

VERNEHMLASSUNGSENTWURF

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
<p>Gesetz über die Information und den Datenschutz (Informations- und Datenschutzgesetz, IDG)</p>	<p>Gesetz über die Information und den Datenschutz (Informations- und Datenschutzgesetz, IDG)</p>	
<p>Vom 10. Februar 2011 (Stand 1. Januar 2018)</p>	<p>Änderung vom ...</p>	<p><i>Revisionsanlass: Anpassung des basellandschaftlichen Informations- und Datenschutzgesetzes (IDG) an die geänderten Vorgaben des europäischen Datenschutzrechts¹.</i></p> <p><i>Als <u>Wegleitung für die kantonalen Rechtsetzungsarbeiten</u> stellte die Konferenz der Kantonsregierungen (KdK) den Kantonen einen Leitfaden zur Verfügung². 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.</i></p>
<p>§ 1 Gegenstand und Zweck ² Es bezweckt: b. die Grundrechte von Personen zu schützen, über welche die öffentlichen Organe Personendaten bearbeiten.</p>	<p>§ 1 Gegenstand und Zweck ² Es bezweckt: b. die Grundrechte von <u>natürlichen</u> Personen zu schützen, über welche die öffentlichen Organe Personendaten bearbeiten.</p>	<p><i>Siehe unten die Bemerkungen zu § 3 Absatz 3.</i></p>

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)

VERNEHMLASSUNGSENTWURF

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
<p>§ 2 Geltungsbereich ² Es findet keine Anwendung:</p> <ul style="list-style-type: none"> a. soweit ein öffentliches Organ am wirtschaftlichen Wettbewerb teilnimmt und dabei privat-rechtlich handelt; b. in hängigen Verfahren der Zivilrechts- und Strafrechtspflege; c. in hängigen Verfahren der Verfassungs- und Verwaltungsgerichtsbarkeit. <p>[Absatz 2^{bis} des Revisionsentwurfs ist neu.]</p>	<p>§ 2 Geltungsbereich ² Es findet keine Anwendung:</p> <ul style="list-style-type: none"> a. [unverändert] b. <u>Aufgehoben.</u> c. <u>Aufgehoben.</u> <p><u>^{2bis} Die Rechte und Ansprüche der betroffenen Person während hängigen Verfahren der Zivilrechts- und Strafrechtspflege sowie der Verfassungs- und Verwaltungsgerichtsbarkeit richten sich ausschliesslich nach dem anwendbaren Verfahrensrecht.</u></p>	<p>Der neue Absatz ^{2bis} ersetzt die bisherigen Buchstaben b und c. Sein Wortlaut entspricht dem Vorschlag im KdK-Leitfaden³. Nach diesem ist die Neuformulierung nötig, weil nach den europarechtlichen Vorgaben⁴ für hängige Gerichtsverfahren keine generellen Geltungsbereich-Ausnahmen in der Datenschutzgesetzgebung mehr vorgesehen werden dürfen.</p> <p>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.</p>

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](#)

VERNEHMLASSUNGSENTWURF

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
<p>§ 3 Begriffe</p> <p>³ Personendaten sind Informationen, die sich auf eine bestimmte oder bestimmbare natürliche oder juristische Person beziehen.</p>	<p>§ 3 Begriffe</p> <p>³ Personendaten sind Informationen, die sich auf eine bestimmte oder bestimmbare natürliche oder <u>juristische</u> Person beziehen.</p>	<p><i><u>Absatz 3:</u> 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-Leitfaden⁷ – 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 <u>§ 1 Absatz 2 Buchstabe b</u> anzupassen (siehe oben).</i></p> <p><i>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.</i></p>

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)

VERNEHMLASSUNGSENTWURF

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
<p>(§ 3 Begriffe)</p> <p>⁴ Besondere Personendaten sind:</p> <p>a. Personendaten, bei deren Bearbeitung eine besondere Gefahr der Grundrechtsverletzung besteht, insbesondere Angaben über:</p> <ol style="list-style-type: none"> 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. <p>b. Zusammenstellungen von Informationen, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlauben (Persönlichkeitsprofil).</p>	<p>(§ 3 Begriffe)</p> <p>⁴ Besondere Personendaten sind:</p> <p>a. [unverändert]</p> <ol style="list-style-type: none"> 1. [unverändert], 2. die Gesundheit, das Erbgut (<i>genetische Daten</i>), die Intimsphäre oder die <i>ethnische Herkunft</i>, <i>2.^{bis} Behinderungen</i>. 3. [unverändert], 4. [unverändert], 5. <i>mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltens-typischen Merkmalen einer natürlichen Person, welche die eindeutige Identifizierung dieser Person ermöglichen oder bestätigen (biometrische Daten)</i>. <p>b. [unverändert]</p>	<p><i>Ziffer 2: Gemäss Empfehlung des KdK-Leitfadens wird der Begriff «Erbgut» mit dem Klammervermerk «genetische Daten» ergänzt⁸ und der Begriff «Rassenzugehörigkeit» durch «ethnische Herkunft» ersetzt⁹. 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 müssen¹⁰.</i></p> <p><i>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 Sinne einer Klarstellung und Präzisierung soll § 3 Absatz 4 mit dem Begriff «Behinderungen» ergänzt werden. Ausschlaggebend für die Qualifizierung als besonderes Personendatum nach kantonalem Recht ist die Vermutung des Bestehens einer «besonderen Gefahr der Grundrechtsverletzung» durch Datenbearbeitung. Die neue Ziffer 5 übernimmt einen Formulierungsvorschlag im KdK-Leitfaden¹¹. 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, Stimmuster, Iris-Muster.</i></p>

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)

VERNEHMLASSUNGSENTWURF

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 <u>Lesen</u> , Verändern, Bekanntgeben, <u>Archivieren</u> , <u>Löschen</u> oder Vernichten <u>sowie das Durchführen logischer und/oder rechnerischer Operationen mit diesen Informationen.</u>	<u>Absatz 5</u> 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.
<i>[Absatz 7 des Revisionsentwurfs ist neu.]</i>	⁷ <u>Profiling ist jede Auswertung von Informationen oder Personendaten, um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen, insbesondere bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, Intimsphäre oder Mobilität.</u>	<u>Absatz 7</u> : 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 .
<i>[Absatz 8 des Revisionsentwurfs ist neu.]</i>	⁸ <u>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.</u>	<u>Absatz 8</u> : 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 <u>Auftragsdatenbearbeiterin / Auftragsdatenbearbeiter</u> 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)

