrierung der Verfahren sollte für die öffentlichen Organe einfacher zu bewältigen sein als das bisherige – bis dato nicht umgesetzte – Register der Datenbestände.* *Das «Verfahren» stellt die Gesamtheit der Prozessschritte zur «Abwicklung einer Aufgabe» dar, bei denen von einem öffentlichen Organ Personendaten (von Bürgerinnen und Bürgern sowie von Mitarbeitenden) bearbeitet werden. Die Zuordnung der Verfahren zu den Informationsbeständen (Anwendungen / Datenbanken / Ablagen etc.) muss nicht öffentlich zugänglich gemacht werden.* *Die erforderlichen Angaben im Verzeichnis regelt die Informations- und Datenschutzverordnung (IDV)*[52]*.*

[51] Siehe vorne Seite 5.
[52] § 12 IDV (SGS 162.11)

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
§ 24 Zugang zu den eigenen Personendaten [1] 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. *[Absatz 2 des Revisionsentwurfs ist neu.]*	**§ 24 Zugang zu den eigenen Personendaten** [1] [unverändert] *[2] Der Zugang umfasst:* *a. die Angaben nach § 14 Absatz 2 und* *b. alle Personendaten zur gesuchstellenden Person.*	*Absatz 2: Die neuen europarechtlichen Grundlagen[53] legen präziser fest, welche Informationen zugänglich zu machen sind, wenn jemand ein Gesuch um Zugang zu den eigenen Personendaten stellt. Der Wortlaut des neuen Absatzes orientiert sich am Formulierungsvorschlag im KdK-Leitfaden[54].*

[53] Artikel 14 EU-Richtlinie 2016/680 / Artikel 8 Ziffer 1 Buchstabe b E-Übereinkommen SEV 108 (vollständige Titel mit Links in Fussnote 1).
[54] Seite 12, Ziffer 5.4 KdK-Leitfaden (vollständiger Titel mit Link in Fussnote 2).

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
[§ 26a des Revisionsentwurfs ist neu.]	***§ 26a Aufsichtsrechtliche Anzeige*** *[1] Jede Person kann der Aufsichtsstelle Datenschutz (§ 35) Tatsachen anzeigen, wonach ein öffentliches Organ oder eine Auftragsdatenbearbeiterin oder ein Auftragsdatenbearbeiter bei der Bearbeitung von sie betreffenden Personendaten gegen die datenschutzrechtlichen Vorschriften verstösst.* *[2] Die anzeigende Person hat nicht die Rechte einer Partei, doch ist ihr innerhalb von höchstens drei Monaten Auskunft über das Ergebnis oder den Stand der Abklärungen zu erteilen.*	*Die europarechtliche Vorgabe[55] verlangt die «Bearbeitung von Beschwerden» durch die Aufsichtsstelle Datenschutz. Da im schweizerischen Rechtssystem – unabhängig von der Möglichkeit einer aufsichtsrechtlichen Anzeige (Aufsichtsbeschwerde) – formelle Rechtsmittel in den einzelnen Verwaltungsverfahren zur Verfügung stehen, ist die EU-Vorgabe niederschwellig in Form einer spezifischen aufsichtsrechtlichen Anzeige bei der Datenschutzaufsichtsstelle umzusetzen.* *Der neue § 26a ist der aufsichtsrechtlichen Anzeige im Verwaltungsverfahrensgesetz BL[56] nachgebildet. Diese kann im vorliegenden Zusammenhang nicht zur Anwendung gelangen, weil sie nicht wie verlangt an die Aufsichtsstelle Datenschutz, sondern an die verwaltungsorganisatorische Aufsichtsbehörde zu richten ist. Die maximal dreimonatige Frist, um die Anzeigenden über das Ergebnis oder den Stand der Abklärungen zu informieren, ist europarechtlich vorgegeben[57].*

