Regierungsrat des Kantons Basel-Stadt

**An den Grossen Rat** **21.1239.01**

PD/P211239

Basel, 29. September 2021

Regierungsratsbeschluss vom 28. September 2021

# Ratschlag zu einer Änderung des Gesetzes über die Information und den Datenschutz vom 9. Juni 2010 (Informations- und Datenschutzgesetz, IDG) und weiterer Gesetze (Anpassung an die europäischen Datenschutzreformen und weitere Anpassungen)

# Inhalt

# 1. Begehren

Mit diesem Ratschlag beantragen wir Ihnen verschiedene Anpassungen des Gesetzes über die Information und den Datenschutz vom 9. Juni 2010 (Informations- und Datenschutzgesetz, IDG; SG 153.260) und einzelner Datenschutz-Bestimmungen in weiteren Gesetzen mit folgendem Zweck:

- Mit der Anpassung soll sichergestellt werden, dass die Anforderungen der EU-Richtlinie zum Datenschutz (Richtlinie [EU] 2016/680), die als Weiterentwicklung des Schengen/Dublin-Besitzstands zwingend ist, erfüllt werden. Zudem sollen die Voraussetzungen geschaffen werden, dass die Schweiz weiterhin einen Angemessenheitsbeschluss erwirken und die modernisierten Europarats-Konvention zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Europarats-Konvention 108+) ratifizieren kann.
- Gleichzeitig sollen bei einigen wenigen IDG-Bestimmungen Anpassungen oder Präzisierungen vorgenommen werden, die sich in der Praxis als erforderlich und sinnvoll gezeigt haben.

# 2. Ausgangslage

Der Europarat hat die Konvention zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (SEV 108)[1] modernisiert. Am 18. Mai 2018 hat das Ministerkomitee das Protokoll zur Änderung der Konvention SEV 108[2] beschlossen. Das ist nötig geworden, weil sich die Technologie seit der Verabschiedung dieser Konvention im Jahre 1981 erheblich verändert hat. Die Bundesversammlung hat das Protokoll zur Änderung der Europaratskonvention 108 am 19. Juni 2020 genehmigt[3]. Damit werden Bund und Kantone verpflichtet, in ihrem Datenschutzrecht die notwendigen Anpassungen vorzunehmen, um dem **Minimalstandard der modernisierten Europarats-Konvention SEV 108** (genannt: **«Konvention 108+»**) gerecht zu werden.

Am 27. April 2016 hat die Europäische Union nach mehrjährigen Verhandlungen eine Datenschutzreform beschlossen, um angesichts der rasanten technologischen Entwicklungen den Datenschutz zu stärken. Die EU-Datenschutzreform besteht aus zwei Rechtsakten:

- Die **EU-Datenschutz-Grundverordnung 2016/679**[4] (DSGVO) gilt generell für alle Datenbearbeiter in der EU, also für Private und staatliche Organe. Sie ist – als Verordnung – für die EU-Mitgliedstaaten unmittelbar verbindlich, nicht aber für die Schweiz, da die Verordnung nicht als Schengen-relevant erklärt wurde. Die Schweiz ist auch nicht unmittelbar verpflichtet, sie umzusetzen. Allerdings muss die EU-Kommission nach Art. 45 DSGVO (wie schon bisher nach Art. 15 RL 95/46/EG[5]) darüber entscheiden, ob die Schweiz ein angemessenes Schutzniveau bietet. Nur dann ist eine Datenübermittlung in die Schweiz ohne weitere Massnahmen zulässig. Im Rahmen dieser Prüfung der Angemessenheit des Schutzniveaus wird auch darauf geachtet, wie die Schweiz (vor allem der Bund, aber auch die Kantone) den Datenschutz sicherstellt.
- Der **EU-Datenschutz-Richtlinie 2016/680**[6] regelt das Datenbearbeiten im Rahmen der justiziellen und polizeilichen Zusammenarbeit. Sie wurde als Schengen-relevant erklärt und der Schweiz am 1. August 2016 notifiziert. Bund und Kantone müssen nun die entsprechenden

---

1 Übereinkommen vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, SR 0.235.1, und Zusatzprotokoll vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung, SR 0.235.11.

2 BBl 2020 599.

3 Vgl. die Botschaft vom 6. Dezember 2019 zur Genehmigung des Protokolls vom 10. Oktober 2018 zur Änderung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (BBl 2020 565). National- und Ständerat haben das Protokoll am 19. Juni 2020 genehmigt. Referendumsvorlage: BBl 2020 5725. Die Referendumsfrist ist am 8. Oktober 2020 ungenutzt verstrichen.

4 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. L 119 vom 4.5.2016, 1 ff.

5 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281 vom 23.11.1995, 31 ff.

6 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. L 119 vom 4.5.2016, 89 ff.

Anpassungen in ihrem Datenschutzrecht vornehmen, wenn sie nicht die Kündigung des Schengen-Assoziierungs-Abkommens riskieren wollen.

Der Bundesrat seinerseits hat das Bundes-Datenschutzgesetz (DSG)[7] evaluiert und aufgrund der festgestellten Schwächen beschlossen, den Datenschutz zu stärken.[8] Am 15. September 2017 hat er den Entwurf zu einer Revision des Datenschutzrechts (E-DSG)[9] veröffentlicht und die entsprechende Botschaft der Bundesversammlung überwiesen.[10] Mit diesem Entwurf will er auch sicherstellen, dass auf Bundesebene die Anforderungen aus der (modernisierten) Europarats-Konvention 108+ und der EU-Datenschutzreform erfüllt werden. Die Bundesversammlung hat die Vorlage aufgeteilt und mit einem «Schengen-Datenschutzgesetz» (SDSG)[11] vorweg die Anpassungen vorgenommen, die wegen der Schengen-relevanten Richtlinie (EU) 2016/680 nötig sind; dieses Gesetz ist seit dem 1. März 2019 in Kraft. Am 25. September 2020 haben die eidgenössischen Räte die Totalrevision des DSG abgeschlossen[12]; die Referendumsfrist ist am 14. Januar 2021 ungenutzt abgelaufen. Mit Inkrafttreten des totalrevidierten DSG (revDSG)[13] soll dann das SDSG wieder aufgehoben werden.

Die Kantone müssen ihr kantonales Datenschutzrecht ebenfalls anpassen, weil die (modernisierte) Europarats-Konvention 108+ auch für sie gelten wird, weil sie aufgrund der Schengen-Assoziierung die Richtlinie (EU) 2016/680 umsetzen müssen und weil das Niveau des kantonalen Rechts bei der Beurteilung der Angemessenheit des Schweizer Datenschutzniveaus durch die EU-Kommission mitberücksichtigt wird. Die Angemessenheit wird von der EU-Kommission periodisch geprüft (aktuell läuft die Prüfung, ob das Schweizer Datenschutzrecht dem neuen EU-Datenschutzrecht, insbesondere der DSGVO, angemessen ist). Die Umsetzung der Schengen-Vorgaben wird im Rahmen von «Schengen-Evaluationen» durch Expertinnen und Experten aus den Schengen-Staaten regelmässig überprüft (letztmals 2018, das nächste Mal spätestens 2023).

Wie bereits bei der Assoziierung der Schweiz an Schengen und Dublin hat die Konferenz der Kantonsregierungen (KdK) auch für die jetzt notwendigen Anpassungen zuhanden der Kantone einen Leitfaden ausarbeiten lassen und den Kantonen zugestellt.[14] Eine Analyse zeigt, dass sich der Anpassungsbedarf für den Kanton Basel-Stadt im interkantonalen Vergleich in Grenzen hält. Viele Bestimmungen des IDG dienten auch als Muster für die KdK-Vorschläge.

# 3. Anpassungsbedarf

## 3.1 Übersicht

Mit dieser Revision soll der Anpassungsbedarf aufgrund der europäischen Weiterentwicklungen gedeckt werden. Es besteht Anpassungsbedarf insbesondere in folgenden Punkten:

- Geltungsbereich: Wegfall von generellen Ausnahmen, Schutz nur für natürliche Personen;
- Begriffe: u.a. Aufnahme von genetischen Daten, Daten über das Sexualleben und die sexuelle Orientierung und biometrische Daten als sog. «sensitive» Personendaten, Profiling als «gefährliche» Datenbearbeitungsart;
- Stärkere Betonung des zeitlichen Elements bei der Verhältnismässigkeit;
- Pflicht zum Nachweis der Datenschutzkonformität;

---

7 Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG), SR 235.1.

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

9 Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBl 2017 7193 (DSG-Gesetzestext ab S. 7206).

10 Botschaft vom 15. September 2017 zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBl 2017 6941; Gesetzesentwurf:

11 Bundesgesetz vom 28. September 2018 über den Datenschutz im Rahmen der Anwendung des Schengen-Besitzstandes in Strafsachen (Schengen-Datenschutzgesetz, SDSG), SR 235.3.

12 Bundesgesetz vom 25. September 2020 über den Datenschutz (Datenschutzgesetz, DSG), BBl 2020 7639.

13 Voraussichtlich im Laufe des Jahres 2022.

14 Leitfaden der Konferenz der Kantonsregierungen (KdK-Leitfaden), EU-Datenschutzreform/Modernisierung der Europarats-Konvention 108: Anpassungsbedarf bei den kantonalen (Informations- und) Datenschutzgesetzen, Bern, 02.02.2017, abrufbar über den Link «KdK Leitfaden DSG Kantone» auf der Website des Datenschutzbeauftragten des Kantons Basel-Stadt (https://www.dsb.bs.ch/datenschutz/privatim-und-kdk-leitfaden.html, Kurz-URL: https://bit.ly/2sfj00f).

- Präzisierung bei der Auftragsdatenbearbeitung;
- Voraussetzung für die Vornahme eines Profilings;
- Verstärkung des präventiven Datenschutzes: Pflicht zur Datenschutz-Folgenabschätzung (als Vorbereitung zur Vorabkonsultation der oder des Datenschutzbeauftragten [bisher: Vorabkontrolle]); Datenschutz durch Technikgestaltung («Privacy by design») und datenschutzfreundliche Voreinstellungen («Privacy by default»);
- Verstärkung der Transparenz: Einführung der Informationspflicht beim Beschaffen von (auch «gewöhnlichen») Personendaten;
- Einführung der Meldepflicht bei Datenschutzverletzungen;
- Recht der betroffenen Personen auf Löschung von Personendaten (bei widerrechtlichem Bearbeiten);
- Pflicht der oder des Datenschutzbeauftragten zur Behandlung von aufsichtsrechtlichen Anzeigen.

Andererseits werden einige Vorgaben aus dem europäischen Datenschutzrecht als nicht erforderlich oder unverhältnismässig beurteilt, weshalb auf ihre Umsetzung bewusst verzichtet wird:
- Verzicht auf die Regelung der automatisierten Einzelentscheidung;
- Verzicht auf die generelle Pflicht der Departemente, Dienststellen und Gemeinden, (betriebliche oder amtsinterne) Datenschutzberaterinnen oder -berater zu benennen, sondern nur Einführung dieser Pflicht im engeren Schengen-Kontext (also für Polizei, Staatsanwaltschaft und Strafvollzug).

Ausserdem besteht unabhängig von den europäischen Datenschutzreformen ein Anpassungs- beziehungsweise Präzisierungsbedarf in folgenden Bereichen:

- Streichung der «Wissenschaft» (Methode) aus der Aufzählung der nicht personenbezogenen Bearbeitungszwecke (§§ 10 und 22 IDG);
- präzisere Umschreibung der Pflichten aus dem Grundsatz der Richtigkeit (§ 11 IDG);
- Pflicht zu Publikation der Videoüberwachungsreglemente (bisher nur auf Verordnungsstufe) und Präzisierung der Ausnahmen (§ 18 IDG);
- Anpassung der Bestimmung zur Herausgabe unanonymisierter Gerichtsurteile an die inzwischen erfolgte Anonymisierungspraxis bei Urteilsveröffentlichungen (§ 22 IDG);
- Präzisierung der Voraussetzungen bei Schutz der eigenen Personendaten (schutzwürdiges Interesse, Kostenlosigkeit) (§ 27 IDG);
- Präzisierungen bei der Pflicht zur Berichterstattung durch die oder den Datenschutzbeauftragten (§ 50 IDG).

Die Begründung der Änderungsvorschläge erfolgt bei den Erläuterungen zu den einzelnen Änderungen (unten Ziff. 3.2).

## 3.2 Zu den einzelnen Änderungen

### 3.2.1 Gegenstand und Zweck (§ 1 IDG)

| Informations- und Datenschutzgesetz vom 9. Juni 2010 | Neu |
|---|---|
| **§ 1.** *Gegenstand und Zweck*<br>[1] Dieses Gesetz regelt den Umgang der öffentlichen Organe mit Informationen.<br>[2] Es bezweckt:<br>a) das Handeln der öffentlichen Organe transparent zu gestalten und damit die freie Meinungsbildung und die Wahrnehmung der demokratischen Rechte zu fördern, soweit nicht überwiegende öffentliche oder private Interessen entgegenstehen, und;<br>b) die Grundrechte von Personen zu schützen, über welche die öffentlichen Organe Personendaten bearbeiten. | **§ 1.** *Gegenstand und Zweck*<br>[1] *unverändert*<br>[2] Es bezweckt:<br>a) *unverändert*<br>b) die Grundrechte von natürlichen Personen zu schützen, über welche die öffentlichen Organe Personendaten bearbeiten. |

**Kommentar**

*Abs. 2 lit. b geändert:*

Anders als die internationalen Vorgaben[15] (und die meisten europäischen Staaten) schützen das IDG wie das DSG und die übrigen kantonalen Datenschutzgesetze bisher nicht nur natürliche, sondern auch juristische Personen. Mit der Totalrevision des Bundesdatenschutzgesetzes wird diese Spezialität aufgehoben.[16] Die Kantone sind zwar nicht verpflichtet, diese Anpassung nachzuvollziehen, doch empfiehlt es sich, das kantonale Recht in diesem Aspekt insbesondere mit dem Datenschutzgesetz des Bundes in Einklang zu bringen, damit der Gegenstand des Datenschutzrechts nicht auseinanderklafft.

Die Auswirkungen für die juristischen Personen sind nicht gross. Der Schutz von Daten juristischer Personen ist nur von geringer praktischer Bedeutung. Für die juristischen Personen gelten zudem ausführliche Publizitätsvorschriften (zum Beispiel im Handelsregisterrecht), die schon bisher die Bekanntgabe von Daten über juristische Personen erlaubt haben. Ausserdem sind die juristischen Personen mit dem Wegfall des Einbezugs nicht schutzlos: Im Bereich des Öffentlichkeitsprinzips gilt weiterhin § 29 Abs. 3 IDG, wodurch der Zugang zu Informationen aus überwiegenden privaten Interessen einzuschränken ist. Private Geheimhaltungsinteressen liegen insbesondere vor, wenn durch den Zugang zu den Informationen Berufs-, Fabrikations- oder Geschäftsgeheimnisse offenbart oder Urheberrechte verletzt würden (§ 29 Abs. 3 lit. b IDG). Diese Bestimmung bleibt unverändert.[17] Ebenso kann der Zugang zu Informationen, die juristische Personen betreffen, weiterhin aufgrund entgegenstehender öffentlicher Interessen oder besonderer gesetzlicher Geheimhaltungspflicht (z.B. Steuergeheimnis) eingeschränkt werden (§ 29 Abs. 1 und 2 IDG).

[15] Art. 1 Abs. 1 der Richtlinie (EU) 2016/680; Art. 1 der geltenden Europarats-Konvention 108 (SR 0.235.1) und der (modernisierten) Europarats-Konvention 108+.
[16] Art. 1, Art. 2 Abs. 1 und Art. 5 lit. a und b des revidierten Bundesdatenschutzgesetzes (revDSG, BBl 2020 7639).
[17] Den Schutz vor Eingriffen durch Private gewährleisten weiterhin etwa der Persönlichkeitsschutz des Zivilgesetzbuchs, das Urheberrecht oder das Gesetz gegen den unlauteren Wettbewerb.

Diese Änderung erfolgt primär durch die Streichung des Begriffs «juristische Personen» in der Begriffsdefinition (§ 3 Abs. 3 IDG). Als Folge davon ist hier die Umschreibung des Gesetzeszwecks anzupassen: Es sollen nur noch die Grundrechte von natürlichen Personen geschützt werden.

### 3.2.2 Geltungsbereich (§ 2 IDG)

| **Informations- und Datenschutzgesetz vom 9. Juni 2010** | **Neu** |
|---|---|
| **§ 2.** *Geltungsbereich* | **§ 2.** *Geltungsbereich* |
| [1] Dieses Gesetz gilt für alle öffentlichen Organe gemäss § 3 Abs. 1. | [1] *unverändert* |
| [2] Es findet keine Anwendung:<br>a) soweit ein öffentliches Organ am wirtschaftlichen Wettbewerb teilnimmt und dabei privatrechtlich handelt;<br>b) in hängigen Verfahren der Zivil- und Strafrechtspflege;<br>c) in hängigen Verfahren der Verfassungs- und Verwaltungsgerichtsbarkeit. | [2] Es findet keine Anwendung, soweit ein öffentliches Organ am wirtschaftlichen Wettbewerb teilnimmt und dabei privatrechtlich handelt. Für das Bearbeiten von Personendaten ist das Bundesgesetz über den Datenschutz (DSG) vom 19. Juni 1992 sinngemäss anwendbar.<br>~~a) soweit ein öffentliches Organ am wirtschaftlichen Wettbewerb teilnimmt und dabei privatrechtlich handelt;~~<br>~~b) in hängigen Verfahren der Zivil- und Strafrechtspflege;~~<br>~~c) in hängigen Verfahren der Verfassungs- und Verwaltungsgerichtsbarkeit.~~<br>[2bis] In hängigen Verfahren der Zivil- und Strafrechtspflege sowie der Verfassungs- und Verwaltungsgerichtsbarkeit richten sich die Rechte und Ansprüche der betroffenen Person, die Informationspflicht des öffentlichen Organs bei der Beschaffung von Personendaten, die Bekanntgabe von Personendaten an Verfahrensbeteiligte, die Information der Öffentlichkeit und der allgemeine Informationszugangsanspruch der Öffentlichkeit ausschliesslich nach dem anwendbaren Verfahrensrecht. |
| [3] Abweichende und ergänzende Bestimmungen in anderen Gesetzen bleiben vorbehalten, sofern sie den Schutz der Grundrechte von Personen, über welche die öffentlichen Organe Personendaten bearbeiten, im Sinne dieses Gesetzes sicherstellen. | [3] *unverändert* |
| [4] Der Regierungsrat sorgt dafür, dass interkantonale Institutionen mit baselstädtischer Beteiligung einen gleichwertigen Datenschutz gewährleisten. | [4] *unverändert* |

## Kommentar

Die neuen internationalen Vorgaben[18] lassen keine generellen Ausnahmen vom Geltungsbereich mehr zu, wie sie das IDG in § 2 Abs. 2 lit. b und c bisher noch kennt.

*Abs. 2 Einleitungssatz und lit. a, geändert:*

Da § 2 Abs. 2 lit. b und c IDG wegfallen, sind der Einleitungssatz von Abs. 2 und der Text von Abs. 2 lit. a zusammenzufassen zum neuen Abs. 2.

Wenn öffentliche Organe am wirtschaftlichen Wettbewerb teilnehmen und dabei privatrechtlich handeln, sind auf ihr Datenbearbeiten nicht die öffentlich-rechtlichen Regeln des IDG, sondern die Regeln für das Bearbeiten von Personendaten durch private Personen aus dem Datenschutzgesetz des Bundes anwendbar. Nur sinngemäss sind die privatrechtlichen Regeln anwendbar, weil die öffentlichen Organe auch bei privatrechtlichem Handeln öffentliche Organe bleiben und nicht Private werden. Sie handeln also nur *wie* Private, nicht *als* Private, und bleiben beispielsweise an die Grundrechte gebunden. Diese Rechtslage besteht schon heute, sie wird neu im Gesetz ausdrücklich festgehalten.

*Abs. 2 lit. b, aufgehoben:*

Nach den internationalen Vorgaben dürfen für hängige gerichtliche Verfahren keine generellen Geltungsbereich-Ausnahmen mehr vorgesehen werden.

Als Begründung für diese Ausnahmen wurde bei der Schaffung der Datenschutzgesetze am Ende der 1980er und anfangs der 1990er Jahre angegeben, es wäre sonst nicht klar, welche Bestimmungen in hängigen Verfahren der Zivil- und Strafrechtspflege sowie der Verfassungs- und Verwaltungsgerichtsbarkeit gelten würden: die Bestimmungen der Prozessordnungen oder diejenigen der Datenschutzgesetze. Das hat sich inzwischen geklärt: Die Lehre unterscheidet zwischen dem allgemeinen Datenschutzrecht und dem besonderen (oder bereichsspezifischen) Datenschutzrecht: Das allgemeine Datenschutzrecht bilden die Datenschutzgesetze mit ihren Grundsätzen, zum Beispiel mit dem Erfordernis einer gesetzlichen Grundlage für das Datenbearbeiten, dem Prinzip der Verhältnismässigkeit und der Transparenz, mit der Verpflichtung zur Informationssicherheit und den Rechten der betroffenen Personen. Ein öffentliches Organ braucht danach für sein Bearbeiten von Personendaten eben eine gesetzliche Grundlage – und die findet es bereichsspezifisch in seinem Fachrecht, also die Sozialhilfe im Sozialhilfegesetz, die Steuerverwaltung in den Steuergesetzen des Bundes und des Kantons usw. Hier, im besonderen Datenschutzrecht, wird also konkret festgelegt, welche Personendaten eine Amtsstelle bearbeiten darf oder muss und welche eben nicht, welche Daten sie anderen Amtsstellen oder Privaten bekannt geben muss, darf oder eben nicht bekannt geben darf (Schweigepflichten) usw. Das allgemeine Datenschutzrecht – also in unserem Kanton das IDG – wird nicht aufgehoben, sondern durch das besondere Datenschutzrecht konkretisiert. Das trifft auch bei den Prozessordnungen zu: Sie bleiben als bereichsspezifisches Datenschutzrecht gültig, auch wenn das IDG mit seinen Grundsätzen neu auch in hängigen Verfahren der Zivil- und Strafrechtspflege sowie der Verfassungs- und Verwaltungsgerichtsbarkeit gelten wird. Das hat zur Konsequenz, dass die Grundsätze des IDG auch für die Gerichte gelten, also zum Beispiel die Pflicht, Informationen vor unbefugtem Zugriff und unbefugter Veränderung zu schützen (§ 8 IDG) oder eine Bearbeitung von Personendaten, die aufgrund der Art der Bearbeitung oder der zu bearbeitenden Daten geeignet ist, besondere Risiken für die Rechte und Freiheit der betroffenen Personen mit sich zu bringen, der oder dem Datenschutzbeauftragten vorab zur Konsultation vorzulegen (§ 13 IDG).

Deshalb soll die Ausnahme für Datenbearbeitungen in hängigen Verfahren der Zivil- und Strafrechtspflege (§ 2 Abs. 2 lit. b IDG) aufgehoben werden.[19]

[18] Art. 2 der Richtlinie (EU) 2016/680; Art. 3 der (modernisierten) Europarats-Konvention 108+.
[19] Vgl. für die ausführliche Herleitung: BEAT RUDIN, Überholte Ausnahmen beim Geltungsbereich, digma 2016, S. 122 ff.