VERNEHMLASSUNGSENTWURF

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
<p>§ 6 Verantwortung</p> <p>¹ Die Verantwortung für den Umgang mit Informationen trägt dasjenige öffentliche Organ, das die Informationen zur Erfüllung seiner gesetzlichen Aufgaben bearbeitet.</p> <p>² Bearbeiten mehrere öffentliche Organe einen gemeinsamen Informationsbestand, regeln sie die Verantwortung untereinander.</p> <p>[Absatz 3 des Revisionsentwurfs ist neu.]</p>	<p>§ 6 Verantwortung</p> <p>¹ [unverändert]</p> <p>² Bearbeiten mehrere öffentliche Organe einen gemeinsamen Informationsbestand, regeln sie die Verantwortung untereinander <u>und legen fest, welches öffentliche Organ die Gesamtverantwortung trägt.</u></p> <p>³ <u>Das verantwortliche öffentliche Organ muss nachweisen können, dass es die Datenschutzbestimmungen einhält. Der Regierungsrat regelt das Nähere für die kantonale Verwaltung, der Gemeinderat regelt das Nähere für die kommunale Verwaltung.</u></p>	<p>Absatz 2: Die Gesamtverantwortung für den Umgang mit Informationen muss einer einzigen Stelle zugeordnet werden. Dies betrifft insbesondere</p> <ul style="list-style-type: none"> – die Festlegung des Schutzbedarfs für das Gesamtsystem, – die Durchführung einer Risikoanalyse sowie – die Verantwortung für das Restrisiko und die angemessene Sicherheit für das Gesamtsystem. <p>Deshalb ist für gemeinsam bearbeitete Informationsbestände 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 klar gestellt.</p> <p>Absatz 3: Nach den geänderten europäischen Rechtsgrundlagen¹⁸ ist gesetzlich festzuschreiben, dass das verantwortliche öffentliche Organ die Einhaltung der Datenschutzbestimmungen nachweisen können muss. Der Wortlaut des neuen Absatzes entspricht dem Vorschlag im KdK-Leitfaden¹⁹.</p>

¹⁸ 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 8^{bis} Ziffer 1 E-Übereinkommen SEV 108 (vollständige Titel mit Links in Fussnote 1)

¹⁹ Seite 9 / Ziffer 4.10 KdK-Leitfaden (vollständiger Titel mit Link in Fussnote 2)

VERNEHMLASSUNGSENTWURF

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
		<p><i>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.</i></p> <p><i>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).</i></p>

VERNEHMLASSUNGSENTWURF

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
<p>§ 7 Bearbeiten im Auftrag</p> <p>¹ Das öffentliche Organ kann das Bearbeiten von Informationen Dritten übertragen, wenn:</p> <p>a. keine rechtliche Bestimmung oder vertragliche Vereinbarung entgegensteht und</p> <p>b. sichergestellt wird, dass die Informationen nur so bearbeitet werden, wie es das öffentliche Organ tun dürfte.</p> <p>² Das öffentliche Organ bleibt für den Umgang mit Informationen nach diesem Gesetz verantwortlich.</p> <p><i>[Absatz 3 des Revisionsentwurfs ist neu.]</i></p>	<p>§ 7 Bearbeiten im Auftrag</p> <p>¹ Das öffentliche Organ kann das Bearbeiten von Informationen <u>einer Auftragsdatenbearbeiterin oder einem Auftragsdatenbearbeiter</u> übertragen, wenn:</p> <p>a. [unverändert]</p> <p>b. [unverändert]</p> <p>² [unverändert]</p> <p>³ <u>Die Auftragsdatenbearbeiterin oder der Auftragsdatenbearbeiter darf ohne vorgängige schriftliche Zustimmung des auftraggebenden öffentlichen Organs die Informationsbearbeitung keiner weiteren Auftragsdatenbearbeiterin oder keinem weiteren Auftragsdatenbearbeiter übertragen.</u></p>	<p><i>Absatz 1: Ersetzung des Begriffs «Dritte» durch den neu eingeführten Begriff «Auftragsdatenbearbeiter/-in» (§ 3 Absatz 8 Revisionsentwurf).</i></p> <p><i>Neuer Absatz 3: Nach dem geänderten europäischen Recht²⁰ 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-Leitfaden²¹.</i></p> <p><i>Die detaillierten Anforderungen für eine zulässige Übertragung auf weitere Auftragsdatenbearbeiter/-innen sind auf Verordnungsstufe zu regeln.</i></p>
<p>§ 9 Voraussetzungen für das Bearbeiten</p> <p>² Besondere Personendaten dürfen bearbeitet werden, wenn</p> <p>a. sich die Zulässigkeit ausdrücklich aus einem Gesetz ergibt oder</p> <p>b. dies zur Erfüllung einer im Gesetz ausdrücklich umschriebenen Aufgabe erforderlich ist.</p> <p><i>[Absatz 4 des Revisionsentwurfs ist neu.]</i></p>	<p>§ 9 Voraussetzungen für das Bearbeiten</p> <p>² Besondere Personendaten dürfen bearbeitet <u>und ein Profiling darf nur vorgenommen</u> werden, wenn:</p> <p>a. [unverändert]</p> <p>b. [unverändert]</p> <p>⁴ <u>Personendaten dürfen nur so lange bearbeitet werden, als es zur Erfüllung der gesetzlichen Aufgabe erforderlich ist.</u></p>	<p><i>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.</i></p> <p><i>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.²²</i></p>

²⁰ Artikel 22 EU-Richtlinie 2016/680 (vollständiger Titel mit Link in Fussnote 1)

²¹ Seite 10 / Ziffer 4.12 KdK-Leitfaden

²² Artikel 5 der EU-Richtlinie 2016/680 (vollständiger Titel mit Link in Fussnote 1), Seite 8 / Ziffer 4.6 KdK-Leitfaden