55 Artikel 17 sowie Artikel 52 und 53 EU-Richtlinie 2016/680 / Artikel 12bis Ziffer 3 E-Übereinkommen SEV 108 (vollständige Titel mit Links in Fussnote 1)
56 Artikel 43 VwVG BL (SGS 175)
57 Artikel 53 Absatz 2 EU-Richtlinie 2016/680 (vollständiger Titel mit Link in Fussnote 1)

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
§ 28 Anonymisierung von Personendaten 1 Ist der Zugang zu den bei einem öffentlichen Organ vorhandenen Personendaten über Drittpersonen nicht schon nach § 27 ganz oder teilweise zu verweigern, so sind diese Personendaten vor der Zugangsgewährung zu anonymisieren. 2 Der Zugang zu nicht anonymisierten Personendaten über Drittpersonen richtet sich nach den Bestimmungen für die Bekanntgabe von Personendaten.	**§ 28 Anonymisierung von Personendaten** 1 Ist der Zugang zu den bei einem öffentlichen Organ vorhandenen Personendaten ~~*über Drittpersonen*~~ nicht schon nach § 27 ganz oder teilweise zu verweigern, ~~*so*~~ sind diese Personendaten vor der Zugangsgewährung zu anonymisieren. *2 Ist eine Anonymisierung nicht oder nicht vollständig möglich, darf das öffentliche Organ den Zugang zu nicht anonymisierten Personendaten gewähren, wenn:* *a. ein überwiegendes öffentliches Interesse am Zugang zu den nicht anonymisierten Personendaten besteht oder* *b. die Voraussetzungen für die Bekanntgabe von Personendaten erfüllt sind (§§ 18 ff.).*	*Per Jahresbeginn 2018 wurde die Regelung des baselstädtischen IDG über die Anonymisierung von Personendaten[58] geändert, zuvor war sie identisch mit jener in unserem Kanton. Die aktuelle Revision des IDG BL bietet Gelegenheit, die entsprechenden Regelungen in den beiden Basel wieder aufeinander abzustimmen.* *Absatz 1: Der Wegfall der Einschränkung «über Drittpersonen» stellt klar, dass grundsätzlich alle Personendaten zu anonymisieren sind. Erhält nämlich eine Person gestützt auf das Öffentlichkeitsprinzip Zugang zu Informationen, muss dies nach dem Grundsatz «access to one – access to all» auch für jede andere Person gelten. Daher sind auch die Personendaten der gesuchstellenden Person zu anonymisieren.* *Absatz 2: Ist eine Anonymisierung der Personendaten nicht möglich, soll der Zugang auch zu nicht anonymisierten Personendaten gewährt werden dürfen, falls daran ein überwiegendes öffentliches Interesse besteht (Buchstabe a). Beispiel: öffentliches Interesse an lückenloser Information nach Fehlern und Ungereimtheiten in der Verwaltung. Das öffentliche Interesse muss das Geheimhaltungsinteresse der Personen überwiegen, deren Personendaten nicht anonymisiert werden können. Buchstabe b entspricht – redaktionell angepasst – dem bisherigen § 28 Absatz 2. Danach ist eine Bekanntgabe beispielsweise zulässig, wenn im konkreten Einzelfall die betroffene Person ausdrücklich zugestimmt hat oder wenn die Personendaten für einen nicht personenbezogenen Zweck (insbesondere Statistik, Planung oder Forschung) benötigt werden und die vorgängige Anonymisierung nicht möglich ist.*

[58] § 30 Informations- und Datenschutzgesetz (IDG BS; SG 153.260); Ratschlag Nr. 17.0998