In zwei Bereichen könnte der Wegfall dieser Ausnahmen vom Geltungsbereich ungewollte Konsequenzen haben:
- bei den *Informationsansprüchen* der betroffenen Personen und
- bei der *Aufsicht* über die Datenbearbeitungen in hängigen Verfahren der Zivil- und Strafrechtspflege.

Dem soll mit zwei neuen Ausnahmeregelungen Rechnung getragen werden: Um Kollisionen zwischen den *verfahrensrechtlichen und den datenschutzrechtlichen Informationsansprüchen* der Parteien/der betroffenen Personen zu vermeiden, soll zum einen festgelegt werden, dass sich die Rechte und Ansprüche der betroffenen Personen während hängigen Verfahren der Zivil- und Strafrechtspflege sowie der Verfassungs- und Verwaltungsgerichtsbarkeit ausschliesslich nach dem anwendbaren Verfahrensrecht richten (neuer Abs. $2^{bis}$ in § 2 IDG). Zum anderen soll festgelegt werden, dass Datenbearbeitungen in den entsprechenden hängigen Verfahren nicht der *Aufsicht* der oder des Datenschutzbeauftragten unterstehen (neue Buchstaben c und d in § 38 Abs. 3 IDG). Diese Ausnahme lassen sowohl die Europarats-Konvention 108+ als auch die schengen-relevante Richtlinie (EU) 2016/680 zu[20]

Das bedeutet an Beispielen aus der Strafverfolgung: Zu den Datenbearbeitungen bei der Internetfahndung in einem konkreten Fall hat die oder der Datenschutzbeauftragte nichts zu sagen, da es sich um eine Datenbearbeitung in einem hängigen Verfahren der Strafrechtspflege handelt. Hingegen gelten die allgemeinen Vorschriften des IDG, etwa zur Sicherstellung der Informationssicherheit (§ 8 IDG), auch für die Staatsanwaltschaft. Ebenso wäre beispielsweise die Beschaffung eines IMSI-Catchers[21] – generell, also losgelöst vom konkreten Einsatzfall – nach § 13 IDG der oder dem Datenschutzbeauftragten zur Vorabkontrolle (neu: Vorabkonsultation) vorzulegen; dabei werden die allgemeinen Fragen zur Datenbearbeitung thematisiert, etwa die Frage, wie mit Daten über andere als die Zielpersonen umgegangen wird.

*Abs. 2 lit. c, aufgehoben:*

Nach den internationalen Vorgaben dürfen wie erwähnt keine generellen Geltungsbereich-Ausnahmen mehr vorgesehen werden für hängige gerichtliche Verfahren. Das betrifft auch die bisherige Ausnahme für Datenbearbeitungen in hängigen Verfahren der Verfassungs- und Verwaltungsgerichtsbarkeit (§ 2 Abs. 2 lit. c IDG). Aus diesem Grund soll auch diese Ausnahme aufgehoben werden. Die beiden neuen Ausnahmen (neuer Abs. $2^{bis}$ in § 2 IDG und neue Buchstaben c und d in § 38 Abs. 3 IDG) gelten auch für die hängigen Verfahren der Verfassungs- und Verwaltungsgerichtsbarkeit.

*Abs. $2^{bis}$, neu:*

Wie in den Ausführungen zur Aufhebung von § 2 Abs. 2 Buchstaben b und c IDG dargelegt, soll das Verhältnis zwischen *den verfahrensrechtlichen und den datenschutzrechtlichen Informationsansprüchen* der betroffenen Personen und der Öffentlichkeit in einem neuen Absatz geklärt werden: Während der Hängigkeit von Verfahren der Zivil- und Strafrechtspflege sowie der Verfassungs- und Verwaltungsgerichtsbarkeit sollen sich die Rechte und Ansprüche der betroffenen Person ausschliesslich nach dem anwendbaren Verfahrensrecht richten, also insbesondere nach der Zivilprozessordnung (ZPO)[22], nach der Strafprozessordnung (StPO)[23] und nach dem Gesetz über die Verfassungs- und Verwaltungsrechtspflege (VRPG)[24]. Das heisst, dass die Rechte der betroffenen Person (§ 26–28 IDG) während der Dauer der Hängigkeit ruhen und dass während dieser Zeit ausschliesslich die spezifischen verfahrensrechtlichen Informationsansprüche geltend

[20] Art. 45 Abs. 2 der Richtlinie (EU) 2016/680; Art. 15 Abs. 10 der Europarats-Konvention 108+.
[21] Ein IMSI-Catcher ist ein Gerät, mit dem die auf der Mobilfunkkarte eines Mobiltelefons gespeicherte International Mobile Subscriber Identity (IMSI) ausgelesen und der Standort eines Mobiltelefons innerhalb einer Funkzelle eingegrenzt kann und mit dem eventuell auch Mobilfunktelefonate abgehört werden können.
[22] SR 272.
[23] SR 312.0.
[24] SG 270.100.

gemacht werden können, zum Beispiel nach Art. 53 ZPO, nach Art. 107 f. StPO und nach den Art. 26 f. Verwaltungsverfahrensgesetz (des Bundes)[25], auf den § 21 VRPG verweist. Analoges gilt für die behördliche Informationspflicht gegenüber der betroffenen Person bei der Beschaffung von Personendaten gemäss dem revidierten § 15 IDG (vgl. unten 3.2.14): auch hier gilt, dass die Informationspflichten der Justizbehörden während der Dauer hängiger gerichtlicher Verfahren sich ausschliesslich nach dem anwendbaren Prozessrecht richten.

Die Bestimmung des Zeitpunkts, ab welchem ein Strafverfahren als eröffnet gilt, ist erfahrungsgemäss nicht einfach, hat aber in den vergangenen Jahren bei der Anwendung der Ausnahmebestimmung von § 2 Abs. 2 lit. b IDG nie zu unüberwindbaren Problemen geführt. Mit dem Begriff «betroffene Person» werden auch Personen erfasst, die nicht unter Art. 104/105 StPO fallen und trotzdem über Informationsrechte verfügen (z.B. Drittpersonen bei einer geheimen Überwachungsmassnahme nach Art. 279 StPO).

Neben den Rechten der betroffenen Personen richtet sich auch die proaktive Information der Öffentlichkeit sowie der Anspruch der Öffentlichkeit auf Zugang zu den bei einem öffentlichen Organ vorhandenen Informationen während der Hängigkeit von gerichtlichen Verfahren nicht nach § 20 bzw. § 25 IDG, sondern ausschliesslich nach den verfahrensrechtlichen Bestimmungen. Diese Bestimmungen setzen das verfassungsrechtliche Prinzip der Justizöffentlichkeit[26] um. In Strafverfahren regelt beispielsweise Art. 74 die Information der Öffentlichkeit während hängigen Verfahren.

### 3.2.3 Begriffsdefinitionen (§ 3 IDG)

| **Informations- und Datenschutzgesetz vom 9. Juni 2010** | **Neu** |
|---|---|
| **§ 3.** *Begriffe* | **§ 3.** *Begriffe* |
| [1] Öffentliche Organe im Sinne dieses Gesetzes sind:<br>a) die Organisationseinheiten des Kantons und der Gemeinden, die eine öffentliche Aufgabe erfüllen;<br>b) die Organisationseinheiten der juristischen Personen des kantonalen und kommunalen öffentlichen Rechts, die eine öffentliche Aufgabe erfüllen;<br>c) Private, soweit ihnen von Kanton oder Gemeinden die Erfüllung öffentlicher Aufgaben übertragen ist. | [1] *unverändert* |
| [2] Informationen im Sinne dieses Gesetzes sind alle Aufzeichnungen, welche die Erfüllung einer öffentlichen Aufgabe betreffen, unabhängig von ihrer Darstellungsform und ihrem Informationsträger. | [2] *unverändert* |
| [3] Personendaten sind Informationen, die sich auf eine bestimmte oder bestimmbare natürliche oder juristische Person beziehen. | [3] Personendaten sind Informationen, die sich auf eine bestimmte oder bestimmbare natürliche ~~oder juristische~~ Person beziehen. |
| [4] Besondere Personendaten sind: | [4] Besondere Personendaten sind: |

[25] SR 172.021.
[26] Art. 30 Abs. 3 der Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (BV, SR 101).

| | |
|---|---|
| a) Personendaten, bei deren Bearbeitung eine besondere Gefahr der Grundrechtsverletzung besteht, insbesondere Angaben über:<br><br>1. die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten,<br><br>2. die Gesundheit, das Erbgut, die persönliche Geheimsphäre oder die ethnische Herkunft,<br><br>3. Massnahmen der sozialen Hilfe und<br><br>4. administrative oder strafrechtliche Verfolgungen und Sanktionen. | a) Personendaten, bei deren Bearbeitung eine besondere Gefahr der Grundrechtsverletzung besteht (sensitive Personendaten), insbesondere ~~Angaben über~~:<br>1. Angaben über die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten,<br>2. Angaben über die Gesundheit, das Erbgut (genetische Daten), die persönliche Geheimsphäre, das Sexualleben, die sexuelle Orientierung oder die ethnische Herkunft,<br>3. Angaben über Massnahmen der sozialen Hilfe, ~~und~~<br>4. Angaben über administrative oder strafrechtliche Verfolgungen und Sanktionen und<br>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) Zusammenstellungen von Informationen, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlauben (Persönlichkeitsprofil). | b) *unverändert* |
| [5] Bearbeiten ist jeder Umgang mit Informationen wie das Beschaffen, Aufbewahren, Verwenden, Verändern, Bekanntgeben oder Vernichten, unabhängig von den angewandten Mitteln und Verfahren. | [5] Bearbeiten ist jeder Umgang mit Informationen, unabhängig von den angewandten Mitteln und Verfahren, insbesondere ~~wie~~ das Beschaffen, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten ~~unabhängig von den angewandten Mitteln und Verfahren,~~ sowie das Durchführen logischer oder rechnerischer Operationen mit diesen Informationen. |
| [6] Bekanntgeben ist jedes Zugänglichmachen von Informationen wie das Einsichtgewähren, Weitergeben oder Veröffentlichen. | [6] *unverändert*<br><br>[7] Profiling ist jede Auswertung von Informationen, um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen, insbesondere bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Geheimsphäre oder Mobilität, vorherzusagen.<br><br>[8] Auftragsdatenbearbeiterin oder Auftragsdatenbearbeiter ist die private Person oder das |

| | |
|---|---|
| | öffentliche Organ, die oder das im Auftrag des für die Bearbeitung verantwortlichen öffentlichen Organs Informationen bearbeitet. |

## Kommentar

*Abs. 3, geändert:*

Wie zur Änderung des Gesetzeszwecks bereits ausgeführt (§ 1 Abs. 2 lit. b IDG) soll der Datenschutz im Sinne des IDG künftig juristischen Personen nicht mehr zukommen. Um das zu erreichen, ist in der Definition des Begriffs «Personendaten» das Attribut «juristische» zu streichen. Zu den begrenzten Auswirkungen auf die Rechtsstellung der juristischen Personen siehe oben Ziff. 3.2.1.

*Abs. 4 geändert:*

Abs. 4 enthält die Legaldefinition des Begriffs «besondere Personendaten». Darunter werden zwei Arten von Personendaten zusammengefasst: die «sensitiven» Personendaten, also Personendaten, bei deren Bearbeitung eine besondere Gefahr der Grundrechtsverletzung besteht (lit. a), und die Persönlichkeitsprofile (lit. b). Mit der Einführung des Begriffs des «Profilings» in Abs. 7 ist die Frage zu beantworten, ob der schon im geltenden Recht verwendete Begriff «Persönlichkeitsprofil» noch als Element der besonderen Personendaten beibehalten werden soll. Persönlichkeitsprofil und Profiling erfassen aber unterschiedliche Aspekte: Persönlichkeitsprofile stellen eine «gefährliche» Art von Personendaten dar. Die besondere Gefahr ergibt sich durch die Zusammenstellung bzw. die grosse Menge von Informationen, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlauben. Der neue Begriff des Profilings erfasst dagegen eine «gefährliche» Art des *Bearbeitens* von Personendaten und deckt sich nicht mit dem Begriff des Persönlichkeitsprofils, weshalb Abs. 4 lit. b beibehalten werden soll.

Im Übrigen werden zu den besonderen Personendaten in den internationalen Vorgaben drei Ergänzungen oder Präzisierungen vorgenommen: Neu ist festzuhalten, dass genetische Daten, Angaben zum Sexualleben bzw. zur sexuellen Orientierung und biometrische Daten zu den besonderen Personendaten gehören, weil bei deren Bearbeitung eine besondere Gefahr der Grundrechtsverletzung besteht.[27] Dem soll durch Änderungen in § 3 Abs. 4 Rechnung getragen werden. Im Einzelnen:

*Abs. 4 lit. a Einleitungssatz und Ziff. 1 bis 4, geändert:*

Mit dem Einfügen der Ziff. 5 muss der Satzteil «Angaben über» vom Einleitungssatz in den Text der Ziff. 1 bis 4 verschoben werden. Inhaltlich wird dadurch nichts geändert.

*Abs. 4 lit. a Ziff. 2, geändert:*

Mit dem Einfügen der Klammer «(genetischen Daten)» zum Begriff «Erbgut» wird klargestellt, dass damit dasselbe gemeint ist wie in den internationalen Erlassen.

Da mit der «Geheimsphäre» nicht zwingend auch Angaben zum Sexualleben bzw. zur sexuellen Orientierung mitverstanden werden, werden diese beiden Kategorien neu in die Bestimmung eingefügt.

[27] Art. 3 Ziff. 12 und 13 und Art. 10 der Richtlinie (EU) 2016/680; Art. 6 Abs. 1 der (modernisierten) Europarats-Konvention 108+.

*Abs. 4 lit. a Ziff. 5, neu:*

Die internationalen Erlasse verlangen, dass auch biometrische Daten als besondere Personendaten behandelt werden. Dem wird durch das Einfügen einer neuen Ziff. 5 Rechnung getragen. Biometrische Daten sind *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. Darunter fallen zum Beispiel durch Gesichtserkennungsprogramme gewonnene Daten zu einem Gesicht – aber nicht jedes Foto eines Gesichts! –, daktyloskopische Daten, Handvenen-Muster, Stimm-Muster und Iris-Muster.

*Abs. 5, geändert:*

Die Definition des Begriffs «Bearbeiten» wird an die Umschreibung im revidierten Bundesdatenschutzgesetz angelehnt. Die Änderung dient vor allem der Klärung: Mit Archivieren ist die Weiteraufbewahrung zu einem anderen als dem Erhebungszweck gemeint; sie erfolgt (im Sinne von § 16 IDG) allenfalls, nachdem die Daten für die Aufgabe, zu deren Erfüllung sie erhoben worden sind, nicht mehr benötigt werden. Vernichten hat schon bisher das endgültige physische «Zerstören» gemeint. Löschen ist das Entfernen von Daten aus dem aktiven Prozess (ähnlich wie das «Löschen» von Strafregistereinträgen). Zum Schluss wird noch – wie in der modernisierten Europarats-Konvention[28] – klargestellt, dass auch das Durchführen logischer und/oder rechnerischer Operationen mit Informationen ein Bearbeiten darstellt.

*Abs. 7, neu:*

Die Richtlinie (EU) 2016/680 regelt neu das Profiling[29] (als besondere, «gefährliche» Art des *Bearbeitens* von Personendaten), das denselben Anforderungen genügen muss wie das Bearbeiten von besonderen Personendaten.[30] Im Interesse der einfachen Formulierung und Verständlichkeit ist «Profiling» in die Begriffsdefinitionen aufzunehmen. Beim Profiling geht es um ein automatisiertes Bearbeiten von Personendaten mit dem Ziel, bestimmte persönliche Aspekte zu bewerten. Im Vordergrund stehen die Analyse persönlicher Merkmale und die Vorhersage von Entwicklungen, insbesondere bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel.

Der Begriff des Persönlichkeitsprofils (§ 3 Abs. 4 lit. b IDG) als eine Erscheinungsform der besonderen Personendaten kann beibehalten werden[31].

*Abs. 8, neu:*

Das internationale Recht definiert die Begriffe der «für die Verarbeitung verantwortlichen Person» (*controller*) und des «Auftragsverarbeiters» (*processor*). Eine Übernahme des Begriffes der oder des Verantwortlichen kann im öffentlichen Recht unterbleiben, da in § 6 IDG die Verantwortlichkeit des öffentlichen Organs, das die Informationen zur Erfüllung seiner gesetzlichen Aufgaben bearbeitet (oder – in Verbindung mit § 7 Abs. 2 IDG – bearbeiten lässt), bereits klar geregelt wird. Hingegen ergibt es Sinn, den Begriff der Auftragsdatenbearbeiterin bzw. des Auftragsdatenbearbeiters zu definieren: Damit ist die private Person oder das (andere) öffentliche Organ gemeint, die oder das im Auftrag des für die Bearbeitung verantwortlichen öffentlichen Organs Informationen bearbeitet. Weil es nicht generell um eine Auftragsbearbeitung, sondern um eine *Daten*bearbeitung im Auftrag geht, wird der Begriff der Auftrags*daten*bearbeiterin bzw. des Auftrags*daten*bearbeiters verwendet[32].

---

28 Art. 2 Bst. b der (modernisierten) Europarats-Konvention 108+.
29 Begriffsdefinition in Art. 3 Ziff. 4 der Richtlinie (EU) 2016/680.
30 Art. 11 Abs. 1 (im Vergleich mit Art. 10) der Richtlinie (EU) 2016/680.
31 KdK-Leitfaden 2017, Ziff. 3.8.
32 Ausserdem wird im schweizerischen Recht seit jeher der Begriff des *Be*arbeitens (und nicht des *Ver*arbeitens) von (Personen-)Daten verwendet.

### 3.2.4 Verantwortung (§ 6 IDG)

| **Informations- und Datenschutzgesetz vom 9. Juni 2010** | **Neu** |
|---|---|
| **§ 6.** *Verantwortung*<br>[1] Die Verantwortung für den Umgang mit Informationen trägt dasjenige öffentliche Organ, das die Informationen zur Erfüllung seiner gesetzlichen Aufgaben bearbeitet. | **§ 6**. *Verantwortung*<br>[1] *unverändert* |
| [2] Bearbeiten mehrere öffentliche Organe einen gemeinsamen Informationsbestand, regeln sie die Verantwortung. | [2] Bearbeiten mehrere öffentliche Organe einen gemeinsamen Informationsbestand, regeln sie die Verantwortung und legen fest, welches öffentliche Organ die Gesamtverantwortung trägt.<br>[3] Das öffentliche Organ muss nachweisen können, dass es die Datenschutzbestimmungen einhält. Der Regierungsrat regelt das Nähere für die kantonale Verwaltung, der Gemeinderat für die kommunale Verwaltung. Für die Gerichte und die selbständigen Anstalten und Körperschaften gilt die Regelung des Kantons sinngemäss. |

**Kommentar**

*Abs. 2, geändert:*

Der bisherige Wortlaut von § 6 Abs. 2 IDG legt fest, dass die an einem Informationsbestand beteiligten öffentlichen Organe untereinander die Verantwortung regeln. In der Praxis hat das dazu geführt, dass in der Regel die Verantwortung geteilt wurde, dass beispielsweise verabredet wurde, jedes öffentliche Organ solle die Verantwortung für «seine» Daten tragen. Das mag korrekt sein in Bezug auf die (inhaltliche) Richtigkeit der Daten (§ 11 IDG). Allerdings wird mit dieser Regelung nicht sichergestellt, dass alle Aspekte einer Datenbearbeitung in den Verantwortungsbereich eines Organs fallen. Insbesondere die Bestimmung des Schutzbedarfs des Gesamtsystems oder die Durchführung einer Risikoanalyse für das Gesamtsystem muss durch *eine* Stelle erfolgen. Aus diesem Grund ist neu festzulegen, dass für solche Informationsbestände ein öffentliches Organ zu bestimmen ist, dem die Gesamtverantwortung zukommt.[33] Es können durchaus Teilverantwortlichkeiten den einzelnen beteiligten Organen zugewiesen werden – alles, was aber nicht in eine solche Teilverantwortlichkeit fällt, obliegt dem Organ, das die Gesamtverantwortung trägt.

*Abs. 3, neu:*

Mehrfach wird in den neuen internationalen Rechtsgrundlagen verlangt, dass das verantwortliche öffentliche Organ oder die Auftragsdatenbearbeiterin / der Auftragsdatenbearbeiter die Einhaltung der Datenschutzbestimmungen nachweisen können muss.[34]

[33] Für einige wichtige Anwendungen und Datenpools bestehen bereits solche Festlegungen: vgl. z.B. für den Datenmarkt: § 3 der Verordnung über den Datenmarkt (Datenmarktverordnung, DMV) vom 4. Juli 2017, SG 153.310; für das Basler Informationssystem Sozialleistungen (BISS): § 35 der Verordnung über die Harmonisierung und Koordination von bedarfsabhängigen Sozialleistungen (SoHaV) vom 25. November 2008, SG 890.710.

[34] Art. 4 Abs. 4 der Richtlinie (EU) 2016/680; Art. 10 Abs. 1 der (modernisierten) Europarats-Konvention 108+.

Wie dieser Nachweis erbracht werden muss, kann und soll nicht auf Gesetzesstufe festgelegt werden. Es soll kein bürokratischer Leerlauf geschaffen werden. Grössere Systeme können heute schon in verantwortlicher Weise nur mit einem Datenschutzmanagementsystem (DSMS) oder einem (um Datenschutzaspekte angereichertes) 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.

Es ist sinnvollerweise auf Verordnungsstufe festzulegen, in welchen Fällen ein solches DSMS obligatorisch sein soll (z.B. nur wenn besondere Personendaten oder Personendaten, die einem besonderen Amtsgeheimnis unterstehen, bearbeitet werden). Die durch den Regierungsrat zu erlassende kantonale Regelung soll – wie die Regelung zur Informationssicherheit nach § 8 Abs. 4 IDG – nicht nur für die Kernverwaltung gelten, sondern auch für die Gerichte, die selbständigen Anstalten und Körperschaften und die administrativ dem Grossen Rat zugeordneten «Kleeblatt-Dienststellen». Da insbesondere die Gerichte nicht unter den Begriff der Verwaltung subsumiert werden können und die Gerichte sowie die selbständigen Anstalten und Körperschaften in der analogen Delegationsbestimmung von § 18 Abs. 5 IDG (hinsichtlich der näheren Regelungen zu Videoüberwachungssystemen) ausdrücklich genannt werden, sind sie auch in § 6 Abs. 3 sowie § 8 Abs. 4 IDG ausdrücklich zu nennen.