VERNEHMLASSUNGSENTWURF

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
<p>[§ 9a des Revisionsentwurfs ist neu.]</p>	<p>§ 9a <u>Voraussetzungen für das Bearbeiten im Rahmen von Pilotversuchen</u></p> <p><i>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:</i></p> <p><i>a. die Aufgaben, die diese Bearbeitung erforderlich machen, in einem Gesetz geregelt sind,</i></p> <p><i>b. ausreichende Massnahmen zur Verhinderung von Persönlichkeitsverletzungen getroffen werden und</i></p> <p><i>c. die praktische Umsetzung einer Datenbearbeitung eine Testphase vor dem Inkrafttreten des Gesetzes zwingend erfordert.</i></p> <p><i>2 Die praktische Umsetzung einer Datenbearbeitung kann eine Testphase zwingend erfordern, wenn:</i></p> <p><i>a. die Erfüllung einer Aufgabe technische Neuerungen erfordert, deren Auswirkungen zunächst evaluiert werden müssen;</i></p> <p><i>b. die Erfüllung einer Aufgabe 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</i></p> <p><i>c. sie die Bekanntgabe von besonderen Personendaten an Dritte mittels eines Abrufverfahrens erfordert.</i></p> <p><i>3 Pilotprojekte sind auf maximal fünf Jahre zu befristen.</i></p>	<p>Die überwiesene Motion 2013-085²³ 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 Pilotprojekten²⁴. 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-Datenschutzgesetz²⁵.</p> <p>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.</p> <p>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</p>

²³ Vom Landrat stillschweigend (oppositionslos) überwiesen.

²⁴ Kanton BS: [Geschäftsnummer 13.0739](#)

²⁵ Artikel 17a "Automatisierte Datenbearbeitung im Rahmen von Pilotversuchen" ([SR 235.1](#))

VERNEHMLASSUNGSENTWURF

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
	<p><u>⁴ Jedes Pilotprojekt ist zu evaluieren.</u></p> <p><u>⁵ Der Regierungsrat regelt die Modalitäten der Datenbearbeitung in einer Verordnung.</u></p>	<p>Gesetzgebung» zu. Diese ermöglicht, die Auswirkungen einer geplanten Gesetzesregelung zunächst während einer Pilotphase zu überprüfen und exakt zu evaluieren.</p> <p>Die Eckpunkte der Gesetzesregelung sind:</p> <p><u>Absatz 1:</u> 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:</p> <ul style="list-style-type: none"> – Die Aufgabe, zu deren Erfüllung das Pilotprojekt dient, muss in einem Gesetz im formellen Sinne festgeschrieben sein (<u>Buchstabe a</u>). – Der Regierungsrat hat zudem per Verordnung die nötigen Massnahmen zur Verhinderung von Persönlichkeitsverletzungen festzulegen (<u>Buchstabe b</u>). – Schliesslich muss auch nachgewiesen sein, dass der Pilotversuch respektive die Testphase zwingend nötig ist (<u>Buchstabe c</u>). <p><u>Absatz 2</u> 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).</p> <p><u>Absatz 3</u> limitiert die Pilotprojekte auf höchstens 5 Jahre und <u>Absatz 4</u> schreibt eine zwingende Evaluationspflicht für jedes Pilotprojekt vor.</p> <p><u>Absatz 5:</u> Der Regierungsrat muss das eigentliche Pilotprojekt im Rahmen einer Verordnung präzise regeln, die Bewilligung nach Absatz 1 genügt aus rechtstaatlicher Sicht nicht. Diese Verordnung macht das Manko der formellgesetzlichen Grundlage für</p>

VERNEHMLASSUNGSENTWURF

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.
<p>§ 10 Richtigkeit ¹ Personendaten müssen richtig und, soweit es der Verwendungszweck erfordert, vollständig sein. <i>[Absätze 2 und 3 des Revisionsentwurfs sind neu]</i></p>	<p>§ 10 Richtigkeit ¹ [unverändert] ² <u>Wer Personendaten bearbeitet, hat sich über deren Richtigkeit zu vergewissern.</u> ³ <u>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.</u></p>	<p>Der Grundsatz von Absatz 1 bleibt unverändert. Neu hinzu kommt die Pflicht der Datenbearbeitenden, sich über die Richtigkeit zu vergewissern (Absatz 2) sowie mangelhafte Daten zu korrigieren oder zu vernichten (Absatz 3). Die beiden neuen Gesetzesbestimmungen stimmen mit der Regelung im Bundes-Datenschutzgesetz (Artikel 5) überein. Sie entsprechen den europarechtlichen Vorgaben und der Empfehlung des KdK-Leitfadens²⁶.</p> <p>Stellen sich Personendaten als unrichtig heraus, ist dafür zu sorgen, dass die Korrektur (Berichtigung oder Löschung 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 Rapportssystem der Polizei der Fall ist.</p>

²⁶ 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)

VERNEHMLASSUNGSENTWURF

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
<p>[§ 11a des Revisionsentwurfs ist neu.]</p>	<p><u>§ 11a Datenschutz-Folgenabschätzung</u> ¹ <u>Das verantwortliche öffentliche Organ prüft bei jedem Vorhaben für eine Personendatenbearbeitung, ob voraussichtlich ein hohes Risiko für die Grundrechte der betroffenen Personen besteht.</u> ² <u>Besteht voraussichtlich ein hohes Risiko, ist eine Datenschutz-Folgenabschätzung durchzuführen.</u></p> <p>³ <u>Die Folgenabschätzung enthält mindestens:</u> a. <u>eine Beschreibung der geplanten Bearbeitungsvorgänge.</u> b. <u>eine Bewertung der in Bezug auf die Grundrechte der betroffenen Personen bestehenden Risiken sowie</u> c. <u>eine Darstellung und Bewertung der geplanten organisatorischen und technischen Abhilfemassnahmen, Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz der Grundrechte der betroffenen Personen sichergestellt und der Nachweis erbracht werden soll, dass die Datenschutzbestimmungen eingehalten werden.</u></p>	<p>Der neue § 11a basiert auf dem Formulierungsvorschlag des KdK-Leitfadens²⁷.</p> <p><u>Absätze 1 und 2:</u> Die einschlägigen europarechtlichen Vorgaben²⁸ 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.</p> <p><u>Absatz 3:</u> 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, Sicherheitsvorkehrungen und Verfahren darzustellen und zu bewerten, mit denen der Grundrechtsschutz gewährleistet und der Nachweis erbracht werden soll, dass die gesetzlichen Vorschriften eingehalten werden.</p> <p>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). Ausserdem 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.</p>