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
§ 36 Stellung [2] Die Mitglieder des Landrats sowie der Landrat und der Regierungsrat als Behörden unterstehen der Aufsichtsstelle nicht.	**§ 36 Stellung** [2] *Der Aufsichtsstelle unterstehen nicht:* *a. die Mitglieder des Landrats sowie der Landrat und der Regierungsrat als Behörden;* *b. Datenbearbeitungen in hängigen Verfahren der Zivilrechts- und Strafrechtspflege, der Verfassungs- und Verwaltungsgerichtsbarkeit sowie in hängigen Rechtshilfeverfahren.*	*Absatz 2 Buchstabe a übernimmt den bisherigen Absatz 2. Mit Buchstabe b wird neu verdeutlicht, dass in hängigen Gerichtsverfahren ausschliesslich das anwendbare Prozessrecht zur Anwendung gelangt (§ 2 Absatz 2bis Revisionsentwurf).*
§ 37 Leitung, Wahl [1] Die oder der Datenschutzbeauftragte leitet die kantonale Aufsichtsstelle.	**§ 37 Leitung, Wahl** *[1] Die kantonale Aufsichtsstelle wird von einer in Datenschutzfragen ausgewiesenen Fachperson geleitet (Die Datenschutzbeauftragte / Der Datenschutzbeauftragte).*	*Die Leiterin / der Leiter der Aufsichtsstelle muss über die zur Aufgabenerfüllung erforderliche Qualifikation, Fachkenntnis und Erfahrung im Bereich des Datenschutzes verfügen[59]. Absatz 1 wird mit einem entsprechenden Hinweis ergänzt.*
§ 40 Aufgaben [1] Die Aufsichtsstelle a. kontrolliert nach einem durch sie autonom aufzustellenden Prüfprogramm die Anwendung der Bestimmungen über den Umgang mit Informationen; b. kontrolliert gemäss § 12 vorab Bearbeitungen von Personendaten; c. berät die öffentlichen Organe in Fragen des Umgangs mit Informationen; d. berät die betroffenen Personen über ihre Rechte; e. vermittelt zwischen betroffenen Personen und öffentlichen Organen; f. nimmt Stellung zu Erlassen, die für den Umgang mit Informationen oder den Datenschutz erheb-	**§ 40 Aufgaben** [1] Die Aufsichtsstelle a. [unverändert] b. *nimmt Stellung zu Rechtsetzungsprojekten und anderen Vorhaben, die ihr zur Vorabkonsultation (§ 12) unterbreitet werden*; c. [unverändert] d. [unverändert] e. [unverändert] f. [unverändert]	*Buchstabe b: Redaktionelle Anpassung an den neu formulierten § 12.*

[59] Artikel 43 Absatz 2 EU-Richtlinie 2016/680 (vollständiger Titel mit Link in Fussnote 1) / Seite 22, Ziffer 8.3 KdK-Leitfaden (vollständiger Titel mit Link in Fussnote 2)

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
lich sind. (§ 40 Aufgaben) *[Buchstaben g., h. und i. des Revisionsentwurfs sind neu.]*	(§ 40 Aufgaben) *g. behandelt aufsichtsrechtliche Anzeigen (§ 26a) und informiert die Anzeigenden über das Ergebnis oder den Stand der Abklärungen;* *h. sensibilisiert die öffentlichen Organe für ihre datenschutzrechtlichen Pflichten sowie die Öffentlichkeit für die Anliegen des Datenschutzes und der Transparenz;* *i. verfolgt die für den Schutz von Personendaten und das Öffentlichkeitsprinzip massgeblichen Entwicklungen.*	*Buchstabe g erwähnt die neu eingeführte aufsichtsrechtliche Anzeige bei der Aufsichtsstelle.* *Buchstabe h entspricht einer europarechtlichen Vorgabe[60].* *Buchstabe i entspricht einer weiteren europarechtlichen Vorgabe[61].*

[60] Artikel 46 Absatz 1 Buchstaben b und d EU-Richtlinie 2016/680 / Artikel 12bis Ziffer 2 Buchstabe e E-Übereinkommen SEV 108 (vollständige Titel mit Links in Fussnote 1), Seite 23, Ziffer 8.4c des KdK-Leitfadens (vollständiger Titel mit Link in Fussnote 2)