### 3.2.5 Auftragsdatenbearbeitung (§ 7 IDG)

| **Informations- und Datenschutzgesetz vom 9. Juni 2010** | **Neu** |
|---|---|
| **§ 7.** *Bearbeiten im Auftrag* | **§ 7.** *Bearbeiten im Auftrag* |
| [1] Das öffentliche Organ kann das Bearbeiten von Informationen einer Auftragsdatenbearbeiterin oder einem Auftragsdatenbearbeiter übertragen, wenn:<br>a) keine rechtliche Bestimmung oder vertragliche Vereinbarung entgegensteht und<br>b) sichergestellt wird, dass die Informationen nur so bearbeitet werden, wie es das öffentliche Organ tun dürfte. | [1] *unverändert* |
| [2] Es bleibt für den Umgang mit Informationen nach diesem Gesetz verantwortlich. | [2] *unverändert* |
| | [3] Eine Auftragsdatenbearbeiterin beziehungsweise ein Auftragsdatenbearbeiter darf ohne die vorgängige schriftliche Zustimmung des auftraggebenden öffentlichen Organs die Datenbearbeitung keiner weiteren Auftragsdatenbearbeiterin und keinem weiteren Auftragsdatenbearbeiter übertragen. |

**Kommentar**

*Abs. 3, neu:*

Die Voraussetzungen für Auftragsdatenbearbeitungen müssen nicht grundsätzlich verändert werden. Zwar stellen sich immer wieder Fragen, inwiefern rechtliche Bestimmungen (zum Beispiel besondere Amtsgeheimnisse wie das Steuergeheimnis, das Sozialhilfegeheimnis oder das Opferhilfegeheimnis oder Berufsgeheimnisse wie das medizinische) einem solchen Auftrag entgegenstehen. Das lässt sich jedoch nicht im Rahmen des IDG klären, sondern braucht klarere gesetzliche Bestimmungen im entsprechenden Fachrecht.

Eine zusätzliche Sicherheit ist aber einzubauen:[35] Die Auftragsdatenbearbeiterin beziehungsweise der Auftragsdatenbearbeiter darf die Datenbearbeitung keiner weiteren Auftragsdatenbearbeiterin und keinem weiteren Auftragsdatenbearbeiter übertragen, es sei denn, das auftraggebende öffentliche Organ hat diesem Subcontracting vorgängig schriftlich zugestimmt. Das kann schon im Rahmen des ursprünglichen Auftrages geschehen oder nachträglich als Ergänzung des ursprünglichen Auftrages. Diese zusätzliche Hürde ist gerechtfertigt, weil das auftraggebende öffentliche Organ nach § 7 Abs. 2 IDG verantwortlich bleibt. Schon mit dem Beizug eines Dritten geht ein gewisser Kontrollverlust einher – der darf aber nicht durch weitere Auslagerungen vergrössert werden, ohne dass das verantwortlich bleibende auftraggebende öffentliche Organ dem zustimmt.

Zur Verstärkung der Wirkung des Subcontracting-Verbots ist die Strafnorm des § 51 IDG anzupassen (unten Ziff. 3.2.31).

Das grundsätzliche Verbot des Subcontracting ohne Zustimmung des auftraggebenden öffentlichen Organs gilt von Gesetzes wegen. Es muss nicht vertraglich vereinbart werden; hingegen ist die Auftragsdatenbearbeiterin beziehungsweise der Auftragsdatenbearbeiter im Auftrag darauf aufmerksam zu machen, dass dieses Verbot gilt und die Verletzung strafrechtlich verfolgt werden kann.

### 3.2.6 Informationssicherheit (§ 8 IDG)

| **Informations- und Datenschutzgesetz vom 9. Juni 2010** | **Neu** |
|---|---|
| **§ 8.** *Informationssicherheit*<br>[1] Das öffentliche Organ schützt Informationen durch angemessene organisatorische und technische Massnahmen.<br>[2] Die Massnahmen richten sich nach den folgenden Schutzzielen:<br>a) Informationen dürfen nicht unrechtmässig zur Kenntnis gelangen (Vertraulichkeit);<br>b) Informationen müssen richtig und vollständig sein (Integrität);<br>c) Informationen müssen bei Bedarf vorhanden sein (Verfügbarkeit);<br>d) Informationsbearbeitungen müssen einer Person zugerechnet werden können (Zurechenbarkeit); | **§ 8**. *Informationssicherheit*<br>[1] *unverändert*<br>[2] *unverändert* |

[35] Art. 22 Abs. 2 der Richtlinie (EU) 2016/680.

| | |
|---|---|
| e) Veränderungen von Informationen müssen erkennbar und nachvollziehbar sein (Nachvollziehbarkeit). | |
| [3] Die zu treffenden Massnahmen richten sich nach der Art der Information, nach Art und Zweck der Verwendung und nach dem jeweiligen Stand der Technik. | [3] *unverändert* |
| [4] Der Regierungsrat regelt das Nähere für die kantonale Verwaltung, der Gemeinderat für die kommunale Verwaltung. | [4] Der Regierungsrat regelt das Nähere für die kantonale Verwaltung, der Gemeinderat für die kommunale Verwaltung. Für die Gerichte und die selbständigen Anstalten und Körperschaften gilt die Regelung des Kantons sinngemäss. |

Schon bisher wies § 18 Abs. 5 IDG ausdrücklich darauf hin, dass die vom Regierungsrat zu erlassende Detailregelung nicht nur für die kantonale Verwaltung (im engeren Sinne) gilt, sondern auch für die Gerichte und die selbständigen Anstalten und Körperschaften. Zwar wurde § 8 Abs. 4 IDG schon bisher ebenso gelesen; die Anpassung führt aber zu mehr Klarheit und Einheitlichkeit des Gesetzes (vgl. die entsprechende Ergänzung von § 6 Abs. 3 IDG). Am Inhalt der Bestimmung ändert sich dadurch nichts.

### 3.2.7 Voraussetzungen für das Bearbeiten von Personendaten (§ 9 IDG)

| **Informations- und Datenschutzgesetz vom 9. Juni 2010** | **Neu** |
|---|---|
| **§ 9.** *Voraussetzungen für das Bearbeiten von Personendaten* | **§ 9.** *Voraussetzungen für das Bearbeiten von Personendaten* |
| [1] Ein öffentliches Organ darf Personendaten bearbeiten, wenn | [1] *unverändert* |
| a) dafür eine gesetzliche Grundlage besteht oder<br>b) dies zur Erfüllung einer gesetzlichen Aufgabe erforderlich ist. | |
| [2] Besondere Personendaten dürfen bearbeitet werden, wenn | [2] Besondere Personendaten dürfen bearbeitet und ein Profiling darf vorgenommen werden, wenn |
| a) ein Gesetz dazu ausdrücklich ermächtigt oder verpflichtet oder<br>b) es für eine in einem Gesetz klar umschriebene Aufgabe zwingend notwendig ist. | a) ein Gesetz dazu ausdrücklich ermächtigt oder verpflichtet oder<br>b) es für eine in einem Gesetz klar umschriebene Aufgabe zwingend notwendig ist. |
| [3] Das Bearbeiten von Personendaten hat nach Treu und Glauben zu erfolgen und muss verhältnismässig sein | [3] *unverändert* |
| | [4] Personendaten dürfen nur so lange bearbeitet werden, als es zur Erfüllung der gesetzlichen Aufgabe erforderlich ist. |

## Kommentar

*Abs. 2 Einleitungssatz, geändert:*

Wie bei den Begriffsdefinitionen bereits ausgeführt (oben Ziff. 3.2.3 zu § 3 Abs. 7 [neu] IDG), verlangt die Richtlinie (EU) 2016/680, dass zur Vornahme eines Profilings (§ 3 Abs. 7 [neu] IDG) die gleichen Voraussetzungen erfüllt sein müssen wie beim Bearbeiten von besonderen Personendaten. Aus diesem Grund wird hier, bei den Voraussetzungen für das Bearbeiten von besonderen Personendaten, das Profiling hinzugeführt. Dieselbe Ergänzung muss bei den Voraussetzungen für das Bekanntgeben von besonderen Personendaten in § 21 Abs. 2 IDG (unten Ziff. 3.2.20) vorgenommen werden.

*Abs. 4, neu:*

Jedes Bearbeiten von Personendaten muss verhältnismässig sein (§ 9 Abs. 3 IDG). Schon bisher gehörte zur Verhältnismässigkeit, dass das Bearbeiten von Personendaten zeitlich befristet sein muss. In der Praxis wird, wie verschiedene Datenschutz-Prüfungen des Datenschutzbeauftragten gezeigt haben, diesem Grundsatz teilweise nicht genügend Beachtung geschenkt.[36] Neu wird verlangt, dass für die Löschung (oder Anonymisierung) von Personendaten bzw. für eine regelmässige Überprüfung, ob Personendaten zur Aufgabenerfüllung noch erforderlich sind, Fristen vorzusehen sind und dass durch verfahrensrechtliche Vorkehrungen sicherzustellen ist, dass diese Fristen eingehalten werden.[37] Erforderlich ist also mindestens eine Vorgabe für die Löschung (oder Anonymisierung) von Personendaten, die zur Aufgabenerfüllung nicht mehr benötigt werden, sofern sie nicht nach Archivrecht zu archivieren sind.

Im neuen Abs. 4 soll der Grundsatz festgehalten werden. Ergänzend dazu findet die zeitliche Begrenzung der Bearbeitung von Personendaten auch im neuen Abs. 2 zu § 16 IDG ihren Niederschlag.

### 3.2.8 Pilotversuche (§ 9a IDG)

| **Informations- und Datenschutzgesetz vom 9. Juni 2010** | **Neu** |
|---|---|
| **§ 9a** *Voraussetzungen für das Bearbeiten von besonderen Personendaten im Rahmen von Pilotversuchen* | **§ 9a.** *Voraussetzungen für das Bearbeiten von besonderen Personendaten im Rahmen von Pilotversuchen* |
| [1] Der Regierungsrat kann, nachdem er im Rahmen einer Vorabkontrolle nach § 13 die Beurteilung der oder des Datenschutzbeauftragten eingeholt hat, vor Wirksamwerden eines Gesetzes die Bearbeitung von besonderen Personendaten bewilligen, wenn: | [1] Der Regierungsrat kann, nachdem er im Rahmen einer ~~Vorabkontrolle~~ Vorabkonsultation nach § 13 die Beurteilung der oder des Datenschutzbeauftragten eingeholt hat, vor Inkrafttreten eines Gesetzes die Bearbeitung von besonderen Personendaten bewilligen, wenn: |
| a) die Aufgaben, die diese Bearbeitung erforderlich machen, in einem Gesetz geregelt sind,<br>b) ausreichende Massnahmen zur Verhinderung von Persönlichkeitsverletzungen getroffen werden und | a)-c) *unverändert* |

[36] Vgl. insbesondere Tätigkeitsbericht 2015 des Datenschutzbeauftragten des Kantons Basel-Stadt, S. 33.
[37] Art. 5 der Richtlinie (EU) 2016/680; Art. 5 Abs. 4 lit. e der (modernisierten) Europarats-Konvention 108+.

| | |
|---|---|
| c) die praktische Umsetzung einer Datenbearbeitung eine Testphase vor dem Wirksamwerden des Gesetzes zwingend erfordert. | |
| [2] Die praktische Umsetzung einer Datenbearbeitung kann eine Testphase dann zwingend erfordern, wenn: | [2] *unverändert* |
| a) die Erfüllung einer Aufgabe technische Neuerungen erfordert, deren Auswirkungen zunächst evaluiert werden müssen, | |
| 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 | |
| c) sie die Übermittlung von besonderen Personendaten an Dritte mittels eines Abrufverfahrens erfordert. | |
| [3] Pilotprojekte sind auf maximal fünf Jahre zu befristen. | [3] *unverändert* |
| [4] Jedes Pilotprojekt ist zu evaluieren. | [4] *unverändert* |
| [5] Der Regierungsrat regelt die Modalitäten der Datenbearbeitung in einer Verordnung. | [5] *unverändert* |

## Kommentar

*Abs. 1, geändert:*

Die bisherige Vorabkontrolle heisst neu Vorabkonsultation (§ 13 IDG, unten Ziff. 3.2.12). Aus diesem Grund muss die Terminologie in § 9a Abs. 1 IDG angepasst werden.

### 3.2.9 Voraussetzungen für das Bearbeiten von Personendaten zu einem nicht personenbezogenen Zweck (§ 10 IDG)

| Informations- und Datenschutzgesetz vom 9. Juni 2010 | Neu |
|---|---|
| **§ 10.** *Voraussetzungen für das Bearbeiten von Personendaten zu einem nicht personenbezogenen Zweck*<br>[1] Ein öffentliches Organ darf Personendaten zu einem nicht personenbezogenen Zweck, namentlich für Statistik, Planung, Wissenschaft oder Forschung, bearbeiten, wenn es<br>a) diese Daten nicht mehr für einen personenbezogenen Zweck verwendet oder weitergibt und<br>b) diese Daten anonymisiert oder pseudonymisiert, sobald es der Bearbeitungszweck erlaubt, und<br>c) die Ergebnisse der Bearbeitung nur so bekannt gibt, dass keine Rückschlüsse auf betroffene Personen möglich sind.<br>[2] … | **§ 10.** *Voraussetzungen für das Bearbeiten von Personendaten zu einem nicht personenbezogenen Zweck*<br>[1] Ein öffentliches Organ darf Personendaten zu einem nicht personenbezogenen Zweck, namentlich für Statistik, Planung~~, Wissenschaft~~ oder Forschung, bearbeiten, wenn es<br>a)-c) *unverändert* |

**Kommentar**

*Abs. 1 Einleitungssatz, geändert:*

Die Erwähnung der «Wissenschaft» geht auf die gemeinsame Erarbeitung der Informations- und Datenschutzgesetze der beiden Basel zurück. Das frühere Datenschutzgesetz des Kantons Basel-Stadt erwähnte in seinem § 15 Abs. 1 im Gegensatz zum Baselbieter DSG (§ 12 Abs. 1) nur Forschung, Statistik und Planung. Mit Erlass des IDG wurde der Begriff der Wissenschaft aus dem basellandschaftlichen Gesetz übernommen. Wissenschaft (bzw. Wissenschaftlichkeit) betrifft jedoch nicht den Bearbeitungszweck, sondern die Methode. Was damit gemeint war, ist weiterhin in «Forschung» mitenthalten. Die Erwähnung der «Wissenschaft» hat deshalb keine eigenständige Bedeutung[38] und soll im Rahmen dieser Revision beseitigt werden (siehe auch unten Ziff. 3.2.21 zu § 22).

### 3.2.10 Richtigkeit (§ 11 IDG)

| Informations- und Datenschutzgesetz vom 9. Juni 2010 | Neu |
|---|---|
| **§ 11.** *Richtigkeit*<br>[1] Personendaten müssen richtig und, soweit es der Verwendungszweck erfordert, vollständig sein. | **§ 11.** *Richtigkeit*<br>[1] *unverändert*<br>[2] Wer Personendaten bearbeitet, hat sich über deren Richtigkeit zu vergewissern. |

[38] BEAT RUDIN, § 10 N 7, in: Beat Rudin/Bruno Baeriswyl (Hrsg.), Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Basel-Stadt, Zürich/Basel/Genf 2014 (im Folgenden zitiert als: PK-IDG/BS).

| | |
|---|---|
| | [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. |

## Kommentar

*Abs. 2, neu:*

Aus dem bisher geltenden Gesetzestext ging nicht hervor, was die Anforderung der Richtigkeit bedeutet.[39] In Übereinstimmung mit der Regelung im Bundesdatenschutzgesetz sollen nun in § 11 Absätze 2 und 3 die Handlungspflichten klar benannt werden.

Das öffentliche Organ, das zur Aufgabenerfüllung Personendaten bearbeitet, muss sich vergewissern, ob die Daten richtig sind. Der Umfang dieser Vergewisserungspflicht ist im Einzelfall zu bestimmen. Stammen die Daten von der betroffenen Person selber, dann darf das öffentliche Organ – aus datenschutzrechtlicher Sicht – auf die Richtigkeit vertrauen, muss also keine zusätzlichen Prüfschritte unternehmen. In einem solchen Fall kann aber aus anderen Gründen eine vertiefte Prüfung angezeigt sein, etwa wenn mit den Daten das Bestehen eines Anspruchs auf eine staatliche Leistung behauptet wird. Die betroffene Person kann dabei eine Mitwirkungspflicht treffen, etwa wenn sich ursprünglich richtig erfasste Daten nachträglich aufgrund von Umständen, die die Behörde nicht kennen kann, als unrichtig erweisen.

Die Vergewisserungspflicht greift nicht permanent, sondern nur, wenn die Personendaten aktiv bearbeitet werden. Wenn ein öffentliches Organ Personendaten zur Aufgabenerfüllung erhebt, muss es die Daten allenfalls noch über die Phase der eigentlichen Aufgabenerfüllung hinaus weiter aufbewahren, weil eine solche Aufbewahrungsfrist gesetzlich vorgesehen ist oder weil die Aufbewahrung zu Beweis- und Sicherungszwecken erforderlich ist (Festlegung einer Frist im neuen Abs. 2 von § 16, siehe auch unten Ziff. 3.2.16). In dieser «inaktiven» Phase muss sich das öffentliche Organ nicht ständig vergewissern, ob die Daten noch richtig sind oder allenfalls unrichtig geworden sind. Die Vergewisserungspflicht lebt erst wieder auf, wenn die Daten wieder aktiv bearbeitet werden, wenn sie also beispielweise erneut für die Prüfung gebraucht werden, ob ein Leistungsanspruch besteht, oder wenn bei einer andauernden Leistung geprüft werden soll, ob der Anspruch noch zu Recht besteht.[40]

*Abs. 3, neu:*

Wenn sich Personendaten als unrichtig herausstellen, dann ist dafür zu sorgen, dass die Korrektur – die Berichtigung oder die Löschung nach § 27 IDG – auch umgesetzt werden kann.[41] Bei Papierdossiers ist dies einfacher zu bewerkstelligen, bei IT-Systemen muss das mit angemessenen Massnahmen sichergestellt werden. Wenn beispielsweise bei einem IT-System wegen der Revisionstauglichkeit (unrichtige) Einträge nicht einfach durch die richtigen Einträge ersetzt werden können, ist auf andere Weise sicherzustellen, dass die Berichtigung umgesetzt wird, etwa durch spätere Ergänzungen, die mit dem ursprünglichen Eintrag verknüpft werden, wie das etwa bei Rapportsystem der Kantonspolizei der Fall ist. Gleichzeitig wird mit dem neuen Gesetzestext auch festgehalten, dass es nicht um eine «absolute» Richtigkeit und Vollständigkeit geht, sondern um Richtigkeit und Vollständigkeit im Hinblick auf dem Zweck der Beschaffung bzw. Bearbeitung der Personendaten.

[39] Vgl. aber Ratschlag 08.0637.01, S. 26; PK-IDG/BS, § 11 N 11 ff.
[40] PK-IDG/BS, § 11 N 12.
[41] PK-IDG/BS, § 11 N 13.

### 3.2.11 Datenschutz-Folgenabschätzung (neuer § 12a IDG)

| Informations- und Datenschutzgesetz vom 9. Juni 2010 | Neu |
|---|---|
| | **§ 12a.** *Datenschutz-Folgenabschätzung*<br>[1] Das verantwortliche öffentliche Organ prüft bei jedem Vorhaben für eine Personendatenbearbeitung, ob voraussichtlich ein hohes Risiko für die Grundrechte der betroffenen Personen besteht. Das hohe Risiko ergibt sich insbesondere bei Verwendung neuer Technologien, aus der Art, dem Umfang, den Umständen und dem Zweck der Bearbeitung.<br>[2] Besteht voraussichtlich ein hohes Risiko, ist eine Datenschutz-Folgenabschätzung durchzuführen.<br>[3] Die Folgenabschätzung enthält mindestens:<br>a) eine allgemeine Beschreibung der geplanten Bearbeitungsvorgänge,<br>b) eine Bewertung der in Bezug auf die Grundrechte der betroffenen Personen bestehenden Risiken sowie<br>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 dieses Gesetz eingehalten wird. |

**Kommentar**

*§ 12a Abs. 1 und 2, neu:*

Neu verlangen die übergeordneten Rechtsgrundlagen[42] eine Datenschutz-Folgenabschätzung (DSFA) durch das verantwortliche öffentliche Organ. Sie ist ein Element des präventiven Datenschutzes mit dem Ziel, ungewollte Datenschutzrisiken rechtzeitig zu erkennen und im Sinne von «privacy by design» zu vermeiden, damit nicht später im Betrieb mühsam und aufwändig nachgebessert werden muss. Es geht darum, die geplanten Bearbeitungsvorgänge zu beschreiben, die in Bezug auf die Grundrechte der betroffenen Personen bestehenden Risiken zu ermitteln und zu bewerten sowie die geplanten Abhilfemassnahmen, Garantien, Sicherheitsvorkehren und Verfahren, durch die der Schutz der Grundrechte der betroffenen Personen sichergestellt und der Nachweis erbracht werden soll, dass dieses Gesetz eingehalten wird, darzustellen und zu bewerten.

Diese Datenschutz-Folgenabschätzung ist zwar neu in den Rechtsgrundlagen verankert. Von den baselstädtischen Behörden verlangt sie aber nichts komplett Neues: Sie mussten schon bisher «gefährliche» Datenbearbeitungsvorhaben der oder dem Datenschutzbeauftragten zur Vorabkontrolle (§ 13 IDG, §§ 2-4 IDV) vorlegen. Die DSFA ist im Grunde genommen nichts anderes als die

[42] Art. 27 der Richtlinie (EU) 2016/680; Art. 10 Abs. 2 der (modernisierten) Europarats-Konvention 108+.

*Vorbereitung des verantwortlichen öffentlichen Organs für die Vorabkontrolle* (§ 13 IDG, neu: Vorabkonsultation, unten Ziff. 3.2.12), und gleichzeitig dient sie dem öffentlichen Organ dazu, die Voraussetzungen zu schaffen, um den Nachweis der Einhaltung der Datenschutzvorschriften (neuer Abs. 3 zu § 6 IDG, oben Ziff. 3.2.4) erbringen zu können.

Unter «Vorhaben», die einer DSFA zu unterziehen sind (und eventuell zur Vorabkonsultation der oder des Datenschutzbeauftragten nach § 13 IDG führen), sind nicht einzelne, konkrete Bearbeitungen wie beispielsweise eine Einzelbekanntgabe von Personendaten zu verstehen – obwohl das verantwortliche Organ natürlich auch bei einer solchen Einzelbekanntgabe sicherstellen muss, dass sie gesetz- und verhältnismässig ist und keine Persönlichkeits- oder Grundrechte der betroffenen Personen verletzt. «Vorhaben» i.S.v. § 12a IDG sind die Neueinrichtung und Änderung von Prozessen, Verfahren, Anwendungen u.ä.

In einem ersten, einer allfälligen DSFA vorangehenden Schritt muss das öffentliche Organ bei jedem Vorhaben, bei dem Personendaten bearbeitet werden sollen, beurteilen, ob dieses Bearbeiten voraussichtlich ein hohes Risiko für die Grundrechte der betroffenen Personen zur Folge hat. Der zweite Satz von Abs. 1 konkretisiert dies und hält fest, dass sich das hohe Risiko aus der Art, dem Umfang, den Umständen und dem Zweck der Bearbeitung ergibt. Je umfangreicher die Bearbeitung, je sensibler die bearbeiteten Daten, je umfassender der Bearbeitungszweck, umso eher ist ein hohes Risiko anzunehmen. Beim Einsatz neuer Technologien ist das Vorliegen eines hohen Risikos für die Grundrechte betroffener Personen besonders sorgfältig zu prüfen.[43] Die Beurteilung ist zu dokumentieren. Dieser erste Schritt soll unkompliziert erfolgen können; die oder der Datenschutzbeauftragte kann für die Durchführung (und Dokumentation) dieser Beurteilung Unterlagen zur Verfügung stellen.

*§ 12a Abs. 2, neu:*

Wenn im ersten Schritt nach Abs. 1 festgestellt worden ist, dass bei einem Vorhaben voraussichtlich ein hohes Risiko besteht, ist eine Datenschutz-Folgenabschätzung durchzuführen.