²⁷ Seite 16 / Ziffer 6.2 KdK-Leitfaden (vollständiger Titel mit Link in Fussnote 2)

²⁸ Artikel 27 EU-Richtlinie 2016/680 / Artikel 8^{bis} Ziffer 2 E-Übereinkommen SEV 108 (vollständige Titel mit Links in Fussnote 1)

VERNEHMLASSUNGSENTWURF

Geltende Fassung	<i>Geänderte Fassung</i>	Erläuterungen zu den geänderten Bestimmungen
		<i>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).</i>

VERNEHMLASSUNGSENTWURF

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
<p>§ 12 Vorabkontrolle</p> <p>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.</p>	<p><u>§ 12 Vorabkonsultation der Aufsichtsstelle Datenschutz</u></p> <p><i><u>¹ Das verantwortliche öffentliche Organ legt der Aufsichtsstelle Datenschutz (§ 35) frühzeitig zur Vorabkonsultation vor:</u></i></p> <p><i><u>a. Rechtsetzungsprojekte, die die Bearbeitung von Personendaten betreffen, und</u></i></p> <p><i><u>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.</u></i></p>	<p><i>Der neu redigierte § 12 Absätze 1 und 2 entspricht dem Formulierungsvorschlag des KdK-Leitfadens²⁹.</i></p> <p><i><u>Absatz 1: Nach den europarechtlichen Vorgaben³⁰ 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</u></i></p> <ul style="list-style-type: none"> <i>– bei Rechtsetzungsvorhaben dafür zu sorgen, dass die verfassungs- und datenschutzrechtlichen Vorschriften berücksichtigt werden,</i> <i>– 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.</i> <p><i>Der Pflicht zur Vorabkonsultation unterliegen:</i></p> <ul style="list-style-type: none"> <i>– Rechtsetzungsvorhaben zur Bearbeitung von Personendaten,</i> <i>– Vorhaben, bei denen in einer Datenschutz-Folgenabschätzung ein hohes Risiko festgestellt wurde,</i> <i>– 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.</i>

²⁹ Seite 16 f. / Ziffer 6.3 KdK-Leitfaden (vollständiger Titel mit Link in Fussnote 2)

³⁰ Artikel 28 EU-Richtlinie 2016/680 (vollständiger Titel mit Link in Fussnote 1)

VERNEHMLASSUNGSENTWURF

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
<p>(§ 12)</p> <p>² Die oder der Datenschutzbeauftragte gibt die Beurteilung in Form einer Empfehlung gemäss § 43 ab.</p>	<p>(§ 12)</p> <p>² <u>Die Aufsichtsstelle kann Kriterien für Bearbeitungsvorgänge festlegen, die ihr zur Vorabkonsultation zu unterbreiten sind.</u></p>	<p><i>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. sein³¹.</i></p> <p><i>Auf den heutigen Absatz 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.</i></p>

³¹ Artikel 28 Absatz 3 EU-Richtlinie 2016/680 (vollständiger Titel mit Link in Fussnote 1)

VERNEHMLASSUNGSENTWURF

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
<p>§ 14 Erkennbarkeit der Datenbeschaffung</p> <p>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.</p> <p>² Werden Personendaten systematisch, namentlich mit Fragebogen oder Onlineerfassungen, erhoben, müssen Rechtsgrundlage und Zweck der Bearbeitung angegeben sein.</p> <p>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.</p>	<p>§ 14 Informationspflicht bei der Datenbeschaffung</p> <p>¹ <u>Das verantwortliche öffentliche Organ informiert über jede Beschaffung von Daten die betroffene Person; diese Informationspflicht gilt auch, wenn die Daten bei Dritten beschafft werden.</u></p> <p>² <u>Die Information umfasst insbesondere Angaben über:</u></p> <p><u>a. das verantwortliche öffentliche Organ samt Kontaktdaten,</u></p> <p><u>b. die bearbeiteten Daten oder die Kategorien der bearbeiteten Daten.</u></p> <p><u>c. alle verfügbaren Informationen über die Herkunft der Personendaten, wenn sie nicht bei der betroffenen Person erhoben worden sind,</u></p> <p><u>d. die Rechtsgrundlage und der Zweck des Bearbeitens,</u></p> <p><u>e. die Datenempfänger oder die Kategorien der Datenempfänger, falls die Daten Dritten bekanntgegeben werden, und</u></p> <p><u>f. die Rechte der betroffenen Person.</u></p>	<p>Der Titel ist redaktionell an die geänderten Absätze 1 und 2 angepasst. Diese übernehmen den Formulierungsvorschlag des KdK-Leitfadens³².</p> <p><u>Absatz 1:</u> Das EU-Recht³³ verlangt eine (aktive) Information über jegliches Beschaffen von Personendaten – nicht mehr nur beim Bearbeiten von besonders schützenswerten (besonderen) Personendaten.</p> <p><u>Absatz 2:</u> Die Informationspflicht betrifft insbesondere</p> <ul style="list-style-type: none"> – die Identität des verantwortlichen öffentlichen Organs (<u>Buchstabe a</u>); – die vom öffentlichen Organ bearbeiteten Daten (<u>Buchstabe b</u>); – falls Daten nicht bei der betroffenen Person selbst erhoben wurden, die verfügbaren Angaben, woher diese Daten stammen (<u>Buchstabe c</u>); 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 (<u>Buchstabe d</u>); – bei Weitergabe der Daten auch deren Empfänger (<u>Buchstabe e</u>) sowie – die Aufklärung der betroffenen Person über ihre Rechte (<u>Buchstabe f</u>).