[61] Artikel 46 Absatz 1 Buchstabe j der EU-Richtlinie 2016/680 (vollständiger Titel mit Link in Fussnote 1) / Seite 23, Ziffer 8.4d des KdK-Leitfadens (vollständiger Titel mit Link in Fussnote 2)

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
§ 41 Kontrollbefugnisse [1] Die Aufsichtsstelle kann bei öffentlichen Organen und bei Drittpersonen, die von einem öffentlichen Organ mit dem Bearbeiten von Personendaten beauftragt sind oder von ihm Personendaten erhalten haben, ungeachtet allfälliger Geheimhaltungspflichten, schriftlich oder mündlich Auskunft über Datenbearbeitungen einholen, Einsicht in alle Unterlagen nehmen, Besichtigungen durchführen und sich Bearbeitungen vorführen lassen. [2] Die öffentlichen Organe und die beauftragten Dritten sind verpflichtet, die Aufsichtsstelle bei der Erfüllung ihrer Aufgaben zu unterstützen. Sie wirken insbesondere an der Feststellung des Sachverhalts mit. [3] Die Berichte, welche die Aufsichtsstelle im Rahmen der Kontrolltätigkeit erstellt oder erstellen lässt, sind samt den ihnen zugrunde liegenden Materialien nicht öffentlich im Sinne von § 23 Absatz 1.	**§ 41 Kontrollbefugnisse** [1] Die Aufsichtsstelle kann bei öffentlichen Organen ~~*und*~~, *bei Auftragsdatenbearbeiterinnen und Auftragsdatenbearbeitern sowie* bei Drittpersonen, die von einem öffentlichen Organ ~~*mit dem Bearbeiten von Personendaten beauftragt sind oder von ihm*~~ Personendaten erhalten haben, ungeachtet allfälliger Geheimhaltungspflichten, schriftlich oder mündlich Auskunft über Datenbearbeitungen einholen, Einsicht in alle Unterlagen nehmen, Besichtigungen durchführen und sich Bearbeitungen vorführen lassen. [2] Die öffentlichen Organe ~~*und*~~, *die Auftragsdatenbearbeiterinnen und Auftragsdatenbearbeiter sowie die Drittpersonen* sind verpflichtet, die Aufsichtsstelle bei der Erfüllung ihrer Aufgaben zu unterstützen. Sie wirken insbesondere an der Feststellung des Sachverhalts mit. [3] [unverändert]	*Die Absätze 1 und 2 werden lediglich redaktionell ohne materielle Änderung angepasst.* *Konkret wird die bisherige Formulierung "Drittpersonen, die von einem öffentlichen Organ mit dem Bearbeiten von Personendaten beauftragt sind." durch den Begriff "Auftragsdatenbearbeiterin / Auftragsdatenbearbeiter" ersetzt. Dieser Begriff wird neu in § 3 Absatz 8 des Revisionsentwurfs umschrieben.*