*§ 12a Abs. 3 Buchstaben a-c, neu:*

Der neue § 12 Abs. 3 IDG umschreibt, welche Informationen das verantwortliche öffentliche Organ zusammentragen bzw. erarbeiten muss, damit es die Datenschutzfolgen für die betroffenen Personen abschätzen kann:

- eine allgemeine Beschreibung der geplanten Bearbeitungsvorgänge (lit. a): Projektbeschreibung, Zweck der Bearbeitung, Rechtsgrundlagen, zu bearbeitende («gewöhnliche» und/oder besondere) Personendaten, Beschaffungsarten und -quellen (bei den Betroffenen oder bei Dritten), Auftragsdatenbearbeitungen, Bekanntgabe von Personendaten, allenfalls ins Ausland;
- eine Bewertung der in Bezug auf die Grundrechte der betroffenen Personen bestehenden Risiken (lit. b);
- 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 dieses Gesetz eingehalten wird (lit. c): Dies betrifft insbesondere Vorkehren zur Sicherstellung der Recht- und Verhältnismässigkeit des Datenbearbeitung, die Verantwortlichkeit(en), die Verfahren zur Sicherstellung der Information der Betroffenen und zur Gewährleistung ihrer Rechte (Zugang zu den eigenen Personendaten, Berichtigung unrichtiger Daten, Löschung zu löschender Daten, Einschränkungen der Datenbekanntgabe), Informationssicherheit (inkl. Periodischer Überprüfung), Schulung des Personals, vertragliche Sicherstellung der Rechtmässigkeit bei Auftragsdatenbearbeitungen (inkl. Audits) usw.

[43] Vgl. Art. 27 Abs. 1 der Richtlinie (EU) 2016/680; Art. 22 Abs. 2 Satz 1 revDSG.

Die DSFA ist zu dokumentieren. Die oder der Datenschutzbeauftragte kann für die Durchführung Unterlagen zur Verfügung stellen.

### 3.2.12 Vorabkonsultation (§ 13 IDG)

| **Informations- und Datenschutzgesetz vom 9. Juni 2010** | **Neu** |
|---|---|
| **§ 13.** *Vorabkontrolle* | **§ 13.** ~~*Vorabkontrolle*~~ *Vorabkonsultation der oder des Datenschutzbeauftragten* |
| [1] Wenn eine Bearbeitung von Personendaten aufgrund der Art der Bearbeitung oder der zu bearbeitenden Daten geeignet ist, besondere Risiken für die Rechte und Freiheit der betroffenen Personen mit sich zu bringen, muss diese Bearbeitung vorab der oder dem Datenschutzbeauftragten zur Kontrolle vorgelegt werden. | [1] ~~Wenn eine Bearbeitung von Personendaten aufgrund der Art der Bearbeitung oder der zu bearbeitenden Daten geeignet ist, besondere Risiken für die Rechte und Freiheit der betroffenen Personen mit sich zu bringen, muss diese Bearbeitung vorab der oder dem Datenschutzbeauftragten zur Kontrolle vorgelegt werden.~~ Das verantwortliche öffentliche Organ legt der oder dem Datenschutzbeauftragten frühzeitig zur Vorabkonsultation vor:<br>a) Rechtsetzungsprojekte, die das Bearbeiten von Personendaten betreffen oder die für den Umgang mit Informationen erheblich sind, und<br>b) Vorhaben zur Bearbeitung von Personendaten, die aufgrund der Art der Bearbeitung oder der zu bearbeitenden Daten zu einem hohen Risiko für die Grundrechte der betroffenen Personen führen. |
| [2] Die oder der Datenschutzbeauftragte gibt die Beurteilung in Form einer Empfehlung gemäss § 46 ab. | [2] ~~Die oder der Datenschutzbeauftragte gibt die Beurteilung in Form einer Empfehlung gemäss § 46 ab.~~ Die oder der Datenschutzbeauftragte erstellt eine Liste der Bearbeitungsvorgänge, die zur Vorabkonsultation zu unterbreiten sind. |

**Kommentar**

*Abs. 1, geändert:*

Die Richtlinie (EU) 2016/680[44] (wie auch die Datenschutz-Grundverordnung) sehen vor, dass bestimmte Vorhaben der oder dem Datenschutzbeauftragten vorab zur Konsultation zu unterbreiten sind:

- 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) ein hohes Risiko für die Grundrechte der betroffenen Person,
- Rechtsetzungsvorhaben, welche das Bearbeiten von Personendaten betreffen.

[44] Art. 28 der Richtlinie (EU) 2016/680.

Dies entspricht dem, was bisher schon im Rahmen der Vorabkontrolle (nach § 13 IDG) und der Einholung einer Stellungnahme der oder des Datenschutzbeauftragten zu Erlassen (nach § 44 lit. f IDG) verlangt war.

Unpräzis war der bisherige Name «Vorab*kontrolle*», weil es noch nicht um eine Kontrolle eines konkreten Datenbearbeitens (im Sinne von § 44 lit. a IDG) ging. Ziel des frühzeitigen Einbezuges ist es, den Datenschutz rechtzeitig sicherzustellen, insbesondere:

- bei Rechtsetzungsvorhaben dafür zu sorgen, dass die verfassungs- sowie die informations- und datenschutzrechtlichen Vorgaben berücksichtigt werden,
- bei anderen (zum Beispiel IT-)Vorhaben die Ermittlung und Bewertung der Risiken und der geplanten Massnahmen, um die Risiken auf ein zulässiges Mass zu reduzieren, zu überprüfen und dafür zu sorgen, dass gegebenenfalls mit rechtlichen, organisatorischen oder technischen Massnahmen das Risiko weiter reduziert wird.

Das soll erreicht werden, indem solche Projekte – genauer: das Ergebnis der entsprechenden Datenschutz-Folgenabschätzung– der oder dem Datenschutz zur Stellungnahme vorgelegt werden muss. Daher ist die Bezeichnung «Vorab*konsultation*» zutreffender.

Vorzulegen sind einerseits *Rechtsetzungsvorhaben* (lit. a). Darunter fallen die Schaffung und Änderung von rechtsetzenden Erlassen des Kantons und der Gemeinden. Voraussetzung ist inhaltlich, dass die Vorhaben das Bearbeiten von Personendaten betreffen oder für den Umgang mit Informationen erheblich sind. Die internationalen (Datenschutz-)Vorgaben verlangen die Vorlage von Vorhaben, die den Datenschutz betreffen. Aufgrund der Zuständigkeit der oder des Datenschutzbeauftragten auch im Bereich des Öffentlichkeitsprinzips sind ihr oder ihm – übereinstimmend mit der bisherigen Regelung in § 44 lit. f IDG – auch Vorhaben zur Vorabkonsultation zu unterbreiten, die für den Umgang mit Informationen erheblich sind. Bewährt hat sich auch, dass die Departemente auch bei Bundesvernehmlassungen die Stellungnahme der oder des Datenschutzbeauftragten zuhanden der Vernehmlassungsantwort des Kantons einholen. Wo dies nicht geschieht, kann sie oder er aufgrund der – entsprechend den internationalrechtlichen Anforderungen gesetzlich garantierten – Unabhängigkeit auch direkt zuhanden der Bundesbehörden Stellung nehmen. Sinnvoll ist ausserdem die Einholung der Stellungnahme bei Vorhaben zur generell-abstrakten Umsetzung von Gesetzes- oder Verordnungsbestimmungen (beispielsweise zu Weisungen bezüglich der Umsetzung von § 8 IDG und der Informationssicherheitsverordnung)[45].

Vorzulegen sind andererseits – wie bisher nach § 13 IDG – *Vorhaben zur Bearbeitung von Personendaten*, die aufgrund der Art der Bearbeitung oder der zu bearbeitenden Daten zu einem besonderen Risiko für die Grundrechte der betroffenen Personen führen (lit. b).

Die europarechtlichen Vorgaben sehen die Pflicht zur Vorabkonsultation bei einem «hohen» Risiko vor. Diese Terminologie (in der Steigerungskette geringes / *hohes* / sehr hohes Risiko) wird hier übernommen. Unter «hohem Risiko» wird dasselbe Mass der Gefährdung verstanden, das bisher im Rahmen der Schutzbedarfsanalyse zu einem «erhöhten» Schutzbedarf geführt hat. Die Einschätzung des Risikos ergibt sich aus der Datenschutz-Folgenabschätzung (nach dem neuen § 12a IDG, oben Ziff. 3.2.11): Aufgabe der oder des Datenschutzbeauftragten ist in diesem Fall einerseits die Prüfung der Risikoermittlung und -bewertung, andererseits die Prüfung, ob mit den vorgeschlagenen Massnahmen das Risiko für die betroffenen Personen auf ein zulässiges und zumutbares Mass reduziert wird. Damit diese Prüfungen möglich sind, sind nicht etwa nur Vorhaben vorzulegen, bei denen nach Implementierung der geplanten Massnahmen immer noch ein hohes Risiko besteht, sondern *alle Vorhaben*, bei denen ein hohes Risiko festgestellt wird, *bevor* die geplanten Massnahmen zur Eindämmung des Risikos implementiert werden.

[45] Verordnung vom 13. Dezember 2016 über die Informationssicherheit (ISV), SG 153.320.

Zur näheren Beschreibung, was zu einem hohen Risiko führt, dient einerseits die Konkretisierung in der Informations- und Datenschutzverordnung.[46] Sie braucht grundsätzlich nicht verändert zu werden: Auch weiterhin sollen das Bearbeiten von besonderen Personendaten, das Vorsehen eines Abrufverfahrens, der Einsatz neuer Technologie, die Bearbeitung einer grossen Anzahl von Personen (mehr als 10'000) oder die Errichtung von Datenpools[47] zur Vorlagepflicht führen. Nicht separat erwähnt werden muss, dass der oder dem Datenschutzbeauftragten auch Vorhaben zur Vorabkonsultation vorzulegen sind, wenn dies (spezial-)gesetzlich vorgesehen ist[48].

*Abs. 2, geändert:*

Nach der Richtlinie (EU) 2016/680[49] ist vorzusehen, dass die oder der Datenschutzbeauftragte eine Liste der Verarbeitungsvorgänge erstellen kann, die der Pflicht zur Vorabkonsultation nach Abs. 1 unterliegen. Eine solche Liste – im Sinne einer Positiv- und/oder Negativliste – erleichtert dem verantwortlichen öffentlichen Organ den Entscheid, ob ein Vorhaben der oder dem Datenschutzbeauftragten zur Vorabkonsultation vorzulegen ist oder nicht, weshalb der oder die Datenschutzbeauftragte verpflichtet wird, eine solche zu erstellen.

Im bisherigen Abs. 2 war geregelt, dass die oder der Datenschutzbeauftragte die Beurteilung in Form einer Empfehlung nach § 46 IDG abgibt. Diese Regelung passt nicht mehr, weil neu auch die Stellungnahme zu Rechtsetzungsvorhaben unter § 13 IDG fällt; eine entsprechende Stellungnahme stellt aber keine Empfehlung nach § 46 IDG dar. Die Bestimmung kann aber weggelassen werden, da sich die Möglichkeit, bei der Vorabkonsultation eine Empfehlung abzugeben, unmittelbar aus § 46 IDG ergibt und deshalb hier nicht erwähnt zu werden braucht.

Wie schon bei der Schaffung von §§ 2 ff. IDV soll gesetzlich keine Frist für die Abgabe der Beurteilung bzw. Ausübung der Befugnisse durch die Datenschutzbeauftragte oder den Datenschutzbeauftragten festgelegt werden[50]. Auch wenn eine solche Frist erst zu laufen beginnt, sobald alle erforderlichen Unterlagen vorliegen, ist sie nur beschränkt tauglich. Kleine Vorabkonsultationen sollen rasch erledigt werden können – bei grossen Projekten findet eine Vorabkonsultation ohnehin in verschiedenen Projektphasen gestaffelt statt. Eine generelle gesetzliche Frist würde daher der Praxis nicht gerecht.

### 3.2.13 Datenschutz durch Technikgestaltung («Privacy by design») und durch datenschutzfreundliche Voreinstellungen («Privacy by default») (§ 14 IDG)

| **Informations- und Datenschutzgesetz vom 9. Juni 2010** | **Neu** |
|---|---|
| **§ 14.** *Datenvermeidung und Datensparsamkeit bei IT-Systemen* | **§ 14.** ~~*Datenvermeidung und Datensparsamkeit bei IT-Systemen*~~ *Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen* |
| [1] Das öffentliche Organ gestaltet informationstechnologische Systeme so, dass keine oder möglichst wenig personenbezogene und personenbeziehbare Daten anfallen. | ~~[1] Das öffentliche Organ gestaltet informationstechnologische Systeme so, dass keine oder möglichst wenig personenbezogene und personenbeziehbare Daten anfallen.~~ |
| [2] Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich | ~~[2] Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich~~ |

[46] § 2 IDV.
[47] § 2 Abs. 1 Bst. a-e IDV.
[48] § 2 Abs. 1 Bst. f IDV; dies ist zum Beispiel der Fall nach § 9a Abs. 1 (Pilotversuche) und § 18 Abs. 4 IDG (Videoüberwachungsreglemente), nach § 12 Abs. 3 Geoinformationsgesetz (SG 214.300), nach § 5 Abs. 3 Datenmarktverordnung (SG 153.310) und nach § 35a IWB-Gesetz (SG 772.300).
[49] Art. 28 Abs. 3 der Richtlinie (EU) 2016/680.
[50] Art: 28 Abs. 5 der Richtlinie (EU) 2016/680 sieht eine Frist von sechs Wochen (verlängerbar um einen Monat) vor.

| | |
|---|---|
| ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. | ~~ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.~~<br>[1] Das öffentliche Organ trifft bei Datenbearbeitungen von Anfang an Massnahmen, die das Risiko von Verletzungen der Grundrechte verringern und solchen Verletzungen vorbeugen.<br>[2] Es stellt mittels geeigneter Voreinstellungen sicher, dass standardmässig nur diejenigen Personendaten bearbeitet werden, die für den jeweiligen Verwendungszweck erforderlich sind. |

## Kommentar

*§ 14, geändert:*

Je mehr die Digitalisierung die staatliche Tätigkeit durchdringt, umso wichtiger wird es, die Technologie von Anfang an datenschutzkonform auszugestalten. Dazu dienen die beiden Prinzipien *«Privacy by design»* (Datenschutz durch Technikgestaltung) und *«Privacy by default»* (datenschutzfreundliche Voreinstellungen).[51] Sie sind gleichsam der Inbegriff des präventiven Datenschutzes, mit dem schon vorweg nach Möglichkeit verhindert werden soll, dass die Grundrechte der betroffenen Personen verletzt werden. Die bisher in § 14 IDG erwähnten Prinzipien der Datenvermeidung und Datensparsamkeit sind in den (neu aufgenommenen) Prinzipien «Privacy by design» und «Privacy by default» mitenthalten; der Text des «alten» Paragrafen kann deshalb vollumfänglich durch den neuen Text ersetzt werden.

*Abs. 1, neu:*

Der Grundsatz *«Privacy by design»* verlangt, dass bei Datenbearbeitungen von Anfang an Massnahmen getroffen werden, die das Risiko von Verletzungen der Grundrechte verringern und solchen Verletzungen vorbeugen. Das bedeutet, dass eine Aufgabenerfüllung, wenn dies möglich ist, im Sinne der Datenvermeidung als Ausfluss des Verhältnismässigkeitsprinzips ohne, ohne sensitive, mit weniger oder mit weniger sensitiven Personendaten erfolgt, dass technische Möglichkeiten wie die Anonymisierung oder Pseudonymisierung genutzt werden und dass weitere datenschutzfreundliche Technologien («Privacy enhancing technologies»/PET) verwendet werden. Umzusetzen ist dies etwa dadurch, dass Personendaten nur erhoben werden, wenn eine Rechtfertigung dafür besteht, dass nur die für die Aufgabenerfüllung tatsächlich erforderlichen Personendaten überhaupt erhoben werden, dass Randdaten, die bei der Nutzung von IT-Systemen anfallen, nicht gespeichert, möglichst rasch anonymisiert oder mindestens pseudonymisiert werden oder dass die Zweckänderung der Datenbearbeitung verhindert wird. Beispielsweise muss der Download von Informationen von einer staatlichen Website anonym möglich sein; bei Apps zur Meldung von defekten Strassenlampen oder zu leerenden Abfallsammlungen muss es möglich sein, die Angabe des Standortes manuell vorzunehmen (und nicht einfach durch eine Ortung durch das Handy). Wenn solche grundrechtsschonenden Möglichkeiten nicht bestehen, werden die Grundrechte der betroffenen Personen unnötigerweise verletzt – und wenn diese Möglichkeiten nicht von Anfang an in den Systemen und Anwendungen eingebaut sind, ist es oft nicht mehr möglich oder sehr viel aufwändiger, dies nachträglich zu tun.

[51] Art. 20 der Richtlinie (EU) 2016/680.

*Abs. 2, neu:*

Das Prinzip *«Privacy by default»* verlangt, dass bei Datenbearbeitungen die Voreinstellungen datenschutzfreundlich gewählt werden. Die betroffene Person soll sich nicht durch Einstellungen kämpfen müssen, um ihr Grundrecht auf informationelle Selbstbestimmung zu schützen. Die Voreinstellungen sollen ihre Selbstbestimmung schützen und nur die Erfassung der absolut notwendigen Daten zulassen. Die betroffene Person soll selber bestimmen, wenn sie eine weiter gehende Einschränkung ihres Grundrechts zulassen will (Opt-in anstelle von Opt-out). Am Beispiel der Apps zur Meldung von defekten Strassenlampen oder zu leerenden Abfallsammlungen: In den Voreinstellungen darf der Standortdienst nicht aktiviert sein. Die Benutzerin oder der Benutzer muss diesen selber aktivieren, wenn sie oder er ihn nutzen will.

### 3.2.14 Informationspflicht bei der Beschaffung von Personendaten (§ 15 IDG)

| **Informations- und Datenschutzgesetz vom 9. Juni 2010** | **Neu** |
|---|---|
| **§ 15.** *Erkennbarkeit der Beschaffung* | **§ 15.** ~~*Erkennbarkeit der Beschaffung*~~ *Informationspflicht bei der Beschaffung* |
| [1] Die betroffene Person muss erkennen können, welche Personendaten über sie beschafft und zu welchem Zweck sie bearbeitet werden, soweit dadurch nicht die Erfüllung der gesetzlichen Aufgabe ernsthaft gefährdet wird. | ~~[1] Die betroffene Person muss erkennen können, welche Personendaten über sie beschafft und zu welchem Zweck sie bearbeitet werden, soweit dadurch nicht die Erfüllung der gesetzlichen Aufgabe ernsthaft gefährdet wird.~~ |
| [2] Werden Personendaten systematisch, namentlich mit Fragebogen oder Onlineerfassungen, erhoben, so müssen Rechtsgrundlage und Zweck der Bearbeitung angegeben sein. | ~~[2] Werden Personendaten systematisch, namentlich mit Fragebogen oder Onlineerfassungen, erhoben, so 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 dadurch nicht die Erfüllung der gesetzlichen Aufgabe ernsthaft gefährdet wird. | ~~[3] Bei der Beschaffung von besonderen Personendaten ist das öffentliche Organ verpflichtet, die betroffene Person über den Zweck der Bearbeitung zu informieren, soweit dadurch nicht die Erfüllung der gesetzlichen Aufgabe ernsthaft gefährdet wird.~~<br>[1] Das verantwortliche öffentliche Organ informiert die betroffene Person über jede Beschaffung von Personendaten. Diese Informationspflicht gilt auch, wenn die Daten bei Dritten beschafft werden.<br>[2] Die Information umfasst insbesondere Angaben über:<br>a) das verantwortliche öffentliche Organ samt Kontaktdaten,<br>b) die bearbeiteten Daten oder die Kategorien der bearbeiteten Daten,<br>c) die Rechtsgrundlage und den Zweck des Bearbeitens,<br>d) die Datenempfangenden oder die Kategorien der Datenempfangenden, falls die Daten Dritten bekannt gegeben werden, und |

| | |
|---|---|
| | e) die Rechte der betroffenen Person.<br>[3] Die Informationspflicht entfällt, wenn<br>a) die betroffene Person bereits über die Informationen nach Abs. 2 verfügt,<br>b) wenn das Bearbeiten der Personendaten gesetzlich ausdrücklich vorgesehen ist oder<br>c) die Information nicht oder nur mit unverhältnismässigem Aufwand möglich ist.<br>[4] Die Übermittlung der Informationen kann unter denselben Voraussetzungen eingeschränkt werden wie der Zugang zu den eigenen Personendaten. |

## Kommentar

*Abs. 1, geändert:*

Der neue § 15 sieht eine weiter gehende Informationspflicht der öffentlichen Organe bei der Beschaffung von Personendaten als bisher vor. Eine Beschaffung von Personendaten liegt vor, wenn ein öffentliches Organ aktiv und gewollt Kenntnis von Daten erlangt oder die Verfügung darüber begründet. Nach dem bisher geltenden Recht musste eine solche Erhebung von Personendaten für die betroffene Person erkennbar sein; wurden besondere Personendaten erhoben, musste die betroffene Person aktiv informiert werden. Die Transparenz für die betroffenen Personen muss nun[52] nach den neuen europarechtlichen Anforderungen[53] dahingehend verstärkt werden, dass die Betroffenen aktiv informiert werden müssen, auch wenn nur «gewöhnliche» Personendaten erhoben werden.

Der bisherige Abs. 1, der die Erkennbarkeit der Datenbeschaffung postuliert, entfällt dementsprechend. An seine Stelle tritt die umfassende Informationspflicht. Um Transparenz für die Betroffenen sicherzustellen, ist auch zu informieren, wenn die Daten bei Dritten, also bei anderen öffentlichen Organen oder Privaten (z.B. bei Personen, die im gleichen Haushalt leben, bei der Arbeitgeberin, bei einer Versicherung usw.) beschafft werden.

*Abs. 2, geändert:*

Der bisherige Abs. 2 entfällt, weil die Pflicht nun allgemein in Abs. 1 (neu) geregelt ist. Im Abs. 2 (neu) wird jetzt der Mindestinhalt der Information festgelegt. Die Betroffenen sind insbesondere zu informieren über:

- das verantwortliche öffentliche Organ (samt Kontaktdaten) (lit. a);
- die bearbeiteten Daten oder die Kategorien der bearbeiteten Daten (lit. b);
- die Rechtsgrundlage der Datenbearbeitung (lit. c);
- den Zweck der Datenbearbeitung (lit. c);
- die Datenempfänger oder die Kategorien der Datenempfänger (wenn die Daten weitergegeben werden) (lit. d) und
- die Rechte der betroffenen Person (lit. e).

Der Aufwand für die Umsetzung dieser Informationspflicht ist überblickbar: In den meisten Fällen, nämlich überall dort, wo Personendaten systematisch, beispielsweise auf einem Anmelde- oder

[52] Der Bund hat diese Informationspflicht, die bereits mit dem Rahmenbeschluss 2008/977/JI verbindlich war, bereits per 1. Oktober 2010 ins DSG übernommen (Art. 18*a* und für die Einschränkungen Art. 18*b* DSG, künftig Art. 19 und 20 revDSG). Im Kanton Basel-Stadt wurde damals darauf verzichtet, das erst gerade beschlossene und noch nicht in Kraft getretene IDG entsprechend zu revidieren. Vgl. dazu PK-IDG/BS, § 15 N 12 ff.