³² Seite 11 / Ziffer 5.2 des KdK-Leitfadens (vollständiger Titel mit Link in Fussnote 2)

³³ Artikel 13 EU-Richtlinie 2016/680 / Artikel 7^{bis} E-Übereinkommen SEV 108 (vollständige Titel mit Links in Fussnote 1)

VERNEHMLASSUNGSENTWURF

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
	<p>(§ 14)</p> <p><u>³ Die Informationspflicht entfällt, wenn:</u></p> <p>a. <u>die betroffene Person bereits über die Informationen nach Absatz 2 verfügt;</u></p> <p>b. <u>das Bearbeiten der Personendaten gesetzlich ausdrücklich vorgesehen ist, oder</u></p> <p>c. <u>die Information nicht oder nur mit unverhältnismässigem Aufwand möglich ist.</u></p> <p><u>⁴ Die Bekanntgabe der Informationen kann unter denselben Voraussetzungen eingeschränkt werden wie der Zugang zu den eigenen Personendaten.</u></p>	<p>Wie schon nach bisherigem Recht³⁴ 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).</p> <p><u>Absatz 4:</u> 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 Vorgabe³⁵, wonach Einschränkungen zulässig sind etwa zur 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.</p>

³⁴ Heutiger § 14 Absatz 3 IDG BL

³⁵ Artikel 15 EU-Richtlinie 2016/680 / Artikel 9 E-Übereinkommen SEV 108 (vollständige Titel mit Links in Fussnote 1)

VERNEHMLASSUNGSENTWURF

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
		<p>EXKURS <u>Verzicht auf Regelung über automatisierte Einzelentscheidungen</u></p> <p>In Übereinstimmung mit dem KdK-Leitfaden zum Anpassungsbedarf bei den kantonalen Datenschutzgesetzen³⁶ wird – analog zum Revisionsentwurf des Kantons Basel-Stadt – aus folgenden Gründen auf eine Regelung über die automatisierte Einzelentscheidung verzichtet:</p> <p>Nach dem Revisionsentwurf des Europarat-Übereinkommens SEV 108³⁷ 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</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>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</p>

³⁶ Seite 15 f. / Ziffer 6.1 des KdK-Leitfadens (vollständiger Titel mit Link in Fussnote 2)

³⁷ [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 \(15./16. Juni 2016\) \(E-Übereinkommen SEV 108\)](#)

VERNEHMLASSUNGSENTWURF

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
		<p><i>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.</i></p> <p><i>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.</i></p>

VERNEHMLASSUNGSENTWURF

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
<p>§ 15 Vernichtung</p> <p>¹ Nicht mehr benötigte Personendaten, die von der gemäss Archivierungsgesetz zuständigen Stelle als nicht archivwürdig beurteilt werden, sind vom öffentlichen Organ zu vernichten.</p> <p><i>[Absatz 2 des Revisionsentwurfs ist neu.]</i></p>	<p>§ 15 Vernichtung</p> <p>¹ [unverändert]</p> <p>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.</p>	<p><i>Absatz 2: Nach der europarechtlichen Vorgabe³⁸ 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-Leitfaden³⁹ hält fest, dass eine archivierungsrechtliche Anbietepflicht⁴⁰ allein nicht genügen dürfte; hingegen könne eine dort verankerte Frist allenfalls als Auffangfrist dienen, wo keine bereichsspezifischen Aufbewahrungs-, Überprüfungs- oder Löschrfristen festgelegt seien.</i></p> <p><i>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.</i></p> <p><i>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.</i></p>

³⁸ Artikel 5 der EU-Richtlinie 2016/680 (vollständiger Titel mit Link in Fussnote 1)

³⁹ Seite 8 / Ziffer 4.6 KdK-Leitfaden (vollständiger Titel mit Link in Fussnote 2)

⁴⁰ BL: § 6 Gesetz über die Archivierung (Archivierungsgesetz, [SGS 163](#))

VERNEHMLASSUNGSENTWURF

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
<p>[§ 15a des Revisionsentwurfs ist neu.]</p>	<p>§ 15a <u>Meldung von Datenschutzverletzungen</u></p> <p><i><u>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.</u></i></p> <p><i><u>2 Das verantwortliche öffentliche Organ meldet der Aufsichtsstelle Datenschutz (§ 35) ohne unangemessene Verzögerung eine Datenschutzverletzung.</u></i></p> <p><i><u>3 Die Auftragsdatenbearbeiterin oder der Auftragsdatenbearbeiter informiert das auftraggebende öffentliche Organ unverzüglich über eine Datenschutzverletzung.</u></i></p> <p><i><u>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.</u></i></p>	<p>Das EU-Recht⁴¹ gibt vor, dass die Datenschutzaufsichtsstelle baldmöglichst über Verletzungen von Datenschutzvorschriften zu informieren ist. Der neue § 15a entspricht dem Formulierungsvorschlag im KdK-Leitfaden⁴².</p> <p><i>Absatz 1</i> umschreibt den Begriff der Datenschutzverletzung.</p> <p><i>Absatz 2:</i> 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).</p> <p><i>Absatz 3:</i> 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.</p> <p>Nach <i>Absatz 4</i> 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.</p>

⁴¹ Artikel 30 und 31 EU-Richtlinie 2016/680 / Artikel 7 Ziffer 2 E-Übereinkommen SEV 108 (vollständige Titel mit Links in Fussnote 1)

⁴² Seite 18, Ziffer 6.4 KdK-Leitfaden (vollständiger Titel mit Link in Fussnote 2)

VERNEHMLASSUNGSENTWURF

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
	<p><i><u>5 Das öffentliche Organ informiert die betroffenen Personen, wenn die Umstände dies erfordern oder die Aufsichtsstelle Datenschutz es verlangt.</u></i></p> <p><i><u>6 Die Benachrichtigung der betroffenen Personen kann ganz oder teilweise unterbleiben oder aufgeschoben werden, wenn eine Einschränkung gemäss § 27 zulässig ist.</u></i></p>	<p><i>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.</i></p> <p><i>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.</i></p>

VERNEHMLASSUNGSENTWURF

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
<p>§ 19 Bekanntgabe von besonderen Personendaten</p> <p>¹ Das öffentliche Organ gibt besondere Personendaten bekannt, wenn</p>	<p>§ 19 Bekanntgabe von besonderen Personendaten</p> <p>¹ Das öffentliche Organ gibt besondere Personendaten <u>oder Resultate eines Profilings</u> bekannt, wenn:</p>	<p><i>Absatz 1 wird mit dem sogenannten "Profiling" ergänzt, das neu in § 3 Absatz 7 definiert ist⁴³.</i></p>
<p>§ 22 Verzeichnis der Informationsbestände mit Personendaten</p> <p>¹ Das öffentliche Organ führt ein vollständiges Verzeichnis seiner Informationsbestände, die Personendaten enthalten.</p>	<p>§ 22 Verzeichnis der <u>Verfahren, bei denen Personendaten bearbeitet werden</u></p> <p>¹ Das öffentliche Organ führt ein vollständiges Verzeichnis seiner <u>Verfahren, bei denen Personendaten bearbeitet werden</u>.</p>	<p><i>Titel und Absatz 1: Angleichung der Formulierung an den Wortlaut der entsprechenden Bestimmung des Kantons BS. 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.</i></p> <p><i>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.</i></p>

⁴³ Siehe vorne Seite 5.