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
Neue Bestimmungen in der Spezialgesetzgebung.	**II.** 1. Das **Einführungsgesetz zur Schweizerischen Jugendstrafprozessordnung (EG JStPO; SGS 242)** wird wie folgt geändert: ***§ 14a Datenschutzberatung (neu)*** *[1] Die Jugendanwaltschaft bezeichnet eine Datenschutzberaterin oder einen Datenschutzberater.* *[2] Sie oder er* *a. berät und unterstützt bei der Bearbeitung von Personendaten,* *b. nimmt Datenschutz-Folgenabschätzungen vor (§ 11a Informations- und Datenschutzgesetz, IDG) und* *c. arbeitet mit der Aufsichtsstelle Datenschutz (§ 35 IDG) zusammen.* 2. Das **Einführungsgesetz zur Schweizerischen Strafprozessordnung (EG StPO; SGS 250)** wird wie folgt geändert: ***§ 13a Datenschutzberatung (neu)*** *[1] Die Staatsanwaltschaft bezeichnet eine Datenschutzberaterin oder einen Datenschutzberater.* *[2] Sie oder er* *a. berät und unterstützt bei der Bearbeitung von Personendaten,* *b. nimmt Datenschutz-Folgenabschätzungen vor (§ 11a Informations- und Datenschutzgesetz, IDG) und*	*Vier Spezialgesetze werden mit einer identischen Regelung ergänzt, einzig die Bezeichnung der angesprochenen Amtsstelle (Absatz 1) ist unterschiedlich.* *Die neue europarechtliche Vorgabe[62] verlangt, dass die Strafverfolgungs- und die Strafvollzugsbehörden innerhalb ihrer Organisation eine Datenschutzberaterin oder einen Datenschutzberater bezeichnen. Die betreffende Person kann auch für mehrere Behörden zuständig sein[63] (z.B. sowohl für die Staatsanwaltschaft als auch die Jugendanwaltschaft).* *Zur Umsetzung ist je eine gleichlautende Bestimmung in den Spezialgesetzen für die Staatsanwaltschaft, die Jugendanwaltschaft, die Polizei Basel-Landschaft und das Amt für Justizvollzug zu schaffen.* *Die in Absatz 2 umschriebenen Aufgaben der Datenschutzberaterinnen und Datenschutzberater richten sich nach den europarechtlichen Vorgaben[64].* *Bei der Bezeichnung von amtsinternen Datenschutzberaterinnen und -beratern geht es nicht um neue Stellen, sondern lediglich um die Zuordnung von ohnehin bestehenden Aufgaben zu einer bestimmten Person.*

62 Artikel 32 – 34 EU-Richtlinie 2016/680 (vollständiger Titel mit Link in Fussnote 1). Die Richtlinie spricht diesbezüglich zwar vom «Datenschutzbeauftragten», meint allerdings nicht die unabhängigen Aufsichtsorgane (im Sinn der Baselbieter Aufsichtsstelle Datenschutz, § 35 IDG), sondern amtsinterne Datenschutzberaterinnen oder -berater.

63 Artikel 32 Absatz 3 EU-Richtlinie 2016/680 (vollständiger Titel mit Link in Fussnote 1).

64 Artikel 34 EU-Richtlinie 2016/680 (vollständiger Titel mit Link in Fussnote 1).

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
	c. arbeitet mit der Aufsichtsstelle Datenschutz (§ 35 IDG) zusammen. 3. Das **Gesetz über den Vollzug von Strafen und Massnahmen (Strafvollzugsgesetz, StVG; SGS 261**) wird wie folgt geändert: ***§ 2a Datenschutzberatung (neu)*** *[1] Das Amt für Justizvollzug bezeichnet eine Datenschutzberaterin oder einen Datenschutzberater.* *[2] Sie oder er* *a. berät und unterstützt bei der Bearbeitung von Personendaten,* *b. nimmt Datenschutz-Folgenabschätzungen vor (§ 11a Informations- und Datenschutzgesetz, IDG) und* *c. arbeitet mit der Aufsichtsstelle Datenschutz (§ 35 IDG) zusammen.* 4. Das **Polizeigesetz (PolG; SGS 700)** wird wie folgt geändert: ***§ 45g[bis] Datenschutzberatung (neu)*** *[1] Die Polizei Basel-Landschaft bezeichnet eine Datenschutzberaterin oder einen Datenschutzberater.* *[2] Sie oder er* *a. berät und unterstützt bei der Bearbeitung von Personendaten,* *b. nimmt Datenschutz-Folgenabschätzungen vor (§ 11a Informations- und Datenschutzgesetz, IDG) und* *c. arbeitet mit der Aufsichtsstelle Datenschutz (§ 35 IDG) zusammen.*	