[53] Art. 13 der Richtlinie (EU) 2016/680; Art. 7[bis] der (modernisierten) Europarats-Konvention 108+.

Gesuchsformular erhoben werden, reicht es, die entsprechenden Angaben auf dem Formular anzubringen. Wo Daten durch Mitarbeitende in einem Gespräch erhoben werden, kann die Information durch die Aushändigung eines Informationsschreibens erfolgen. Zudem entfällt in verschiedenen Fällen die Informationspflicht (sogleich Abs. 3) oder kann eingeschränkt werden (Abs. 4).

*Abs. 3, geändert:*

Der bisherige Abs. 3 entfällt, weil die umfassende Pflicht nun in Abs. 1 (neu) geregelt ist. Der zweite Nebensatz enthielt eine Einschränkung; sie ist neu in den Einschränkungen in Abs. 4 (neu) enthalten.

Der neue Abs. 3 hält fest, wann die Informationspflicht entfällt. Das ist dann der Fall, wenn:
- die betroffene Person über die Information, die ihr zukommen müsste, bereits verfügt (insbesondere also, wenn sie in einer früheren Phase der Beschaffung bereits einmal informiert worden ist);
- wenn die Beschaffung oder Bekanntgabe der Personendaten gesetzlich ausdrücklich vorgesehen ist (d.h. wenn die betroffenen Personen aus den gesetzlichen Grundlagen mit hinreichender Präzision herauslesen können, welche Daten über sie zu welchem Zweck bearbeitet werden, sog. Fiktion der Gesetzeskenntnis), oder
- wenn die Information der betroffenen Person nicht oder nur mit unverhältnismässigem Aufwand möglich ist.

*Abs. 4, neu:*

In weiteren Fällen kann die Informationspflicht beim Erheben von Personendaten eingeschränkt werden. Der neue Abs. 4 hält fest, dass dies unter den gleichen Voraussetzungen der Fall ist wie beim Zugang zu den eigenen Personendaten (§ 26 IDG). Dafür ist § 29 IDG einschlägig. Er legt fest, dass das öffentliche Organ die Bekanntgabe von oder den Zugang zu Informationen im Einzelfall ganz oder teilweise zu verweigern oder aufzuschieben hat, wenn eine besondere gesetzliche Geheimhaltungspflicht oder ein überwiegendes öffentliches oder privates Interesse entgegensteht. Die bis anhin in Abs. 3 vorgesehene Einschränkung («soweit dadurch nicht die Erfüllung der gesetzlichen Aufgabe ernsthaft gefährdet wird») kann unter § 29 Abs. 2 lit. e IDG («wenn die zielkonforme Durchführung konkreter behördlicher, insbesondere polizeilicher Massnahmen beeinträchtigt») subsumiert werden.

Aus dem Grundsatz der Verhältnismässigkeit ergibt sich, dass die Einschränkung nur so lange gilt, als der Grund für die Einschränkung besteht: Sobald der Einschränkungsgrund wegfällt, ist die Information der betroffenen Person nachzuholen.

### 3.2.15 Keine Regelung über die automatisierte Einzelentscheidung

Nach der (modernisierten) Europarats-Konvention 108+ hat jede Person das Recht, nicht einer Entscheidung unterworfen zu sein, die sie erheblich beeinträchtigt und aufgrund eines ausschliesslich automatisierten Bearbeitens entstanden ist, ohne dass ihr Standpunkt berücksichtigt wird[54]. Daraus kann 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.

[54] Art. 9 Abs. 1 lit. a der (modernisierten) Europarats-Konvention 108+; vgl. ebenso Art. 11 der Richtlinie (EU) 2016/680.

Von Bedeutung ist diese Regelung v.a. im Privatrecht (zum Beispiel bei einem automatisierten Entscheid über die Kreditwürdigkeit einer Person). Im öffentlichen Recht ergehen Einzelentscheidungen mit rechtlichen Wirkungen in aller Regel in Form der Verfügung. Weil diese eröffnet werden müssen, ist die Information der betroffenen Personen sichergestellt. Da den betroffenen Personen im Vorfeld des Erlasses von Verfügungen ein Anspruch auf rechtliches Gehör zukommt, ist auch sichergestellt, dass die betroffenen Personen sich zur Einzelentscheidung äussern können. Aus diesem Grund ist davon auszugehen, dass es keine spezifische Regelung in den kantonalen (Informations- und) Datenschutzgesetzen braucht.

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, dann wird darauf zu achten sein, dass im entsprechenden Fachgesetz eine ausdrückliche und klare formell-gesetzliche Grundlage dafür geschaffen wird und dabei sichergestellt ist, dass den betroffenen Personen die Möglichkeit gegeben wird, sich zur automatisierten Einzelentscheidung und zu den bearbeiteten Daten zu äussern.

### 3.2.16 Vernichtung (§ 16 IDG)

| **Informations- und Datenschutzgesetz vom 9. Juni 2010** | **Neu** |
|---|---|
| **§ 16.** *Vernichtung*<br>[1] Nicht mehr benötigte Personendaten, die von der gemäss Archivgesetz zuständigen Stelle als nicht archivwürdig beurteilt werden, sind vom öffentlichen Organ zu vernichten. | **§ 16.** *Vernichtung*<br>[1] *unverändert*<br><br>[2] Für Informationsbestände, die Personendaten enthalten, sind Fristen für die Vernichtung beziehungsweise für die Überprüfung, ob die Daten zur Aufgabenerfüllung noch erforderlich sind, festzulegen. |

**Kommentar**

*Abs. 2, neu:*

Wie bereits oben ausgeführt,[55] muss ein stärkeres Augenmerk auf die zeitliche Befristung des Bearbeitens von Personendaten gerichtet werden. Neu wird verlangt, dass für die Vernichtung von Personendaten, bzw. für eine regelmässige Überprüfung, ob Personendaten zur Aufgabenerfüllung noch erforderlich sind, Fristen vorzusehen sind und dass durch verfahrensrechtliche Vorkehrungen sicherzustellen ist, dass diese Fristen eingehalten werden.[56] Der Grundsatz der zeitlichen Befristung soll unter den allgemeinen Voraussetzungen für das Bearbeiten von Personendaten (neuer Abs. 4 zu § 9 IDG) festgehalten werden.

Die Anbietungspflicht nach dem anwendbaren Archivrecht[57] allein dürfte nicht genügen, um den erhöhten Anforderungen an die Befristung aufgrund des internationalen Rechts zu entsprechen. Allerdings kann die in der Registratur- und Archivverordnung verankerte Frist[58] allenfalls als Auffangfrist dienen, wenn nicht bereichsspezifisch Aufbewahrungs-, Überprüfungs- oder Löschfristen verankert sind. Verlangt ist nur, aber immerhin, dass für jeden Informationsbestand bestimmt ist,

[55] Vgl. Kommentierung zum neuen § 9 Abs. 4 IDG.
[56] Art. 5 der Richtlinie (EU) 2016/680; Art. 5 Ziff. 4 lit. e der (modernisierten) Europarats-Konvention 108+.
[57] § 7 Archivgesetz (SG 153.600); §§ 21 ff. Registratur- und Archivierungsverordnung (SG 153.610).
[58] §§ 21 f. der Registratur- und Archivierungsverordnung sehen vor, dass die öffentlichen Organe Unterlagen, die sie nicht mehr benötigen, in der Regel spätestens 10 Jahre nach Abschluss der Unterlagen dem Staatsarchiv anbieten müssen. Elektronische Unterlagen müssen zum frühestmöglichen Zeitpunkt angeboten werden, vom Regierungsrat abgeschlossene Urkunden und Verträge sofort nach ihrer Ausfertigung.

wie lange die Personendaten darin aufbewahrt werden bzw. innert welcher Fristen jeweils zu prüfen ist, ob die Personendaten zur Aufgabenerfüllung noch weiter erforderlich sind oder ob sie archiviert oder vernichtet werden müssen.

Die Vorkehrungen für die Umsetzung müssen nicht auf Gesetzesstufe festgelegt werden. Sie können im Verordnungsrecht umschrieben werden. Die Umsetzung selber kann auch in einem DSMS, wie es zum Nachweis der Einhaltung der Datenschutzvorschriften dient[59], erfolgen.

### 3.2.17 Meldepflicht bei Datenschutzverletzungen (neuer § 16a IDG)

| **Informations- und Datenschutzgesetz vom 9. Juni 2010** | **Neu** |
|---|---|
| | **§16a.** *Meldung von Datenschutzverletzungen*<br>[1] Das verantwortliche öffentliche Organ meldet der oder dem Datenschutzbeauftragten ohne unangemessene Verzögerung eine Datenschutzverletzung.<br>[2] Die Auftragsdatenbearbeiterin oder der Auftragsdatenbearbeiter informiert das auftraggebende öffentliche Organ unverzüglich über eine Datenschutzverletzung.<br>[3] Eine Datenschutzverletzung liegt vor, wenn durch eine Verletzung der Informationssicherheit bearbeitete Personendaten unwiederbringlich vernichtet werden oder verloren gehen, unbeabsichtigt oder unrechtmässig verändert oder offenbart werden oder Unbefugte Zugang zu solchen Personendaten erhalten.<br>[4] Eine Meldepflicht besteht nicht, wenn die Datenschutzverletzung voraussichtlich nicht zu einem Risiko für die Grundrechte der betroffenen Person führt.<br>[5] Das öffentliche Organ informiert die betroffenen Personen, wenn die Umstände dies erfordern oder der oder die Datenschutzbeauftragte es verlangt.<br>[6] Die Benachrichtigung der betroffenen Personen kann ganz oder teilweise unterbleiben oder aufgeschoben werden, wenn eine Einschränkung gemäss § 29 zulässig ist. |

**Kommentar**

*§ 16a, neu:*

Wie zahlreiche Beispiele zeigen, werden in der digitalen Welt des 21. Jahrhunderts Datenschutzverletzungen zunehmend zu einem grösseren Problem. Wenn ein Unternehmen oder eine Verwal-

[59] Neuer Abs. 3 zu § 7 IDG (oben Ziff. 3.2.5).

tungsstelle der Pflicht zur Sicherstellung der Informationssicherheit nicht nachkommt oder die getroffenen Massnahmen durch Systemfehler, durch Unachtsamkeit der Betreiber oder durch Angreifer ausgehebelt werden, tragen potenziell die betroffenen Personen den Schaden. Eine Verletzung des Schutzes von Personendaten kann, wenn nicht rechtzeitig und angemessen reagiert wird, einen physischen, materiellen oder immateriellen Schaden für die betroffenen Personen nach sich ziehen, wie etwa Verlust der Kontrolle über ihre Personendaten oder Einschränkung ihrer Rechte, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Personendaten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die betroffene Person. Zur Verbesserung der Transparenz werden weltweit Meldepflichten bei Datenschutzverletzungen eingeführt («*Data breach notifications*») – so auch durch die neuen übergeordneten Rechtsgrundlagen.[60] Zweck ist es sicherzustellen, dass bei einer Datenschutzverletzung rechtzeitig und angemessen reagiert wird. Dafür muss eine Datenschutzverletzung (Begriffsdefinition: Abs. 3) primär der Aufsichtsbehörde, also der oder dem Datenschutzbeauftragten, gemeldet werden (Abs. 1), ausser wenn die Datenschutzverletzung voraussichtlich nicht zu einem Risiko für die Grundrechte der betroffenen Person führt (Abs. 4). Im Falle einer Auftragsdatenbearbeitung muss das auftraggebende öffentliche Organ unverzüglich informiert werden (Abs. 2). Selbstverständlich und damit hier nicht zu regeln ist es, dass eine betroffene Verwaltungsstelle auch ihre vorgesetzte Stelle und die mit der Informationssicherheit befassten Fachstellen zu informieren hat. Allenfalls müssen auch die betroffenen Personen informiert werden (Abs. 5, Ausnahmen: Abs. 6).

*Abs. 1, neu:*

Eine Datenschutzverletzung (die Begriffsdefinition erfolgt in Abs. 3) ist ohne unangemessene Verzögerung *der oder dem Datenschutzbeauftragten zu melden* (Abs. 1). Zur Meldung gehören:

- die Beschreibung der Verletzung: Was ist geschehen? Wer ist betroffen?
- Die Beschreibung der wahrscheinlichsten Folgen der Verletzung: Welches sind die Auswirkungen der Verletzung auf die staatliche Aufgabenerfüllung und vor allem auf die Grundrechte der betroffenen Personen?
- die Darstellung der Massnahmen, die zur Wiederherstellung des Schutzes bzw. zur Abmilderung der Folgen der Verletzung bereits getroffen worden sind oder getroffen werden sollen, so u.a.: Wie wird das Andauern der Verletzung verhindert? Wer wird informiert? Soll eine Strafanzeige eingereicht werden? Soll die Verletzung weiter untersucht werden (wobei zu beachten ist, dass mit Untersuchungshandlungen allenfalls Datenspuren und Beweise verwischt oder vernichtet werden können)?

Die oder der Datenschutzbeauftragte soll die Wahrnehmung der Meldepflicht dadurch erleichtern, indem sie oder er – am besten in Abstimmung mit anderen Kantonen – ein Meldeformular zur Verfügung stellt.

Aufgabe der oder des Datenschutzbeauftragten ist es primär zu prüfen, ob rechtzeitig und angemessen auf die Verletzung reagiert wird. Im Fokus steht insbesondere die Frage, welches Risiko für die Grundrechte betroffener Personen besteht und welche weiteren Kommunikationsmassnahmen zu treffen sind, beispielsweise ob die betroffenen Personen zu informieren sind (Abs. 5).

Ohne unangemessene Verzögerung bedeutet in der Regel spätestens innert 72 Stunden, nachdem dem verantwortlichen öffentlichen Organ die Verletzung bekannt geworden ist.[61]

*Abs. 2, neu:*

Im Falle einer *Auftragsdatenbearbeitung* hat die Auftragsdatenbearbeiterin oder der Auftragsdatenbearbeiter das auftraggebende öffentliche Organ *unverzüglich* zu informieren. Eine sehr rasche

[60] Art. 30 f. der Richtlinie (EU) 2016/680; Art. 7 Ziff. 2 der (modernisierten) Europarats-Konvention 108+.
[61] Art. 30 Abs. 1 der Richtlinie (EU) 2016/680.

Information ist erforderlich, da das auftraggebende öffentliche Organ, das nach § 7 Abs. 2 IDG ja verantwortlich bleibt, seinerseits seinen Melde- und Informationspflichten in der Regel innert 72 Stunden nachkommen muss. Auf diese Pflicht zur unverzüglichen Meldung an das auftraggebende öffentliche Organ – am besten mit einer einzuhaltenden Frist – ist sinnvollerweise im Vertrag, mit dem nach § 7 Abs. 1 lit. b IDG sichergestellt wird, dass eine Auftragsdatenbearbeiterin oder ein Auftragsdatenbearbeiter Daten nur so bearbeitet, wie es das auftraggebende öffentliche Organ tun dürfte, hinzuweisen.

*Abs. 3, neu:*

Abs. 3 enthält eine *Begriffsdefinition der Datenschutzverletzung*: Eine solche liegt vor, wenn die Informationssicherheit 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.

*Abs. 4, neu:*

Wenn die Datenschutzverletzung nach Abs. 3 voraussichtlich nicht zu einem Risiko für die Grundrechte der betroffenen Personen führt, dann *entfällt* die Meldepflicht (Abs. 4). Da aber die Meldung an die Datenschutzbeauftragte oder den Datenschutzbeauftragten dem Zweck dient, aus einer Aussensicht zu prüfen, welches Risiko für die Grundrechte betroffener Personen besteht, darf auf die Meldung nur verzichtet werden, wenn mit einer bestimmten Gewissheit feststeht, dass die Datenschutzverletzung voraussichtlich nicht zu einem Risiko für die Grundrechte der betroffenen Personen führt. Im Zweifelsfall ist die oder der Datenschutzbeauftragte beizuziehen.

Im Vergleich zur Prüfung, ob eine Datenschutz-Folgenabschätzung durchgeführt werden muss (neuer § 12a IDG), sind hier die Risiken für die betroffenen Personen gleichsam «konkreter» zu beurteilen. Zwar beeinflusst auch hier die Art und der Umfang der von der Datenschutzverletzung betroffenen Daten, die Umstände und der Zweck der Datenbearbeitung das Risiko für die betroffenen Personen. Bedeutsam ist aber insbesondere, ob durch die Information der betroffenen Person deren Risiko reduziert werden kann, etwa wenn sie selber Vorkehren zu ihrem Schutz treffen kann (oder muss), indem sie beispielsweise Zugangsdaten oder Passwörter ändert.

*Abs. 5, neu:*

Die *betroffenen Personen* sind zu informieren, wenn es die Umstände erfordern, beispielsweise wenn – wie soeben erwähnt – sie (oder sogar nur sie) Massnahmen ergreifen können (oder müssen), um einen physischen, materiellen oder immateriellen Schaden durch die Datenschutzverletzung abzuwenden. Die Benachrichtigung kann hingegen unterbleiben, wenn durch nachträgliche Vorkehrungen sichergestellt werden konnte, dass das Risiko für die Grundrechte der betroffenen Personen aller Wahrscheinlichkeit nach nicht mehr besteht.

Wenn das öffentliche Organ nicht selber aufgrund der Umstände zum Schluss kommt, die betroffenen Personen zu informieren (oder dies im Moment der Meldung an die Aufsichtsstelle schon getan hat), kann die oder der Datenschutzbeauftragte verlangen, dass dies getan wird – nötigenfalls in Form einer Weisung nach § 47 IDG.

*Abs. 6, neu:*

Die Benachrichtigung der betroffenen Personen kann ganz oder teilweise unterbleiben oder aufgeschoben werden, wenn eine Tatbestandsvariante von § 29 IDG erfüllt ist, wenn also eine besondere gesetzliche Geheimhaltungspflicht besteht oder öffentliche oder private Geheimhaltungsinteressen überwiegen.

### 3.2.18 Keine Datenschutzberaterinnen und Datenschutzberater

Die Richtlinie (EU) 2016/680 verlangt – in Übereinstimmung mit der Datenschutz-Grundverordnung (EU) 2016/679 – die Benennung eines Datenschutzbeauftragten[62]. Gemeint sind damit nicht die Aufsichtsorgane (die vollständig unabhängigen Datenschutzbeauftragten[63] im Sinne von § 37 IDG), sondern (wie der Bund sie nennt[64]) (betriebliche oder amtsinterne) Datenschutzberaterinnen oder -berater.

Es stellt sich die Frage, ob diese Funktion generell für alle öffentlichen Organe oder mindestens für alle Departement und die Gemeinden vorgeschrieben werden soll. Angesichts der Tatsache, dass die Dienststellen mit den umfangreichsten Datenbearbeitungen schon heute interne Ansprechpersonen bezeichnet haben, erscheint die Pflicht, für jedes öffentliche Organ oder mindestens für jedes Departement und jede Gemeinde eine Datenschutzberaterin oder einen Datenschutzberater einzusetzen, als unverhältnismässig. Deshalb wird darauf verzichtet. Hingegen ist die Pflicht mindestens im Zusammenhang mit der justiziellen und polizeilichen Zusammenarbeit umzusetzen, also für die Polizei, die Staatsanwaltschaft und die Justizvollzugsbehörde (unten Ziff. 3.2.31).

### 3.2.19 Reglement für Videoüberwachungssysteme (§ 18 IDG)

| **Informations- und Datenschutzgesetz vom 9. Juni 2010** | **Neu** |
|---|---|
| **§ 18.** *Reglement für das Videoüberwachungssystem* | **§ 18.** *Reglement für das Videoüberwachungssystem* |
| [1] Für jedes Videoüberwachungssystem muss vor seiner Inbetriebnahme ein Reglement erlassen werden, das insbesondere den Zweck des Systems, die Verantwortlichkeit und die Löschungsfrist regelt. | [1] *unverändert* |
| [2] Zuständig für den Erlass der Reglemente sind:<br>a) die Departemente bei Systemen im Verantwortungsbereich kantonaler öffentlicher Organe;<br>b) der Gemeinderat bei Systemen im Verantwortungsbereich kommunaler öffentlicher Organe;<br>c)[65)] der Gerichtsrat bei Systemen im Verantwortungsbereich von Gerichten;<br>d) die Direktion selbständiger Anstalten und Körperschaften des öffentlichen Rechts bei Systemen in ihrem Verantwortungsbereich. | [2] *unverändert* |
| [3] Das Reglement ist jeweils auf eine Dauer von maximal vier Jahren zu befristen. Vor einer allfälligen Verlängerung ist die Wirksamkeit der Videoüberwachung zu evaluieren. | [3] *unverändert* |
| [4] Vor dem Erlass und der Verlängerung eines Reglements ist das Vorhaben der oder | [4] Vor dem Erlass und der Verlängerung eines Reglements ist das Vorhaben der oder |

[62] Art. 32-34 der Richtlinie (EU) 2016/680; Art. 37-39 der Datenschutz-Grundverordnung (EU) 2016/679.
[63] Die werden im EU-Recht «unabhängige Aufsichtsbehörden» genannt.
[64] Vgl. Art. 9 E-DSG und bisher schon Art. 23 der Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz (VDSG), SR 235.11.
[65)] Fassung vom 3. Juni 2015, wirksam seit 1. Juli 2016 (KB 06.06.2015)

| | |
|---|---|
| dem Datenschutzbeauftragten zur Vorabkontrolle vorzulegen. | dem Datenschutzbeauftragten zur ~~Vorabkontrolle~~ Vorabkonsultation vorzulegen. |
| | 4bis Die Reglemente sind der Öffentlichkeit leicht zugänglich zu machen. |
| | 4ter Soweit durch die Bekanntgabe der Kamerastandorte oder anderer Einsatzdetails die Zweckerreichung verunmöglicht wird, kann auf deren Veröffentlichung verzichtet werden. |
| 5 Der Regierungsrat regelt das Nähere für die kantonale Verwaltung. Für die Gerichte, die Gemeinden und die selbständigen Anstalten und Körperschaften gilt die Regelung des Kantons sinngemäss. | 5 *unverändert* |

## Kommentar

*Abs. 4, geändert:*

Die bisherige Vorabkontrolle heisst neu Vorabkonsultation (§ 13 IDG, oben Ziff. 3.2.12). Aus diesem Grund muss die Terminologie in § 18 Abs. 4 IDG angepasst werden.

*Abs. 4$^{bis}$, neu:*

Der neue Abs. 4$^{bis}$ übernimmt die Regelung von § 6 Abs. 1 IDV.[66] Da nur die Zugänglichkeit der Reglemente es rechtfertigt, auf die Regelung der einzelnen Videoüberwachungssysteme in Gesetz oder Verordnung zu verzichten, muss die Veröffentlichungspflicht verstärkt werden. Deshalb ist die Übernahme auf Gesetzesstufe angezeigt, umso mehr, als aufgrund der Erfahrungen mit der Umsetzung der Verordnungsbestimmung die Ausnahmen von der Veröffentlichungspflicht erweitert werden sollen (neuer Abs. 4$^{ter}$). Damit wird die zum Schutz der Grundrechte notwendige Transparenz für die Bürgerinnen und Bürger eingeschränkt, was wiederum nach einer Regelung auf Gesetzesstufe verlangt.