VERNEHMLASSUNGSENTWURF

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
<p>§ 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. <i>[Absatz 2 des Revisionsentwurfs ist neu.]</i></p>	<p>§ 24 Zugang zu den eigenen Personendaten ¹ [unverändert]</p> <p>² <u>Der Zugang umfasst:</u> <u>a. die Angaben nach § 14 Absatz 2 und</u> <u>b. alle Personendaten zur gesuchstellenden Person.</u></p>	<p><i>Absatz 2: Die neuen europarechtlichen Grundlagen⁴⁴ 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-Leitfaden⁴⁵.</i></p>

⁴⁴ Artikel 14 EU-Richtlinie 2016/680 / Artikel 8 Ziffer 1 Buchstabe b E-Übereinkommen SEV 108 (vollständige Titel mit Links in Fussnote 1).

⁴⁵ Seite 12, Ziffer 5.4 KdK-Leitfaden (vollständiger Titel mit Link in Fussnote 2).

VERNEHMLASSUNGSENTWURF

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
[§ 26a des Revisionsentwurfs ist neu.]	<p>§ 26a <u>Aufsichtsrechtliche Anzeige</u></p> <p><i>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.</i></p> <p><i>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.</i></p>	<p>Die europarechtliche Vorgabe⁴⁶ 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.</p> <p>Der neue § 26a ist der aufsichtsrechtlichen Anzeige im Verwaltungsverfahrensgesetz BL⁴⁷ 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 vorgegeben⁴⁸.</p>

⁴⁶ Artikel 17 sowie Artikel 52 und 53 EU-Richtlinie 2016/680 / Artikel 12^{bis} Ziffer 3 E-Übereinkommen SEV 108 (vollständige Titel mit Links in Fussnote 1)

⁴⁷ Artikel 43 VwVG BL ([SGS 175](#))

⁴⁸ Artikel 53 Absatz 2 EU-Richtlinie 2016/680 (vollständiger Titel mit Link in Fussnote 1)

VERNEHMLASSUNGSENTWURF

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
<p>§ 28 Anonymisierung von Personendaten</p> <p>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.</p> <p>² Der Zugang zu nicht anonymisierten Personendaten über Drittpersonen richtet sich nach den Bestimmungen für die Bekanntgabe von Personendaten.</p>	<p>§ 28 Anonymisierung von Personendaten</p> <p>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.</p> <p>² <i>Ist eine Anonymisierung nicht oder nicht vollständig möglich, darf das öffentliche Organ den Zugang zu nicht anonymisierten Personendaten gewähren, wenn:</i></p> <p><i>a. ein überwiegendes öffentliches Interesse am Zugang zu den nicht anonymisierten Personendaten besteht oder</i></p> <p><i>b. die Voraussetzungen für die Bekanntgabe von Personendaten erfüllt sind (§§ 18 ff.).</i></p>	<p><i>Per Jahresbeginn 2018 wurde die Regelung des baselstädtischen IDG über die Anonymisierung von Personendaten⁴⁹ 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.</i></p> <p><i>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.</i></p> <p><i>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.</i></p>

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

VERNEHMLASSUNGSENTWURF

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
<p>§ 36 Stellung</p> <p>² Die Mitglieder des Landrats sowie der Landrat und der Regierungsrat als Behörden unterstehen der Aufsichtsstelle nicht.</p>	<p>§ 36 Stellung</p> <p>² <u>Der Aufsichtsstelle unterstehen nicht:</u></p> <p>a. <u>die Mitglieder des Landrats sowie der Landrat und der Regierungsrat als Behörden;</u></p> <p>b. <u>Datenbearbeitungen in hängigen Verfahren der Zivilrechts- und Strafrechtspflege sowie der Verfassungs- und Verwaltungsgerichtsbarkeit.</u></p>	<p><i>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 2^{bis} Revisionsentwurf).</i></p>
<p>§ 37 Leitung, Wahl</p> <p>¹ Die oder der Datenschutzbeauftragte leitet die kantonale Aufsichtsstelle.</p>	<p>§ 37 Leitung, Wahl</p> <p>¹ <u>Die kantonale Aufsichtsstelle wird von einer in Datenschutzfragen ausgewiesenen Fachperson geleitet (Die Datenschutzbeauftragte / Der Datenschutzbeauftragte).</u></p>	<p><i>Die Leiterin / der Leiter der Aufsichtsstelle muss über die zur Aufgabenerfüllung erforderliche Qualifikation, Fachkenntnis und Erfahrung im Bereich des Datenschutzes verfügen⁵⁰. Absatz 1 wird mit einem entsprechenden Hinweis ergänzt.</i></p>
<p>§ 40 Aufgaben</p> <p>¹ Die Aufsichtsstelle</p> <p>a. kontrolliert nach einem durch sie autonom aufzustellenden Prüfprogramm die Anwendung der Bestimmungen über den Umgang mit Informationen;</p> <p>b. kontrolliert gemäss § 12 vorab Bearbeitungen von Personendaten;</p> <p>c. berät die öffentlichen Organe in Fragen des Umgangs mit Informationen;</p> <p>d. berät die betroffenen Personen über ihre Rechte;</p> <p>e. vermittelt zwischen betroffenen Personen und öffentlichen Organen;</p> <p>f. nimmt Stellung zu Erlassen, die für den Umgang mit Informationen oder den Datenschutz erheblich sind.</p>	<p>§ 40 Aufgaben</p> <p>¹ Die Aufsichtsstelle</p> <p>a. [unverändert]</p> <p>b. <u>nimmt Stellung zu Rechtsetzungsprojekten und anderen Vorhaben, die ihr zur Vorabkonsultation unterbreitet werden (§. 12);</u></p> <p>c. [unverändert]</p> <p>d. [unverändert]</p> <p>e. [unverändert]</p> <p>f. [unverändert]</p>	<p><i>Buchstabe b: Redaktionelle Anpassung an den neu formulierten § 12.</i></p>

⁵⁰ 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)

VERNEHMLASSUNGSENTWURF

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
(§ 40) [Buchstaben g., h. und i. des Revisionsentwurfs sind neu.]	(§ 40) <u>g. behandelt aufsichtsrechtliche Anzeigen und informiert die Anzeigenden über das Ergebnis oder den Stand der Abklärungen (§ 26a);</u> <u>h. sensibilisiert die öffentlichen Organe für ihre datenschutzrechtlichen Pflichten und die Öffentlichkeit für die Anliegen des Datenschutzes und der Transparenz;</u> <u>i. verfolgt die für den Schutz von Personendaten und das Öffentlichkeitsprinzip massgeblichen Entwicklungen.</u>	<u>Buchstabe g:</u> Erwähnung der neu eingeführten aufsichtsrechtlichen Anzeige bei der Aufsichtsstelle. <u>Buchstabe h</u> entspricht einer europarechtlichen Vorgabe ⁵¹ . <u>Buchstabe i</u> entspricht ebenfalls einer europarechtlichen Vorgabe ⁵² .

⁵¹ Artikel 46 Absatz 1 Buchstaben b und d EU-Richtlinie 2016/680 / Artikel 12^{bis} 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)

⁵² 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)

VERNEHMLASSUNGSENTWURF

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
<p>(§ 40) [Absätze 2 – 5 des Revisionsentwurfs sind neu.]</p>	<p>(§ 40) ² Die Dienstleistungen der Aufsichtsstelle im Sinn von Absatz 1 Buchstabe c sind für öffentliche Organe ausserhalb der kantonalen Verwaltung gebührenpflichtig, ausgenommen ist die Erstberatung von maximal einer Stunde pro Fall. ³ Bei Fragestellungen, die für alle öffentlichen Organe von grundsätzlicher Bedeutung sind, kann die Aufsichtsstelle ausnahmsweise von der Gebührenerhebung absehen. ⁴ Die Dienstleistungen der Aufsichtsstelle im Sinn von Absatz 1 Buchstaben d und e sind kostenlos. ⁵ Der Regierungsrat erlässt einen Gebührentarif.</p>	<p>Die vom Landrat überwiesene Motion 2015-418 "Verrechnungsmöglichkeit Datenschutz"⁵³ beauftragt den Regierungsrat, die gesetzliche Grundlage für die Verrechnung der Dienstleistungen der Aufsichtsstelle Datenschutz gegenüber "Stellen ausserhalb der kantonalen Verwaltung" auszuarbeiten und dem Landrat vorzulegen.</p> <p>Das Anliegen des parlamentarischen Vorstosses wird im Revisionsentwurf mit den neuen Absätzen 2 – 5 zum § 40 wie folgt umgesetzt:</p> <p><u>Absatz 2</u> erklärt die Beratungstätigkeit der Aufsichtsstelle gegenüber öffentlichen Organen ausserhalb der kantonalen Verwaltung als grundsätzlich kostenpflichtig, wobei die Erstberatung von maximal einer Stunde pro Fall noch kostenlos sein soll. Eine analoge Regelung gilt für die Behandlung von Informationszugangsgesuchen durch das zuständige öffentliche Organ (Öffentlichkeitsprinzip)⁵⁴. Auch dort ist der verursachte Behördenaufwand ab der zweiten Stunde kostenpflichtig.</p> <p>Für zeitintensive Beratungstätigkeiten gegenüber öffentlichen Organen ausserhalb der kantonalen Verwaltung muss also die Aufsichtsstelle im Sinn der Motion 2015-418 in Zukunft finanziell entschädigt werden. Ungewiss ist, in welchem Ausmass – insbesondere von den Gemeinden – aufwändigere Dienstleistungen nachgefragt werden, wenn sie neu finanziell abgegolten werden müssen.</p>

⁵³ Überweisung beschlossen mit 55:17 Stimmen bei 3 Enthaltungen.

⁵⁴ § 34 Informations- und Datenschutzgesetz (IDG; [SGS 162](#)) in Verbindung mit § 24 Informations- und Datenschutzverordnung (IDV; [SGS 162.11](#)).

VERNEHMLASSUNGSENTWURF

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
		<p>Die öffentlichen Organe, die nicht zur kantonalen Verwaltung zählen, sind:</p> <ul style="list-style-type: none"> - die neben der Kantonsverwaltung im engeren Sinn⁵⁵ bestehenden "anderen Träger öffentlicher kantonalen Aufgaben"⁵⁶ (bspw. die finanziell-organisatorisch selbständigen kantonalen Betriebe mit eigener Rechtspersönlichkeit); - Private, soweit ihnen von Kanton oder Gemeinden die Erfüllung öffentlicher Aufgaben übertragen ist⁵⁷ (bspw. Spitex-Organisationen, Alters- und Pflegeheime); - die Gerichtsorgane; - die Gemeinden und ihre Organe. <p><u>Absatz 2 zweiter Halbsatz</u> nimmt, wie im Nachgang vom Motionär vorgeschlagen, die erste Beratung von der Kostenpflicht aus.</p> <p><u>Absatz 3</u> enthält die vom Motionär im Nachgang angeregte Ausnahmemöglichkeit von der Kostenpflicht (Ausnahmekriterium: Beratung zu Grundsatzfragen von weitreichender Bedeutung).</p> <p><u>Absatz 4</u>: Aufgrund der verbindlichen europarechtlichen Vorgaben⁵⁸ muss die Beratung von Privatpersonen über ihre (Datenschutz-)Rechte sowie die Vermittlung zwischen Privatpersonen und öffentlichen Organen in Datenschutzfragen weiterhin unentgeltlich bleiben.</p>

⁵⁵ § 79 Absatz 1 Kantonsverfassung (KV, [SGS 100](#)): "Die kantonale Verwaltung besteht aus fünf Direktionen und der Landeskantlei."

⁵⁶ § 80 KV

⁵⁷ § 3 Absatz 1 Buchstabe c Informations- und Datenschutzgesetz (IDG; [SGS 162](#))

⁵⁸ Artikel 46 Absatz 3 EU-Richtlinie 2016/680 (vollständiger Titel mit Link in Fussnote 1): Die Erfüllung der Aufgaben jeder Aufsichtsbehörde ist für die betroffene Person und für den Datenschutzbeauftragten unentgeltlich. Nach Artikel 17 Ziffer 1 in Verbindung mit Artikel 8 Ziffer 1 Buchstabe g, Artikel 12^{bis} Ziffer 3 und Artikel 14 Ziffer 1 E-Übereinkommen SEV 108 (vollständiger Titel mit Link in Fussnote 1) hat jede Person bei der Ausübung ihrer Datenschutz-Rechte Anspruch auf unentgeltliche Unterstützung durch die Aufsichtsbehörde.