*Abs. 4$^{ter}$, neu:*

§ 6 Abs. 2 IDV sieht, als Ausnahme von der Veröffentlichungspflicht nach § 6 Abs. 1 IDV, vor, dass auf die Veröffentlichung der Kamerastandorte verzichtet werden kann, soweit durch deren Bekanntgabe die Zweckerreichung verunmöglicht wird. In der Praxis hat sich gezeigt, dass nicht nur die Veröffentlichung der Kamerastandorte, sondern auch weiterer Einsatzdetails die Zweckerreichung vereiteln kann. Wenn etwa der Zugang zu einem zu schützenden Objekt nur von 22 bis 5 Uhr überwacht wird, kann das dazu führen, dass jemand knapp vor 22 Uhr oder just nach 5 Uhr einzudringen versucht. Aus diesem Grund soll auch auf die Veröffentlichung weiterer Einsatzdetails verzichtet werden können, wenn deren Bekanntgabe die Zweckerreichung verunmöglicht. Im Rahmen der Vorabkonsultation vor Erlass oder Verlängerung eines Videoüberwachungsreglements kann die oder der Datenschutzbeauftragte prüfen, ob eine solche Ausnahme gerechtfertigt ist.

[66] Zur Umsetzung vgl. Tätigkeitsbericht 2016 des Datenschutzbeauftragten des Kantons Basel-Stadt, S. 8 ff.

### 3.2.20 Bekanntgabe von Personendaten (§ 21 IDG)

| **Informations- und Datenschutzgesetz vom 9. Juni 2010** | **Neu** |
|---|---|
| **§ 21.** *Bekanntgabe von Personendaten* | **§ 21.** *Bekanntgabe von Personendaten* |
| [1] Das öffentliche Organ gibt Personendaten bekannt, wenn | [1] *unverändert* |
| a) eine gesetzliche Bestimmung dazu verpflichtet oder ermächtigt, oder<br>b) dies zur Erfüllung einer gesetzlichen Aufgabe erforderlich ist oder<br>c) im Einzelfall die betroffene Person ausdrücklich zugestimmt hat oder, falls sie dazu nicht in der Lage ist, die Bekanntgabe in ihrem Interesse liegt und ihre Zustimmung in guten Treuen vorausgesetzt werden darf. | |
| [2] Besondere Personendaten gibt das öffentliche Organ bekannt, wenn | [2] Besondere Personendaten <u>oder Resultate eines Profilings</u> gibt das öffentliche Organ bekannt, wenn |
| a) ein Gesetz dazu ausdrücklich verpflichtet oder ermächtigt oder | a) *unverändert* |
| b) dies zur Erfüllung einer in einem Gesetz klar umschriebenen Aufgabe zwingend notwendig ist oder | b) *unverändert* |
| c) im Einzelfall die betroffene Person ausdrücklich zugestimmt hat oder, falls sie dazu nicht in der Lage ist, die Bekanntgabe in ihrem Interesse liegt und ihre Zustimmung in guten Treuen vorausgesetzt werden darf. | c) *unverändert* |

**Kommentar**

*Abs. 2, geändert:*

Wie bei den Begriffsdefinitionen bereits ausgeführt (oben Ziff. 3.2.3 zu § 3 Abs. 7 [neu] IDG), verlangt die Richtlinie (EU) 2016/680, dass bei Vornahme eines Profilings (§ 3 Abs. 7 [neu] IDG) die gleichen Voraussetzungen erfüllt sein müssen wie beim Bearbeiten von besonderen Personendaten. Aus diesem Grund werden hier, bei den Voraussetzungen für das Bekanntgeben von besonderen Personendaten, die Resultate eines Profilings hinzugeführt. Dieselbe Ergänzung ist bei den Voraussetzungen für das Bearbeiten von besonderen Personendaten in § 9 Abs. 2 IDG (oben Ziff. 3.2.7) vorgesehen.

### 3.2.21 Bekanntgabe von Personendaten für einen nicht personenbezogenen Zweck (§ 22 IDG)

| **Informations- und Datenschutzgesetz vom 9. Juni 2010** | **Neu** |
|---|---|
| **§ 22.** *Bekanntgabe von Personendaten für einen nicht personenbezogenen Zweck* | **§ 22.** *Bekanntgabe von Personendaten für einen nicht personenbezogenen Zweck* |
| [1] Das öffentliche Organ kann anderen öffentlichen Organen im Kanton, in anderen Kantonen oder im Bund Personendaten zur Bearbeitung für einen nicht personenbezogenen Zweck, namentlich für Statistik, Planung, Wissenschaft oder Forschung, bekannt geben, sofern dies nicht durch eine besondere Geheimhaltungsbestimmung ausgeschlossen ist. | [1] Das öffentliche Organ kann anderen öffentlichen Organen im Kanton, in anderen Kantonen oder im Bund Personendaten zur Bearbeitung für einen nicht personenbezogenen Zweck, namentlich für Statistik, Planung~~,~~ ~~Wissenschaft~~ oder Forschung, bekannt geben, sofern dies nicht durch eine besondere Geheimhaltungsbestimmung ausgeschlossen ist. |
| [2] Die Empfängerin oder der Empfänger hat sich zu verpflichten:<br>a) die Personendaten zu anonymisieren oder zu pseudonymisieren, sobald es der Bearbeitungszweck zulässt, und<br>b) die Auswertungen nur so bekannt zu geben, dass keine Rückschlüsse auf betroffene Personen möglich sind. | [2] *unverändert* |
| [3] … | [3] *unverändert* |
| [4] Privaten kann das öffentliche Organ Personendaten zur Bearbeitung für Zwecke der Wissenschaft und Forschung bekannt geben, sofern dies nicht durch eine besondere Geheimhaltungsbestimmung ausgeschlossen ist und sich die Empfängerin oder der Empfänger zusätzlich zu den Anforderungen von Abs. 2 verpflichtet,<br>a) die Personendaten nicht für andere Zwecke zu bearbeiten und<br>b) die Personendaten nicht an Dritte weiterzugeben und<br>c) für die Informationssicherheit zu sorgen. | [4] Privaten kann das öffentliche Organ Personendaten zur Bearbeitung für Zwecke der ~~Wissenschaft und~~ Forschung bekannt geben, sofern dies nicht durch eine besondere Geheimhaltungsbestimmung ausgeschlossen ist und sich die Empfängerin oder der Empfänger zusätzlich zu den Anforderungen von Abs. 2 verpflichtet,<br>a) *unverändert*<br>b) *unverändert*<br>c) *unverändert* |
| [5] Unter den gleichen Voraussetzungen kann die richterliche Behörde den in einem kantonalen Anwaltsregister nach dem Anwaltsgesetz des Bundes [67)] eingetragenen Advokatinnen und Advokaten zum Zweck der Berufsausübung Urteile mit Personendaten bekannt geben. | [5] Unter den gleichen Voraussetzungen kann die richterliche Behörde den in einem kantonalen Anwaltsregister nach dem Bundesgesetz über die Freizügigkeit der Anwältinnen und Anwälte (Anwaltsgesetz, BGFA) vom 23. Juni 2000 eingetragenen Advokatinnen und Advokaten zum Zweck der Berufsausübung Urteile mit Personendaten bekannt |

[67] SR 935.61.

| | |
|---|---|
| | geben, sofern die Urteile nicht bereits in anonymisierter Form vorliegen. |

**Kommentar**

*Abs. 1, geändert:*

Hier soll – wie in § 10 Abs. 1 – der unpassende Begriff der Wissenschaft beseitigt werden. Vgl. zur Begründung oben Ziff. 3.2.8.

*Abs. 4, geändert:*

Dasselbe gilt auch für die Beseitigung des Begriffs der Wissenschaft in Abs. 4.

*Abs. 5, geändert:*

Bei der Schaffung des IDG wurde dieser Absatz eingefügt, da die Gerichte nicht über die notwendigen Ressourcen verfügten, um zahlreiche Urteile nachträglich zu anonymisieren.[68] Inzwischen veröffentlicht ein Teil der kantonalen richterlichen Behörden ihre Urteile in anonymisierter Form.[69] Aus diesem Grund ist hier zu präzisieren, dass die Bekanntgabe von unanonymisierten Urteilen durch richterliche Behörden[70] gegenüber Anwältinnen und Anwälten nur zulässig ist, wenn die Urteile nicht schon in anonymisierter Form vorliegen.

### 3.2.22 Beibehaltung des Verzeichnisses der Verfahren, bei denen Personendaten bearbeitet werden (§ 24 IDG)

Mit der Schaffung des IDG wurde auf das frühere Register der Datensammlungen verzichtet zugunsten eines Verzeichnisses der Verfahren, bei denen Personendaten bearbeitet werden. Nun sieht die Richtlinie (EU) 2016/680 eine Pflicht, ein Verzeichnis über die Datenbearbeitungstätigkeiten zu führen, nur für Justiz- und Polizeibehörden vor. Dementsprechend könnte eine solche Pflicht bereichsspezifisch umgesetzt werden (zum Beispiel im Polizeigesetz und im Einführungsgesetz zur StPO). Das bestehende und im Internet aufgeschaltete Verzeichnis[71] hat allerdings für die Bürgerinnen und Bürger eine wichtige Transparenzfunktion, damit sie ihre Rechte – insbesondere das Recht auf Zugang zu den eigenen Personendaten (§ 26 IDG) – wahrnehmen können. Aus diesem Grund soll § 24 IDG nicht aufgehoben werden.

[68] Ratschlag 08.0637.01, S. 40.
[69] Das Appellationsgericht veröffentlicht seine Urteile seit 2014 in anonymisierter Form, das Sozialversicherungsgericht seit 2018. Für eine Anonymisierung der älteren Urteile dieser beiden Gerichte sowie für die Anonymisierung der übrigen richterlichen Behörden fehlt es aber nach wie vor an den notwendigen Ressourcen.
[70] Darunter fällt auch die Staatsanwaltschaft in Bezug auf die Strafbefehle.
[71] http://www.staatskanzlei.bs.ch/oeffentlichkeitsprinzip/verfahren.html.

### 3.2.23 Zugang zu den eigenen Personendaten (§ 26 IDG)

| **Informations- und Datenschutzgesetz vom 9. Juni 2010** | **Neu** |
|---|---|
| **§ 26.** *Zugang zu den eigenen Personendaten*<br>[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. | **§ 26.** *Zugang zu den eigenen Personendaten*<br>[1] *unverändert*<br>[2] Der Zugang umfasst:<br>a) alle Personendaten zur gesuchstellenden Person;<br>b) alle verfügbaren Informationen über die Herkunft der Personendaten, wenn sie nicht bei der betroffenen Person erhoben worden sind und<br>c) die weiteren Angaben nach § 15 Abs. 2. |

**Kommentar**

*Abs. 2, neu:*

Die internationalen Rechtsgrundlagen[72] legen präziser fest, welche Informationen einer gesuchstellenden Person bei einem Gesuch um Zugang zu den eigenen Personendaten zugänglich zu machen sind. Insbesondere die verfügbaren Angaben darüber, woher die Daten stammen, sind der gesuchstellenden Person offenzulegen. Auf diesem Weg kann diese, wenn die Daten unrichtig sind, sich mit dem Berichtigungsanspruch an die Quelle der Unrichtigkeit wenden. Ausserdem sind – quasi als «Metadaten» zu den erwähnten Personendaten über die gesuchstellende Person – die Angaben mitzuliefern, über die nach der Transparenzbestimmung (neuer Abs. 2 zu § 15 IDG) die betroffene Person bei der Datenerhebung ohnehin schon zu informieren ist.

### 3.2.24 Schutz der eigenen Personendaten (§ 27 IDG)

| **Informations- und Datenschutzgesetz vom 9. Juni 2010** | **Neu** |
|---|---|
| ***§ 27.*** *Schutz der eigenen Personendaten*<br>[1] Jede betroffene Person kann vom öffentlichen Organ verlangen, dass es<br>a) unrichtige Personendaten berichtigt oder, falls die Berichtigung nicht möglich ist, vernichtet;<br>b) das widerrechtliche Bearbeiten von Personendaten unterlässt;<br>c) die Folgen des widerrechtlichen Bearbeitens von Personendaten beseitigt; | **§ 27.** *Schutz der eigenen Personendaten*<br>[1] Jede betroffene Person kann vom öffentlichen Organ verlangen, dass es kostenlos<br>a) *unverändert*<br>b) *unverändert*<br>c) die Folgen des widerrechtlichen Bearbeitens von Personendaten beseitigt, |

[72] Art. 14 der Richtlinie (EU) 2016/680 (ebenso wie Art. 15 Abs. 2 der Verordnung [EU] 2016/679); Art. 9 Abs. 1 lit. b der (modernisierten) Europarats-Konvention 108+.

| | |
|---|---|
| | insbesondere die sie betreffenden Personendaten löscht oder ihre Bekanntgabe an Dritte sperrt; |
| d) die Widerrechtlichkeit des Bearbeitens von Personendaten schriftlich feststellt. | d) *unverändert* |
| | [1bis] Das schutzwürdige Interesse der betroffenen Person wird vermutet. |
| | [1ter] Die Berichtigung, Vernichtung oder Löschung von Personendaten und die Sperrung der Bekanntgabe an Dritte ist ausserdem jenen Personen oder Stellen, denen die Daten zuvor bekannt gegeben worden sind, mitzuteilen, soweit dies nicht unmöglich oder mit unverhältnismässigem Aufwand verbunden ist. |
| [2] Der Regierungsrat regelt das Nähere. | [2] *unverändert* |

## Kommentar

*Abs. 1, Einleitungssatz, geändert:*

Zum Recht auf informationelle Selbstbestimmung (§ 11 Abs. 1 lit. j KV) gehört auch das Recht auf Zugang zu den eigenen Personendaten und auf Berichtigung unrichtiger Personendaten. Das IDG hält schon fest, dass für die Ausübung des verfassungsrechtlichen Zugangsrecht (nach § 26 IDG) keine Gebühr erhoben werden darf (§ 36 Abs. 2 IDG). Mit der Einfügung in § 27 Abs. 1 soll festgehalten werden, dass die Kostenlosigkeit auch für das verfassungsrechtliche Berichtigungsrecht gilt.

*Abs. 1 lit. c, geändert:*

Die übergeordneten Rechtsgrundlagen sehen im Zusammenhang mit den Ansprüchen nach Abs. 1, also bei widerrechtlich bearbeiteten Personendaten, auch einen Anspruch an Löschung bzw. Einschränkung der Bearbeitung vor.[73] Bei der Berichtigung ist die Vernichtung als Anspruch bereits enthalten (dann nämlich, wenn eine Berichtigung durch Änderung der Daten oder Hinzufügung von Informationen, die zur Richtigkeit führen). Löschung ist eine Form der Beseitigung der Folgen einer widerrechtlichen Datenbearbeitung; aus diesem Grund soll der Anspruch nicht generell, etwa als zusätzlicher Abs. 1[bis], eingefügt werden, sondern nur hier bei Abs. 1 lit. c. Während bei Abs. 1 lit. a die («definitive») Vernichtung verlangt werden kann, besteht hier nur ein Anspruch auf Löschung, d.h. die widerrechtlich bearbeiteten Daten müssen aus dem aktiven Bearbeitungsprozess entfernt werden (z.B. in einem IT-System durch Deaktivierung eines Datensatzes), können aber im Archivsystem erhalten bleiben, wenn dies zur Dokumentation des widerrechtlichen Bearbeitens nötig ist. Einer Löschung stehen allenfalls spezialgesetzliche Aufbewahrungsfristen entgegen. Wenn beispielsweise § 29 Abs. 2 des Gesundheitsgesetzes[74] ausdrücklich die Aufbewahrung der Behandlungsdokumentation (der «Krankengeschichte») während zehn Jahren nach Behandlungsabschluss vorschreibt, dann geht diese Regelung dem Löschungsanspruch vor. Bei anderen Aufbewahrungsregelungen ist jeweils durch Auslegung zu bestimmen, ob sie dem Löschungsanspruch vorgehen. Als Einschränkung kann aber verlangt werden, dass solche (weiter aufbewahrte) Daten nicht mehr weitergegeben werden – und zwar an jegliche Dritte, im Gegensatz zum Sperrrecht nach § 28 IDG, das nur die Bekanntgabe an Private verbietet. Zu beachten ist, dass diese beiden Ansprüche (Löschung und Einschränkung der Bearbeitung) nur der betroffenen Person zustehen.

[73] Art. 16 Abs. 2 der Richtlinie (EU) 2016/680; Art. 9 Abs. 1 lit. e der (modernisierten) Europarats-Konvention 108+.
[74] Gesundheitsgesetz vom 21. September 2011 (GesG), SG 300.100.

*Abs. 1bis, neu:*

In der Lehre ist umstritten, ob die von einer Datenbearbeitung betroffene Person bei der Geltendmachung eines der in § 27 IDG genannten Ansprüche ein schutzwürdiges Interesse nachweisen muss.[75] Ein schutzwürdiges Interesse wird nach herrschender Lehre bejaht, wenn die betroffene Person ein besonderes, unmittelbares und aktuelles Interesse vorweisen kann. Die betroffene Person ist regelmässig besonders und unmittelbar betroffen, wenn *ihre* Personendaten unrichtig sind oder unrechtmässig bearbeitet werden. Deshalb wird ihr schutzwürdiges Interesse vermutet, muss also von der betroffenen Person nicht nachgewiesen werden. Die gesetzliche Vermutung kann aber im konkreten Fall durch das öffentliche Organ, an das ein Gesuch nach § 27 IDG gerichtet wird, umgestossen werden.

*Abs. 1ter, neu:*

Die internationalen Vorgaben verlangen, dass, wenn eine Person mit ihren Ansprüchen nach Berichtigung bzw. Vernichtung und Löschung obsiegt, dies den Empfängerinnen und Empfängern der entsprechenden Daten mitgeteilt wird.[76] Diese Regelung wird in Abs. 1ter aufgenommen. Damit kann erreicht werden, dass bei den empfangenden Organen und Personen nicht unrichtige Daten oder Daten widerrechtlich weiterbearbeitet werden. Die Mitteilungspflicht steht unter dem Vorbehalt, dass sie überhaupt möglich und nicht mit unverhältnismässigem Aufwand verbunden ist.[77]

### 3.2.25 Aufsichtsrechtliche Anzeige an die Datenschutzbeauftragte oder den Datenschutzbeauftragten (neuer § 28a IDG)

| **Informations- und Datenschutzgesetz vom 9. Juni 2010** | **Neu** |
|---|---|
| | **§ 28a.** *Aufsichtsrechtliche Anzeige an die Datenschutzbeauftragte oder den Datenschutzbeauftragten*<br>[1] Jede Person hat das Recht, sich mit einer aufsichtsrechtlichen Anzeige an die Datenschutzbeauftragte oder den Datenschutzbeauftragten zu wenden, wenn sie der Ansicht ist, dass ein öffentliches Organ, eine Auftragsbearbeiterin oder ein Auftragsbearbeiter bei der Bearbeitung von sie betreffenden Personendaten gegen die datenschutzrechtlichen Vorschriften verstösst.<br>[2] Der anzeigenden Person kommt in diesem Verfahren keine Parteistellung zu.<br>[3] Die oder der Datenschutzbeauftragte informiert sie innert drei Monaten über den Stand beziehungsweise das Ergebnis der Abklärungen und die Erledigung. |

[75] Vgl. zu diesem Absatz PK-IDG/BS-Husi, § 27 N 8 ff. (mit weiteren Hinweisen).
[76] Art. 16 Abs. 6 der Richtlinie (EU) 2016/680.
[77] Diesen Vorbehalt sieht die Datenschutz-Grundverordnung ausdrücklich vor: Art. 19 der Verordnung (EU) 2016/679.

## Kommentar

*§ 28a Abs. 1, neu:*

Nach den internationalen Vorgaben[78] ist vorzusehen, dass jede betroffene Person unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs das «Recht auf Beschwerde» bei der oder dem Datenschutzbeauftragten hat, wenn sie der Ansicht ist, dass die Bearbeitung der sie betreffenden Personendaten gegen die datenschutzgesetzlichen Vorschriften verstösst. Verwaltungsrechtlich handelt es sich um eine «Aufsichtsbeschwerde» («aufsichtsrechtliche Anzeige» im Sinne von § 51 Organisationsgesetz[79]).

*§ 28a Abs. 2, neu:*

Der formlose Rechtsbehelf der aufsichtsrechtlichen Anzeige muss vom formellen verwaltungsrechtlichen (Rekurs-)Verfahren unterschieden werden. Während in einem formeller Verfahren den Involvierten (zum Beispiel Gesuchstellerin, Einsprecher usw.) Parteistellung zukommt, ist dies in einem aufsichtsrechtlichen Anzeigeverfahren nicht der Fall. Dies soll hier im neuen Abs. 2 ausdrücklich festgehalten werden (und im Abs. 3 durch eine inhaltliche Einschränkung die Information ergänzt werden).

*§ 28a Abs. 3, neu:*

Der neue Abs. 3 legt zweierlei fest:

- Erstens hat die anzeigende Person einen Anspruch, von der oder dem Datenschutzbeauftragten auf ihre Anzeige (in der Terminologie der internationalen Vorgaben: auf ihre «Beschwerde») eine Antwort zu erhalten – und zwar (spätestens) innert drei Monaten. Wenn die Abklärungen innert dieser Frist abgeschlossen werden konnten, ist über das Ergebnis zu informieren. Falls die Abklärungen nach drei Monaten noch andauern, weil beispielsweise mit dem öffentlichen Organ noch nach einer datenschutzkonformen Lösung gesucht wird, ist die anzeigende Person über den Zwischenstand zu orientieren; sobald die Abklärungen abgeschlossen sind, ist die Information der anzeigenden Person über das Ergebnis der Abklärungen nachzuholen.
- Zweitens wird – entsprechend der Nichtparteistellung der anzeigenden Person nach Abs. 2 und wie nach § 51 Abs. 2 OG – der Inhalt der Information eingeschränkt: Die anzeigende Person erhält *nur* Informationen über den Stand beziehungsweise das Ergebnis der Abklärungen und die Erledigung. Anders als eine Verfahrenspartei in Verwaltungs-, Verwaltungsrekurs- oder gerichtlichen Verfahren kommt ihr nicht ein umfassendes Akteneinsichtsrecht zu und sie erhält keinen vollständigen, begründeten Entscheid. Im Sinne einer besonderen gesetzlichen Geheimhaltungsbestimmung nach § 29 Abs. 1 IDG wird die anzeigende Person in Verfahren nach dieser neuen Bestimmung ausschliesslich über das Ergebnis der Abklärungen und die Erledigung informiert. Das soll nicht einfach in einem «Zweizeiler» erfolgen, sondern es sollen ihr so viele Informationen zukommen, dass sie die Beurteilung der oder des Datenschutzbeauftragten nachvollziehen kann. Mehr wird auch nach den internationalen Vorgaben nicht verlangt: Nach der Richtlinie (EU) 2016/680 wird «(d)ie betroffene Person (...) von der zuständigen Aufsichtsbehörde über den Stand und das Ergebnis der Beschwerde einschliesslich der Möglichkeit eines gerichtlichen Rechtsbehelfs nach Art. 53 unterrichtet»[80]; nach der (modernisierten) Europarats-Konvention 108+ «hält (die Aufsichtsbehörde die betroffene Person) über die Fortgang auf dem Laufenden»[81].