VERNEHMLASSUNGSENTWURF

Geltende Fassung	<i>Geänderte Fassung</i>	Erläuterungen zu den geänderten Bestimmungen
		<p><i>Absatz 5: Für die Gebührenfestlegung könnte der Stundenansatz von 100 Franken für die Bearbeitung von aufwändigen Informationszugangsgesuchen⁵⁹ übernommen werden. In beiden Fällen geht es um die Einhaltung von datenschutzrechtlichen Vorschriften, weshalb ein analoger Gebührentarif sachlich gerechtfertigt ist.</i></p>

⁵⁹ § 24 Absatz 2 Informations- und Datenschutzverordnung (IDV; [SGS 162.11](#))

VERNEHMLASSUNGSENTWURF

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
<p>§ 41 Kontrollbefugnisse</p> <p>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.</p> <p>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.</p> <p>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.</p>	<p>§ 41 Kontrollbefugnisse</p> <p>¹ Die Aufsichtsstelle kann bei öffentlichen Organen, <u>bei Auftragsdatenbearbeiterinnen und Auftragsdatenbearbeitern sowie</u> bei Drittpersonen, die von einem öffentlichen Organ 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.</p> <p>² Die öffentlichen Organe, <u>die Auftragsdatenbearbeiterinnen und Auftragsdatenbearbeiter sowie die Drittpersonen</u> sind verpflichtet, die Aufsichtsstelle bei der Erfüllung ihrer Aufgaben zu unterstützen. Sie wirken insbesondere an der Feststellung des Sachverhalts mit.</p> <p>³ [unverändert]</p>	<p><i>Die Absätze 1 und 2 werden lediglich redaktionell ohne materielle Änderung angepasst.</i></p> <p><i>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.</i></p>

VERNEHMLASSUNGSENTWURF

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
Neue Bestimmungen in der Spezialgesetzgebung.	<p>II.</p> <p>1. Das Einführungsgesetz vom 23. September 2010 zur Schweizerischen Jugendstrafprozessordnung (EG JStPO; SGS 242) wird wie folgt geändert:</p> <p>§ 14a Datenschutzberatung (neu)</p> <p><u>¹ Die Jugendanwaltschaft bezeichnet eine Datenschutzberaterin oder einen Datenschutzberater.</u></p> <p><u>² Sie oder er</u></p> <p><u>a. berät und unterstützt bei der Bearbeitung von Personendaten,</u></p> <p><u>b. nimmt Datenschutz-Folgenabschätzungen vor (§ 11a Informations- und Datenschutzgesetz, IDG) und</u></p> <p><u>c. arbeitet mit der Aufsichtsstelle Datenschutz (§ 35 IDG) zusammen.</u></p> <p>2. Das Einführungsgesetz vom 12. März 2009 zur Schweizerischen Strafprozessordnung (EG StPO; SGS 250) wird wie folgt geändert:</p> <p>§ 13a Datenschutzberatung (neu)</p> <p><u>¹ Die Staatsanwaltschaft bezeichnet eine Datenschutzberaterin oder einen Datenschutzberater.</u></p> <p><u>² Sie oder er</u></p> <p><u>a. berät und unterstützt bei der Bearbeitung von Personendaten,</u></p> <p><u>b. nimmt Datenschutz-Folgenabschätzungen vor (§ 11a Informations- und Datenschutzgesetz, IDG) und</u></p>	<p>Die neue europarechtliche Vorgabe⁶⁰ 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 sein⁶¹ (z.B. sowohl für die Staatsanwaltschaft als auch die Jugendanwaltschaft).</p> <p>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.</p> <p>Die in Absatz 2 umschriebenen Aufgaben der Datenschutzberaterinnen und Datenschutzberater richten sich nach den europarechtlichen Vorgaben⁶².</p> <p>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.</p>

⁶⁰ 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.

⁶¹ Artikel 32 Absatz 3 EU-Richtlinie 2016/680 (vollständiger Titel mit Link in Fussnote 1).

⁶² Artikel 34 EU-Richtlinie 2016/680 (vollständiger Titel mit Link in Fussnote 1).

VERNEHMLASSUNGSENTWURF

Geltende Fassung	Geänderte Fassung	Erläuterungen zu den geänderten Bestimmungen
	<p><i>c. <u>arbeitet mit der Aufsichtsstelle Datenschutz (§ 35 IDG) zusammen.</u></i></p> <p><i>3. Das Gesetz vom 21. April 2005 über den Vollzug von Strafen und Massnahmen (Strafvollzugsgesetz, StVG; SGS 261) wird wie folgt geändert:</i></p> <p><u>§ 2a Datenschutzberatung (neu)</u></p> <p><i><u>1 Das Amt für Justizvollzug bezeichnet eine Datenschutzberaterin oder einen Datenschutzberater.</u></i></p> <p><i><u>2 Sie oder er</u></i></p> <p><i><u>a. berät und unterstützt bei der Bearbeitung von Personendaten,</u></i></p> <p><i><u>b. nimmt Datenschutz-Folgenabschätzungen vor (§ 11a Informations- und Datenschutzgesetz, IDG) und</u></i></p> <p><i><u>c. arbeitet mit der Aufsichtsstelle Datenschutz (§ 35 IDG) zusammen.</u></i></p> <p><i>4. Das Polizeigesetz vom 28. November 1996 (PolG; SGS 700) wird wie folgt geändert:</i></p> <p><u>§ 45g^{bis} Datenschutzberatung (neu)</u></p> <p><i><u>1 Die Polizei Basel-Landschaft bezeichnet eine Datenschutzberaterin oder einen Datenschutzberater.</u></i></p> <p><i><u>2 Sie oder er</u></i></p> <p><i><u>a. berät und unterstützt bei der Bearbeitung von Personendaten,</u></i></p> <p><i><u>b. nimmt Datenschutz-Folgenabschätzungen vor (§ 11a Informations- und Datenschutzgesetz, IDG) und</u></i></p> <p><i><u>c. arbeitet mit der Aufsichtsstelle Datenschutz (§ 35 IDG) zusammen.</u></i></p>	