[78] Art. 52 der Richtlinie (EU) 2016/680; Art. 15 Abs. 4 der (modernisierten) Europarats-Konvention 108+.
[79] SG 153.100.
[80] Art. 52 Ab. 4 der Richtlinie (EU) 2016/680
[81] Art. 15 Abs. 4 der (modernisierten) Europarats-Konvention 108+.

Betrifft die Anzeige einen Sachverhalt, der nicht in den Aufsichtsbereich der oder des Datenschutzbeauftragten fällt, hat sie oder er sie unverzüglich an die zuständige Datenschutzbeauftragte beziehungsweise den zuständigen Datenschutzbeauftragten weiterzuleiten.

Befasst sich die oder der Datenschutzbeauftragte, an die oder den die Anzeige gerichtet wurde, trotz Zuständigkeit nicht mit ihr, besteht die Möglichkeit einer aufsichtsrechtlichen Anzeige gegen sie oder ihn. Sie ist an das Büro des Grossen Rates zu richten, dem die oder der Datenschutzbeauftragte administrativ zugeordnet ist (§ 38 Abs. 2 IDG). Entsprechend dieser Zuordnung kann das Büro natürlich der oder dem Datenschutzbeauftragten keine inhaltliche Weisung erteilen (§ 38 Abs. 1 IDG). Ein systematisches Nichtaktivwerden könnte aber vom Ratsbüro moniert werden.[82]

### 3.2.26 Aufsichtsbefugnisse der oder des Datenschutzbeauftragten (§ 38 IDG)

| **Informations- und Datenschutzgesetz vom 9. Juni 2010** | **Neu** |
|---|---|
| **§ 38.** *Stellung* | **§ 38.** *Stellung <u>und Aufsichtszuständigkeit</u>* |
| [1] Die oder der Datenschutzbeauftragte erfüllt die Aufgaben weisungsunabhängig. | [1] *unverändert* |
| [2] Die Aufsichtsstelle ist organisatorisch dem Büro des Grossen Rates zugeordnet. | [2] *unverändert* |
| [3] Der Kontrolle durch die Datenschutzbeauftragte oder den Datenschutzbeauftragten unterstehen nicht: | [3] *unverändert* |
| a) die Mitglieder des Grossen Rates und der Grosse Rat als Behörde; | a) *unverändert* |
| b) der Regierungsrat als Behörde. | b) der Regierungsrat als Behörde~~.~~<u>;</u><br><u>c) Datenbearbeitungen in hängigen Verfahren der Zivil- und Strafrechtspflege und</u><br><u>d) Datenbearbeitungen in hängigen Verfahren der Verfassungs- und Verwaltungsgerichtsbarkeit.</u> |

**Kommentar**

*Paragrafenüberschrift, geändert:*

Aufgrund der Ergänzung von Abs. 3 durch lit. c und d erhält die Einschränkung der Aufsichtsbefugnis ein höheres Gewicht. Deshalb ist es angezeigt, die Paragrafenüberschrift zu ergänzen.

*Abs. 3, neuer lit. c*

Neu soll das Informations- und Datenschutzgesetz auch für Datenbearbeitungen in hängigen Verfahren der Zivil- und Strafrechtspflege gelten (Streichung des bisher geltenden § 2 Abs. 2 lit. b IDG, oben Ziff. 3.2.2). Das Datenbearbeiten in solchen *hängigen Verfahren* soll aber nicht zusätzlich der Aufsicht der oder des Datenschutzbeauftragten unterstehen. Deshalb braucht es hier in § 38 Abs. 3 IDG neu die Ausnahme bezüglich der Aufsichtszuständigkeit der oder des Datenschutzbeauftragten (neuer lit. c). Unbenommen bleibt die Aufsichtszuständigkeit bei Datenbearbeitungen ausserhalb der hängigen Datenbearbeitungen, also etwa bei Datenbearbeitungen im Personalbereich, in der Gerichtsverwaltung, bei Vorabkonsultationen nach § 13 IDG usw.

[82] Vgl. die Ausführungen und das Beispiel in: PK-IDG/BS, § 38 N 2.

*Abs. 3, neuer lit. d*

Dasselbe gilt für die Datenbearbeitungen in hängigen Verfahren der Verfassungs- und Verwaltungsgerichtsbarkeit (Streichung des bisher geltenden § 2 Abs. 2 lit. c IDG, oben Ziff. 3.2.2, neuer lit. d in § 38 Abs. 3 IDG).

### 3.2.27 Aufgaben der oder des Datenschutzbeauftragten (§ 44 IDG)

| **Informations- und Datenschutzgesetz vom 9. Juni 2010** | **Neu** |
|---|---|
| **§ 44.** *Aufgaben* | **§ 44.** *Aufgaben* |
| 1 1 Die oder der Datenschutzbeauftragte | 1 *unverändert* |
| a) kontrolliert nach einem autonom aufzustellenden Prüfprogramm die Anwendung der Bestimmungen über den Umgang mit Informationen; | a) *unverändert* |
| b) kontrolliert vorab Bearbeitungen von Personendaten gemäss § 13; | b) ~~kontrolliert vorab Bearbeitungen von Personendaten gemäss § 13;~~ nimmt Stellung zu Rechtsetzungs- und anderen Vorhaben, die ihr oder ihm nach § 13 zur Vorabkonsultation vorzulegen sind; |
| c) berät die öffentlichen Organe in Fragen des Umgangs mit Informationen; | c) *unverändert* |
| d) berät die betroffenen Personen über ihre Rechte; | d) *unverändert* |
| e) vermittelt zwischen betroffenen Personen und öffentlichen Organen; | e) *unverändert* |
| f) nimmt Stellung zu Erlassen, die für den Umgang mit Informationen oder den Datenschutz erheblich sind. | f) ~~nimmt Stellung zu Erlassen, die für den Umgang mit Informationen oder den Datenschutz erheblich sind~~ behandelt aufsichtsrechtliche Anzeigen nach § 28a; |
| | g) sensibilisiert die öffentlichen Organe für ihre datenschutzrechtlichen Pflichten und die Öffentlichkeit für die Anliegen des Datenschutzes und der Transparenz; |
| | h) verfolgt die für den Schutz von Personendaten und das Öffentlichkeitsprinzip massgeblichen Entwicklungen. |

**Kommentar**

*lit. b, geändert:*

Die Formulierung von lit. b ist der Neuformulierung von § 13 IDG (oben Ziff. 3.2.12) anzupassen.

*lit. f, geändert:*

Bisher war die Aufgabe der oder des Datenschutzbeauftragten, zu Erlassen Stellung zu nehmen, einzig in lit. f geregelt. Neu wird die Pflicht der öffentlichen Organe, Rechtsetzungsvorhaben zur

Vorabkonsultation vorzulegen, ebenfalls in § 13 IDG statuiert. Die bisher in lit. f erwähnte Aufgabe der oder des Datenschutzbeauftragten ist neu damit bereits in lit. b mitenthalten.

Der neue § 28a IDG legt fest, dass jede Person das Recht hat, sich mit einer aufsichtsrechtlichen Anzeige an die Datenschutzbeauftragte oder den Datenschutzbeauftragten zu wenden, wenn sie der Ansicht ist, dass ein öffentliches Organ, eine Auftragsbearbeiterin oder ein Auftragsbearbeiter bei der Bearbeitung von sie betreffenden Personendaten gegen die datenschutzrechtlichen Vorschriften verstösst. In der Neufassung von § 44 wird in lit. f die Behandlung dieser aufsichtsrechtlichen Anzeigen in den Aufgabenkatalog der oder des Datenschutzbeauftragten aufgenommen.

*lit. g, neu:*

Nach den internationalen Vorgaben[83] gehört es zu den Aufgaben der oder des Datenschutzbeauftragten,
- die Öffentlichkeit für ihre oder seine Aufgaben, Befugnisse und Tätigkeiten,
- die Öffentlichkeit für die Rechte der betroffenen Personen und die Ausübung dieser Rechte und
- die für die Verarbeitung von Informationen verantwortlichen öffentlichen Organe und die Auftragsdatenbearbeiterinnen und -bearbeiter für ihre Verantwortung sensibilisieren,

Diese Aufgaben werden im neuen Buchstaben g in den Aufgabenkatalog der oder des Datenschutzbeauftragten aufgenommen, ergänzt um den ebenfalls in ihren/seinen Zuständigkeitsbereich fallenden Bereich des Öffentlichkeitsprinzips. Der Datenschutzbeauftragte des Kantons Basel-Stadt kam diesen Aufgaben mit Weiterbildungsangeboten, Schulungen und Öffentlichkeitsarbeit bisher schon nach.

*lit. h, neu:*

Nach den internationalen Vorgaben[84] gehört es auch zu den Aufgaben der oder des Datenschutzbeauftragten, massgebliche Entwicklungen zu verfolgen, soweit sie sich auf den Schutz von Personendaten auswirken, insbesondere die Entwicklung der Informations- und Kommunikationstechnologie. Diese Aufgabe wird im neuen lit. h in den Aufgabenkatalog der oder des Datenschutzbeauftragten aufgenommen, ergänzt um den ebenfalls in ihren/seinen Zuständigkeitsbereich fallenden Bereich des Öffentlichkeitsprinzips. Im Stellenbeschrieb des Datenschutzbeauftragten des Kantons Basel-Stadt war diese Aufgabe schon bisher verankert.

### 3.2.28 Kontrollbefugnisse (§ 45 IDG)

| **Informations- und Datenschutzgesetz vom 9. Juni 2010** | **Neu** |
|---|---|
| **§ 45.** *Kontrollbefugnisse*<br>[1] Die oder der Datenschutzbeauftragte kann bei öffentlichen Organen 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 | **§ 45.** *Kontrollbefugnisse*<br>[1] Die oder der Datenschutzbeauftragte kann bei öffentlichen Organen<u>, bei Auftragsdatenbearbeiterinnen und Auftragsdatenbearbeitern</u> 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 |

[83] Art. 12[bis] Ziff. 2 lit. e der (modernisierten) Europarats-Konvention 108+; Art. 46 Abs. 1 lit. b und d der Richtlinie (EU) 2016/680.
[84] Art. 46 Abs. 1 lit. j der Richtlinie (EU) 2016/680.

| | |
|---|---|
| vorführen lassen. | 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 Sachverhaltes mit. | [2] Die öffentlichen Organe ~~und die beauftragten Dritten~~, die Auftragsdatenbearbeiterinnen und Auftragsdatenbearbeiter sowie Drittpersonen, die von einem öffentlichen Organ Personendaten erhalten haben, sind verpflichtet, die Aufsichtsstelle bei der Erfüllung ihrer Aufgaben zu unterstützen. Sie wirken insbesondere an der Feststellung des Sachverhaltes mit. |
| [3] Die Berichte, welche die oder der Datenschutzbeauftragte im Rahmen der Kontrolltätigkeit erstellt, und die ihnen zugrunde liegenden Materialien sind nicht öffentlich zugänglich im Sinne von § 25 Abs. 1. [85)] | [3] *unverändert* |

**Kommentar**

*Abs. 1, geändert:*

Weil der Begriff Auftragsdatenbearbeiterin/Auftragsdatenbearbeiter neu in § 3 Abs. 8 IDG definiert wird (oben Ziff. 3.2.3), kann hier der bisher verwendete Begriff der beauftragten Drittperson ersetzt werden; der Vollständigkeit halber werden die in Abs. 1 erwähnten Drittpersonen, die von einem öffentlichen Organ Personendaten erhalten haben, auch in Abs. 2 aufgenommen.

*Abs. 2, geändert:*

Dasselbe gilt auch für Abs. 2.

### 3.2.29 Keine Sanktionsregelung

Die übergeordneten Rechtsgrundlagen sehen Sanktionen bei Verstössen gegen die Datenschutzbestimmungen vor; die Sanktionen müssten wirksam, verhältnismässig und abschreckend sein.[86] In der Datenschutz-Grundverordnung ist vorgesehen, dass die Datenschutzaufsichtsstellen sehr hohe Bussen verhängen können.[87]

Mit der vorliegenden Revision soll keine spezifische Sanktionsregelung geschaffen werden. Insbesondere soll die oder der Datenschutzbeauftragte gegenüber öffentlichen Organen, welche Datenschutzrecht verletzen, keine Bussen verhängen können. Eine Busse, die einem öffentlichen Organ kantonsintern auferlegt wird (d.h. innerhalb der gleichen Rechnung), ergibt nicht viel Sinn. Die bestehenden Sanktionsmöglichkeiten, insbesondere die Strafbestimmung für Amtsgeheimnisverletzungen[88] und für das vertragswidrige Bearbeiten von Personendaten nach § 51 Abs. 1 und 2 IDG, reichen aus.

[85] § 45 Abs. 3 beigefügt durch Abschn. II Ziff. 3 des GRB vom 13. 3. 2013 (wirksam seit 28. 4. 2013; Geschäftsnr. 12.1046).
[86] Art. 57 der Richtlinie (EU) 2016/680.
[87] Art. 83 der Richtlinie (EU) 2016/680.
[88] Art. 320 des Schweizerischen Strafgesetzbuches (StGB) vom 21. Dezember 1937, SR 311.0.

### 3.2.30 Berichterstattung (§ 50 IDG)

| **Informations- und Datenschutzgesetz vom 9. Juni 2010** | **Neu** |
|---|---|
| **§ 50.** *Berichterstattung*<br>[1] Die oder der Datenschutzbeauftragte erstattet der Wahlbehörde periodisch Bericht über Umfang und Schwerpunkte der Tätigkeiten, über wichtige Feststellungen und Beurteilungen sowie über die Wirkung des Gesetzes.<br>[2] Der Bericht wird veröffentlicht. | **§ 50.** *Berichterstattung*<br>[1] Die oder der Datenschutzbeauftragte erstattet der Wahlbehörde und der Öffentlichkeit periodisch und bei Bedarf Bericht über Umfang und Schwerpunkte der Tätigkeiten, über wichtige Feststellungen und Beurteilungen sowie über die Wirkung des Gesetzes.<br>~~[2] Der Bericht wird veröffentlicht.~~ |

**Kommentar**

*Abs. 1, geändert:*

Die Information der Wahlbehörde (des Grossen Rates), der anderen Behörden und der Öffentlichkeit gehört einerseits zu Rechenschaftsablage, andererseits zur Sensibilisierungsaufgabe der oder des Datenschutzbeauftragten (neuer lit. h von § 44 IDG). Das geschieht – schon bisher – nicht nur durch die Zustellung und Veröffentlichung des jährlichen Tätigkeitsberichts, sondern bei Bedarf in anderer Form (z.B. durch Medienmitteilungen, Veröffentlichung auf der Website) auch zwischendurch. Dies soll in § 50 Abs. 1 IDG klargestellt werden.

*Abs. 2, aufgehoben:*

Mit der Änderung des ersten Absatzes kann Abs. 2 von § 50 IDG aufgehoben werden.

### 3.2.31 Vertragswidriges Bearbeiten von Personendaten (§ 51 IDG)

| **Informations- und Datenschutzgesetz vom 9. Juni 2010** | **Neu** |
|---|---|
| **§ 51.** *Vertragswidriges Bearbeiten von Personendaten* | **§ 51.** *Vertragswidriges Bearbeiten von Personendaten* |
| [1] Wer als beauftragte Drittperson gemäss § 7 ohne ausdrückliche Ermächtigung des auftraggebenden öffentlichen Organs vorsätzlich oder fahrlässig Personendaten für sich oder andere verwendet oder anderen bekannt gibt, wird mit Busse bestraft. | [1] Mit Busse bestraft wird, wer<br>a) als Auftragsdatenbearbeiterin oder Auftragsdatenbearbeiter gemäss § 7 ohne ausdrückliche Ermächtigung des auftraggebenden öffentlichen Organs vorsätzlich oder fahrlässig Personendaten für sich oder andere verwendet oder anderen bekannt gibt oder<br>b) als Auftragsdatenbearbeiterin oder Auftragsdatenbearbeiter gemäss § 7 ohne vorgängige schriftliche Einwilligung des auftraggebenden öffentlichen Organs die Datenbearbeitung einer weiteren Auftragsdatenbearbeiterin und einem weiteren Auftragsdatenbearbeiter überträgt. |
| [2] Wer Personendaten, die sie oder er von einem öffentlichen Organ zum Bearbeiten zu nicht personenbezogenen Zwecken erhalten hat, vorsätzlich oder fahrlässig entgegen der Verpflichtung gemäss § 22 Abs. 4 für andere Zwecke bearbeitet oder an Dritte weitergibt, wird mit Busse bestraft. | [2] *unverändert* |

**Kommentar**

*Abs. 1, geändert:*

Der Straftatbestand des bisherigen Abs. 1 bleibt inhaltlich unverändert (Abs. 1 neuer lit. a). Weil der Begriff Auftragsdatenbearbeiterin oder Auftragsdatenbearbeiter neu in § 3 Abs. 8 IDG definiert wird (oben Ziff. 3.2.3), kann hier der bisher verwendete Begriff der beauftragten Drittperson ersetzt werden.

Neu kommt aber die Strafdrohung für ein nicht durch die Einwilligung des auftraggebenden öffentlichen Organs gerechtfertigtes Subcontracting (neuer Abs. 3 zu § 7 IDG, oben Ziff. 3.2.5) hinzu.

### 3.2.32 Änderung und Aufhebung bisherigen Rechts (§§ 52 und 53 IDG)

### 3.2.32.1 Änderung des Gesetzes über die Organisation der Gerichte und der Staatsanwaltschaft (Gerichtsorganisationsgesetz, GOG) vom 3. Juni 2015[89]

| Gesetz über die Organisation der Gerichte und der Staatsanwaltschaft (Gerichtsorganisationsgesetz, GOG) vom 3. Juni 2015 | Neu |
|---|---|
| | ***7.5 Datenschutzberatung***<br>**§ 98a.**<br>[1] Die Staatsanwaltschaft bezeichnet eine Datenschutzberaterin oder einen Datenschutzberater für die Staats- und Jugendanwaltschaft.<br>[2] Diese Person hat die folgenden Aufgaben:<br>1. Sie berät und unterstützt bei der Bearbeitung von Personendaten.<br>2. Sie nimmt Datenschutz-Folgenabschätzungen gemäss § 12a Abs. 1 des Gesetzes über die Information und den Datenschutz (Informations- und Datenschutzgesetz, IDG) vom 9. Juni 2010 vor.<br>3. Sie arbeitet mit der oder dem Datenschutzbeauftragten zusammen. |

**Kommentar**

*§ 98a, neu:*

Die Richtlinie (EU) 2016/680 verlangt – in Übereinstimmung mit der Datenschutz-Grundverordnung (EU) 2016/679 – die Benennung eines Datenschutzbeauftragten[90]. Gemeint sind damit nicht die Aufsichtsorgane (die vollständig unabhängigen Datenschutzbeauftragten[91] im Sinne von § 37 IDG), sondern (wie der Bund sie nennt[92]) (betriebliche oder amtsinterne) Datenschutzberaterinnen oder -berater.

Weil darauf verzichtet wird, jedes öffentliche Organ oder mindestens jedes Departement und jede Gemeinde zur Einsetzung einer Datenschutzberaterin oder eines Datenschutzberaters zu verpflichten (oben Ziff. 3.2.18), muss diese Pflicht aber im Zusammenhang mit der justiziellen und polizeilichen Zusammenarbeit, also mindestens für die Polizei (unten Ziff. 3.2.32.4), die Staatsanwaltschaft und den Justizvollzug (unten Ziff. 3.2.32.3) eingeführt werden.

*Abs. 1, neu:*

Der neue Abs. 1 verpflichtet die Staatsanwaltschaft zur Benennung einer Datenschutzberaterin oder eines Datenschutzberaters.

89 SG 154.100.
90 Art. 32-34 der Richtlinie (EU) 2016/680; Art. 37-39 der Datenschutz-Grundverordnung (EU) 2016/679.
91 Die werden im EU-Recht «unabhängige Aufsichtsbehörden» genannt.
92 Vgl. Art. 9 E-DSG und bisher schon Art. 23 der Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz (VDSG), SR 235.11.

*Abs. 2, neu:*

Der neue Abs. 2 umschreibt die Aufgaben der Datenschutzberaterin oder des Datenschutzberaters: die Beratung der Staatsanwaltschaft und der betroffenen Personen, die sich an die Staatsanwaltschaft wenden, die Vornahme von Datenschutz-Folgenabschätzungen nach § 12a (neu) IDG und die Zusammenarbeit mit der oder dem Datenschutzbeauftragten.

### 3.2.32.2 Änderung des Geoinformationsgesetzes (KGeoIG) vom 16. November 2011[93]

| **Geoinformationsgesetz vom 16. November 2011** | **Neu** |
|---|---|
| **§ 12.** *Elektronischer Zugriff* | **§ 12.** *Elektronischer Zugriff* |
| [1] Bevor der Regierungsrat die Geodaten gemäss § 3 lit. a mittels direktem elektronischen Zugriff als öffentlich zugänglich erklärt, prüft er die daraus entstehenden möglichen Auswirkungen auf die betroffenen Personen. | [1] *unverändert* |
| [2] Bevor die Gemeinde die Geodaten gemäss § 3 lit. b mittels direktem elektronischen Zugriff als öffentlich zugänglich erklärt, prüft sie die daraus entstehenden möglichen Auswirkungen auf die betroffenen Personen. | [2] *unverändert* |
| [3] Werden die Geodaten gemäss § 3 mit Downloaddienst zugänglich gemacht, ist eine Vorabkontrolle durch die Beauftragte oder den Beauftragten für den Datenschutz gemäss § 13 des Informations- und Datenschutzgesetzes vom 9. Juni 2010 erforderlich. | [3] Werden die Geodaten gemäss § 3 mit Downloaddienst zugänglich gemacht, ist ~~eine Vorabkontrolle durch~~ vorab die oder der Datenschutzbeauftragte ~~die Beauftragte oder den Beauftragten für den Datenschutz~~ gemäss § 13 des Informations- und Datenschutzgesetzes (Informations- und Datenschutzgesetz, IDG) vom 9. Juni 2010 ~~erforderlich~~ zu konsultieren. |

**Kommentar**

*Abs. 3, geändert:*

Begriffliche Anpassung an den neuen Begriff gemäss § 13 IDG und an die korrekte Bezeichnung des Aufsichtsorgans gemäss § 37 IDG.

[93] SG 214.300.

### 3.2.32.3 Änderung des Gesetzes über den Justizvollzug (Justizvollzugsgesetz, JVG) vom 13. November 2019[94]

| Gesetz über den Justizvollzug (Justizvollzugsgesetz, JVG) vom 13. November 2019 | Neu |
|---|---|
| | **§ 28a.** *Datenschutzberatung*<br>[1] Die Vollzugsbehörde bezeichnet eine Datenschutzberaterin oder einen Datenschutzberater.<br>[2] Diese Person hat die folgenden Aufgaben:<br>a) Sie berät und unterstützt bei der Bearbeitung von Personendaten;<br>b) sie nimmt Datenschutz-Folgenabschätzungen gemäss § 12a Abs. 1 des Gesetzes über die Information und den Datenschutz (Informations- und Datenschutzgesetz, IDG) vom 9. Juni 2010 vor;<br>c) sie arbeitet mit der oder dem Datenschutzbeauftragten zusammen. |

**Kommentar**

*§ 28a, neu:*

Siehe die Ausführungen zur Änderung des Gesetzes über die Organisation der Gerichte und der Staatsanwaltschaft (Gerichtsorganisationsgesetz, GOG) vom 3. Juni 2015; oben Ziff. 3.2.32.1.

### 3.2.32.4 Änderung des Gesetzes betreffend die Kantonspolizei des Kantons Basel-Stadt (Polizeigesetz, PolG) vom 13. November 1996[95]

| Gesetz betreffend die Kantonspolizei des Kantons Basel-Stadt vom 13. November 1996 | Neu |
|---|---|
| **§ 57.** *Grundsatz*<br>[1] Für Akten der Kantonspolizei gelten die Bestimmungen über das Amtsgeheimnis, den Datenschutz und die Akteneinsicht.<br>[2] Die Bearbeitung und Weitergabe von Personendaten durch die Kantonspolizei sowie das Einsichtsrecht in polizeiliche Datensammlungen richten sich nach den Bestimmungen der Datenschutzgesetzgebung und im interkantonalen sowie internationalen | **§ 57.** *Grundsatz*<br>[1] *unverändert*<br>[2] *unverändert* |

[94] SG 258.200.
[95] SG 510.100.

| | |
|---|---|
| Verkehr nach den Bestimmungen der Bundesgesetzgebung sowie der internationalen Rechtshilfeabkommen. | |
| [3] Polizeilich relevante Informationen dürfen weitergegeben werden, sofern diese der Gefahrenabwehr oder dem Schutz der Polizeigüter dient. | [3] *unverändert* |
| [4] Die Kantonspolizei führt die zur recht- und zweckmässigen Erfüllung ihrer Aufgaben notwendigen Datensammlungen. | [4] *unverändert* |
| | [5] Die Kantonspolizei darf besondere Personendaten bearbeiten sowie Profiling vornehmen, soweit es zur Erfüllung ihrer gesetzlichen Aufgaben zwingend notwendig ist. |

**Kommentar**

*Abs. 5, neu:*

Das Profiling (§ 3 Abs. 7 [neu] IDG, oben Ziff. 3.2.3) bedarf neu einer formellgesetzlichen Grundlage wie das Bearbeiten besonderer Personendaten (§ 9 Abs. 2 IDG), oben Ziff. 3.2.7). Da die Kantonspolizei bereits heute Profiling betreibt, muss im Polizeigesetz die entsprechende formellgesetzliche Grundlage geschaffen werden. Dabei wird ihr nicht einfach jedes automatisierte Bearbeiten erlaubt, sondern nur dasjenige, das zur Erfüllung ihrer gesetzlichen Aufgaben, die sich aus dem Polizeigesetz, der Strafprozessordnung oder anderer Gesetze ergeben, zwingend notwendig ist.

| **Gesetz betreffend die Kantonspolizei des Kantons Basel-Stadt vom 13. November 1996** | **Neu** |
|---|---|
| | **§ 57a.** *Datenschutzberatung*<br>[1] Die Kantonspolizei bezeichnet eine Datenschutzberaterin oder einen Datenschutzberater.<br>[2] Diese Person hat die folgenden Aufgaben:<br>a) Sie berät und unterstützt bei der Bearbeitung von Personendaten;<br>b) sie nimmt Datenschutz-Folgenabschätzungen gemäss § 12a Abs. 1 des Gesetzes über die Information und den Datenschutz (Informations- und Datenschutzgesetz, IDG) vom 9. Juni 2010 vor;<br>c) sie arbeitet mit der oder dem Datenschutzbeauftragten zusammen. |

**Kommentar**

*§* 57a*, neu:*

Siehe die Ausführungen zur Änderung des Gesetzes über die Organisation der Gerichte und der Staatsanwaltschaft (Gerichtsorganisationsgesetz, GOG) vom 3. Juni 2015; oben Ziff. 3.2.32.5.

### 3.2.32.5 Änderung des Finanz- und Verwaltungskontrollgesetzes (FVKG) vom 17. September 2003[96]

| Finanz- und Verwaltungskontrollgesetz vom 17. September 2003 | Neu |
|---|---|
| **§ 22.** *Dokumentation und Datenzugriff* | **§ 22.** *Dokumentation und Datenzugriff* |
| [1] Beschlüsse und Verfügungen des Grossen Rats, der Regierung, der Gerichte, der Departemente und der Dienststellen sowie der selbständigen öffentlich-rechtlichen und privatrechtlichen Anstalten, die den Finanzhaushalt des Kantons betreffen, sind der Finanzkontrolle zugänglich zu machen. | [1] *unverändert* |
| [2] Die Finanzkontrolle hat das Recht, die für die Wahrnehmung der Finanzaufsicht erforderlichen Personendaten aus den Datensammlungen der Departemente und Dienststellen, der Gerichte sowie der selbständigen öffentlich-rechtlichen und privatrechtlichen Anstalten abzurufen. Soweit die Daten für die Aufgabenerfüllung geeignet und erforderlich sind, erstreckt sich das Zugriffsrecht auch auf besonders schützenswerte Personendaten. Die Finanzkontrolle unterliegt dabei der gleichen Geheimhaltungspflicht wie die geprüfte Stelle. Die Finanzkontrolle darf die ihr derart zur Kenntnis gebrachten Personendaten nur bis zum Abschluss des Revisionsverfahrens aufbewahren oder speichern. Die Zugriffe auf die verschiedenen Datensammlungen und die damit verfolgten Zwecke müssen dokumentiert sein. | [2] Die Finanzkontrolle hat das Recht, die für die Wahrnehmung der Finanzaufsicht erforderlichen Personendaten aus den Datensammlungen der Departemente und Dienststellen, der Gerichte sowie der selbständigen öffentlich-rechtlichen und privatrechtlichen Anstalten abzurufen. Soweit die Daten für die Aufgabenerfüllung geeignet und erforderlich sind, erstreckt sich das Zugriffsrecht auch auf ~~besonders schützenswerte~~ besondere Personendaten. Die Finanzkontrolle unterliegt dabei der gleichen Geheimhaltungspflicht wie die geprüfte Stelle. Die Finanzkontrolle darf die ihr derart zur Kenntnis gebrachten Personendaten nur bis zum Abschluss des Revisionsverfahrens aufbewahren oder speichern. Die Zugriffe auf die verschiedenen Datensammlungen und die damit verfolgten Zwecke müssen dokumentiert sein. |

**Kommentar**

*Abs. 2, geändert:*

Anpassung an die seit 2012 geltende Begrifflichkeit (§ 3 Abs. 4 IDG). Eine Ergänzung in dem Sinne, dass auch das Profiling (neuer § 3 Abs. 7 IDG) erlaubt werden soll, ist nicht notwendig, da im Zusammenhang mit der Finanz- und Verwaltungskontrolle kein Profiling zur Aufgabenerfüllung erforderlich ist.

[96] SG 610.200.

### 3.2.32.6 Änderung des Gesetzes über die direkten Steuern (Steuergesetz) vom 12. April 2000[97]

| Gesetz über die direkten Steuern vom 12. April 2000 | Neu |
|---|---|
| **§ 141a.** | **§ 141a.** |
| [1] Die Steuerverwaltung betreibt zur Erfüllung ihrer Aufgaben ein Informationssystem. Dieses kann auch besonders schützenswerte Personendaten über administrative und strafrechtliche Sanktionen enthalten, die steuerrechtlich wesentlich sind. | [1] Die Steuerverwaltung betreibt zur Erfüllung ihrer Aufgaben ein Informationssystem. Dieses kann auch ~~besonders schützenswerte~~ besondere Personendaten über administrative und strafrechtliche Sanktionen enthalten, die steuerrechtlich wesentlich sind. |
| [1bis] ... | [1bis] *unverändert* |
| [2] ... | [2] *unverändert* |
| [3] ... | [3] *unverändert* |
| [4] ... | [4] *unverändert* |

**Kommentar**

*Abs. 1, geändert:*

Anpassung an die seit 2012 geltende Begrifflichkeit (§ 3 Abs. 4 IDG). Eine Ergänzung in dem Sinne, dass auch das Profiling (neuer § 3 Abs. 7 IDG) erlaubt werden soll, ist nicht notwendig, da im Zusammenhang mit der Erhebung der Steuern kein Profiling zur Aufgabenerfüllung erforderlich ist.

### 3.2.32.7 Änderung des Gesetzes über die Industriellen Werke Basel (IWB-Gesetz) vom 11. Februar 2009[98]

| Gesetz über die Industriellen Werke Basel vom 11. Februar 2009 | Neu |
|---|---|
| **§ 35a** | **§ 35a** |
| [1] Die IWB sind berechtigt, mit Hilfe intelligenter, fernauslesbarer Messeinrichtungen (Smart Meter) Personendaten ohne Einwilligung der betroffenen Personen zu bearbeiten, soweit dies erforderlich ist für<br>a) die Lieferung von Energie und Wasser (insbesondere für die Erstellung von Verbrauchsprognosen, Bilanzgruppenmeldungen, Leistungsnominationen, die Energiebeschaffung und das Portfoliomanagement);<br>b) die Messung des Energie- und Wasserverbrauchs, der Energieproduktion und der Einspeisemenge; | [1] *unverändert* |

[97] SG 640.100.
[98] SG 772.300.

| | |
|---|---|
| c) die Abrechnung des Energie- und Wasserverbrauchs und die Vergütung von Einspeisemengen;<br>d) die Ermittlung des Netzzustandes und die Sicherstellung sicherer, effizienter und leistungsstarker Netze;<br>e) das Auffinden und Unterbinden von Leistungserschleichungen. | |
| [2] Die IWB sind zudem berechtigt, mit Einwilligung der betroffenen Personen Personendaten zum Zwecke der Entwicklung und Bereitstellung von Energiedienstleistungen zu bearbeiten. | [2] *unverändert* |
| [3] Die Einzelheiten der Datenbearbeitung gemäss Abs. 1 und 2 werden in vom Verwaltungsrat zu erlassenden und vom Regierungsrat zu genehmigenden Ausführungsbestimmungen für jedes Medium (Elektrizität, Erdgas, Fernwärme und Wasser) separat geregelt. Diese Ausführungsbestimmungen zur Datenbearbeitung sind der oder dem kantonalen Datenschutzbeauftragten im Rahmen eines Vorabkontrollverfahrens vorzulegen. | [3] Die Einzelheiten der Datenbearbeitung gemäss Abs. 1 und 2 werden in vom Verwaltungsrat zu erlassenden und vom Regierungsrat zu genehmigenden Ausführungsbestimmungen für jedes Medium (Elektrizität, Erdgas, Fernwärme und Wasser) separat geregelt. Diese Ausführungsbestimmungen zur Datenbearbeitung sind der oder dem kantonalen Datenschutzbeauftragten im Rahmen ~~eines Vorabkontrollverfahrens~~ einer Vorabkonsultation vorzulegen. |
| [4] … | [4] *unverändert* |
| [5] … | [5] *unverändert* |

**Kommentar**

*Abs. 3, geändert*

Die bisherige Vorabkontrolle wird durch die Vorabkonsultation abgelöst (§ 13 IDG, vgl. oben Ziff. 3.2.12). Entsprechend ist die Terminologie in § 35a Abs. 3 des IWB-Gesetzes anzupassen.

### 3.2.32.8 Änderung des Gesetzes betreffend die Tagesbetreuung von Kindern (Tagesbetreuungsgesetz) vom 17. September 2003[99]

| **Gesetz betreffend die Tagesbetreuung von Kindern vom 17. September 2003** | **Neu** |
|---|---|
| **§ 15.** *Datenbearbeitung*<br>[1] Für die Bearbeitung der Daten, einschliesslich besonders schützenswerter Personendaten, ist das Gesetz über die Harmonisierung und Koordination von bedarfsabhängigen Sozialleistungen im Kanton Basel-Stadt vom 25. Juni 2008 (Harmonisierungsgesetz Sozialleistungen) massgebend. | **§ 15.** *Datenbearbeitung*<br>[1] Für die Bearbeitung der Daten, einschliesslich ~~besonders schützenswerter~~ besonderer Personendaten, ist das Gesetz über die Harmonisierung und Koordination von bedarfsabhängigen Sozialleistungen im Kanton Basel-Stadt (Harmonisierungsgesetz Sozialleistungen, SoHaG) vom 25. Juni 2008 massgebend. |

[99] SG 815.100.

## Kommentar

*Abs. 1, geändert:*

Anpassung an die seit 2012 geltende Begrifflichkeit (§ 3 Abs. 4 IDG). Eine Ergänzung in dem Sinne, dass auch das Profiling (neuer § 3 Abs. 7 IDG) erlaubt werden soll, ist nicht notwendig, da im Zusammenhang mit der Tagesbetreuung kein Profiling zur Aufgabenerfüllung erforderlich ist.

### 3.2.32.9 Änderung des Gesetzes über die Harmonisierung und Koordination von bedarfsabhängigen Sozialleistungen (Harmonisierungsgesetz Sozialleistungen, SoHaG) vom 25. Juni 2008[100]

| **Gesetz über die Harmonisierung und Koordination von bedarfsabhängigen Sozialleistungen (Harmonisierungsgesetz Sozialleistungen, SoHaG) vom 25. Juni 2008** | **Neu** |
|---|---|
| **§ 25.** *Bekanntgabe von Daten aus der zentralen Datenbank für statistische und weitere nicht personenbezogene Zwecke* | **§ 25.** *Bekanntgabe von Daten aus der zentralen Datenbank für statistische und weitere nicht personenbezogene Zwecke* |
| [1] Die Bekanntgabe von Daten an die zentrale Statistikstelle des Kantons richtet sich nach den Bestimmungen des Gesetzes über die öffentliche Statistik (StatG) vom 21. Mai 2014. | [1] *unverändert* |
| [2] Die Bekanntgabe von Daten für einen nicht personenbezogenen Zweck, namentlich für Planung, Wissenschaft und Forschung, an andere öffentliche Organe im Kanton sowie an öffentliche Organe in anderen Kantonen oder des Bundes richtet sich nach § 22 IDG. | [2] Die Bekanntgabe von Daten für einen nicht personenbezogenen Zweck, namentlich für Planung~~, Wissenschaft~~ und Forschung, an andere öffentliche Organe im Kanton sowie an öffentliche Organe in anderen Kantonen oder des Bundes richtet sich nach § 22 IDG. |
| [3] Die Bekanntgabe von Daten an Private kann zum Zweck der Wissenschaft und Forschung ausschliesslich in anonymisierter Form erfolgen. | [3] Die Bekanntgabe von Daten an Private kann zum Zweck der ~~Wissenschaft und~~ Forschung ausschliesslich in anonymisierter Form erfolgen. |
| [4] Anfragen für die Bekanntgabe von Daten sind an das für die zentrale Datenbank zuständige Organ gemäss § 13 dieses Gesetzes zu richten. | [4] *unverändert* |

## Kommentar

*Abs. 2, geändert:*

Hier soll der unpassende Begriff der Wissenschaft aufgrund der Streichung in § 10 Abs. 1 IDG beseitigt werden. Vgl. zur Begründung oben Ziff. 3.2.9.

*Abs. 3, geändert:*

Dasselbe gilt auch für die Streichung des Begriffs der Wissenschaft in Abs. 3.

[100] SG 890.700.

## 4. Finanzielle Auswirkungen

Die beantragten Änderungen haben nur geringe finanzielle Auswirkungen, die mit den bestehenden Ressourcen bewältigt werden können. Die Pflicht, bei neuen Projekten eine Datenschutz-Folgenabschätzung durchzuführen (neuer § 12a IDG), verursacht keinen zusätzlichen Aufwand, weil diese Beurteilung auch bisher schon als Vorbereitung für die Vorabkontrolle (neu: Vorabkonsultation, § 13 IDG) vorgenommen werden musste. Die Prinzipien des Datenschutzes durch Technik («Privacy by design», neuer § 14 Abs. 1 IDG) und durch datenschutzfreundliche Voreinstellungen («Privacy by default», neuer § 14 Abs. 2 IDG) sind im Rahmen von Projekten zu beachten und führen unter Umständen sogar zu geringerem Aufwand, weil datenschutzrechtliche Erfordernisse von Anfang an zu berücksichtigen sind und nicht nachträglich mit grösserem Aufwand implementiert werden müssen. Die Informationspflicht bei der Beschaffung von Personendaten (neuer § 15 IDG) führt bei der Formulierung der Hinweise (in Informationsbroschüren, auf Formularen und Webseiten) zu einem gewissen Anfangsaufwand. Selbst die Meldepflicht bei Datenschutzverletzungen dürfte kaum zu einem neuen Mehraufwand führen: Schon bisher waren aufgrund der Grundsatzes von Treu und Glauben die von einer Datenschutzverletzung betroffenen Personen zu informieren, und die Meldung an die oder den Datenschutzbeauftragten verursacht keinen relevanten Aufwand. Ein gewisser Initialaufwand dürfte aufgrund der Anpassung gewisser interner Prozesse mit Bezug zum Datenschutz entstehen sowie aufgrund allenfalls notwendiger Schulungen des Personals, etwa bei der Umsetzung der erweiterten Pflicht zur Information der betroffenen Person.

Auch bei der oder dem Datenschutzbeauftragten hält sich der Mehraufwand aufgrund der Gesetzesrevision in Grenzen.

Schliesslich bleibt die Benennung von Datenschutzberaterinnen und Berater bei der Staatsanwaltschaft, der Polizei und beim Amt für Justizvollzug. Hier geht es aber nicht um neue Stellen, sondern nur um die Zuordnung von Aufgaben, die ohnehin bestehen, zu einer bestimmten Person.

## 5. Formelle Prüfungen und Regulierungsfolgenabschätzung

Das Finanzdepartement hat den vorliegenden Gesetzesentwurf gemäss § 8 des Gesetzes über den kantonalen Finanzhaushalt (Finanzhaushaltgesetz) vom 14. März 2012 auf die finanzielle und wirtschaftliche Tragweite und das Justiz- und Sicherheitsdepartement auf die Aufnahme in die Gesetzessammlung geprüft.

Der Vortest zur Klärung der Betroffenheit von Unternehmen hat ergeben, dass kein Bedarf für eine Regulierungsfolgeabschätzung besteht.

## 6. Antrag

Gestützt auf unsere Ausführungen beantragen wir dem Grossen Rat die Annahme des beiliegenden Beschlussentwurfes.

Im Namen des Regierungsrates des Kantons Basel-Stadt

| | |
|---|---|
| Beat Jans<br>Präsident | Barbara Schüpbach-Guggenbühl<br>Staatsschreiberin |

**Beilagen**
- Entwurf Grossratsbeschluss
- Synopse

# Gesetz über die Information und den Datenschutz (Informations- und Datenschutzgesetz, IDG)

Änderung vom [Datum]

---

*Der Grosse Rat des Kantons Basel-Stadt,*

nach Einsichtnahme in den Ratschlag des Regierungsrates Nr. [Nr. eingeben] vom [Datum eingeben] sowie in den Bericht der Justiz-, Sicherheits- und Sportkommission Nr. [Nr. eingeben] vom [Datum eingeben],

*beschliesst:*

I.
Gesetz über die Information und den Datenschutz (Informations- und Datenschutzgesetz, IDG) vom 9. Juni 2010 [1)] (Stand 4. Januar 2018) wird wie folgt geändert:

**§ 1 Abs. 2 (geändert)**

[2] Es bezweckt:

b) **(geändert)** die Grundrechte von natürlichen Personen zu schützen, über welche die öffentlichen Organe Personendaten bearbeiten.

**§ 2 Abs. 2 (geändert), Abs. 2[bis] (neu)**

[2] Es findet keine Anwendung, soweit ein öffentliches Organ am wirtschaftlichen Wettbewerb teilnimmt und dabei privatrechtlich handelt. Für das Bearbeiten von Personendaten ist das Bundesgesetz über den Datenschutz (DSG) vom 19. Juni 1992 sinngemäss anwendbar.

a) *Aufgehoben.*
b) *Aufgehoben.*
c) *Aufgehoben.*

[2bis] In hängigen Verfahren der Zivil- und Strafrechtspflege sowie der Verfassungs- und Verwaltungsgerichtsbarkeit richten sich die Rechte und Ansprüche der betroffenen Person, die Informationspflicht des öffentlichen Organs bei der Beschaffung von Personendaten, die Bekanntgabe von Personendaten an Verfahrensbeteiligte, die Information der Öffentlichkeit und der allgemeine Informationszugangsanspruch der Öffentlichkeit ausschliesslich nach dem anwendbaren Verfahrensrecht.

**§ 3 Abs. 3 (geändert), Abs. 4, Abs. 5 (geändert), Abs. 7 (neu), Abs. 8 (neu)**

[3] Personendaten sind Informationen, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen.

[4] Besondere Personendaten sind:

a) **(geändert)** Personendaten, bei deren Bearbeitung eine besondere Gefahr der Grundrechtsverletzung besteht (sensitive Personendaten), insbesondere:
   1. **(geändert)** Angaben über die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten;
   2. **(geändert)** Angaben über die Gesundheit, das Erbgut (genetische Daten), die persönliche Geheimsphäre, das Sexualleben, die sexuelle Orientierung oder die ethnische Herkunft;
   3. **(geändert)** Angaben über Massnahmen der sozialen Hilfe;
   4. **(geändert)** Angaben über administrative oder strafrechtliche Verfolgungen und Sanktionen und

---

[1)] SG 153.260

5. **(neu)** 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).

[5] Bearbeiten ist jeder Umgang mit Informationen, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten sowie das Durchführen logischer oder rechnerischer Operationen mit diesen Informationen.

[7] Profiling ist jede Auswertung von Informationen, um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen, insbesondere bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Geheimsphäre oder Mobilität, vorherzusagen.

[8] Auftragsdatenbearbeiterin oder Auftragsdatenbearbeiter ist die private Person oder das öffentliche Organ, die oder das im Auftrag des für die Bearbeitung veröffentlichen öffentlichen Organs Informationen bearbeitet.

**§ 6 Abs. 2 (geändert)**, **Abs. 3 (neu)**

[2] Bearbeiten mehrere öffentliche Organe einen gemeinsamen Informationsbestand, regeln sie die Verantwortung und legen fest, welches öffentliche Organ die Gesamtverantwortung trägt.

[3] Das öffentliche Organ muss nachweisen können, dass es die Datenschutzbestimmungen einhält. Der Regierungsrat regelt das Nähere für die kantonale Verwaltung, der Gemeinderat für die kommunale Verwaltung. Für die Gerichte und die selbständigen Anstalten und Körperschaften gilt die Regelung des Kantons sinngemäss.

**§ 7 Abs. 3 (neu)**

[3] Eine Auftragsdatenbearbeiterin beziehungsweise ein Auftragsdatenbeauftragter darf ohne vorgängige schriftliche Zustimmung des auftraggebenden öffentlichen Organs die Datenbearbeitung keiner weiteren Auftragsdatenbearbeiterin und keinem weiteren Auftragsdatenbearbeiter übertragen.

**§ 8 Abs. 4 (geändert)**

[4] Der Regierungsrat regelt das Nähere für die kantonale Verwaltung, der Gemeinderat für die kommunale Verwaltung. Für die Gerichte und die selbständigen Anstalten und Körperschaften gilt die Regelung des Kantons sinngemäss.

**§ 9 Abs. 2 (geändert)**, **Abs. 4 (neu)**

[2] Besondere Personendaten dürfen bearbeitet und ein Profiling darf vorgenommen werden, wenn

*Aufzählung unverändert.*

[4] Personendaten dürfen nur so lange bearbeitet werden, als es zur Erfüllung der gesetzlichen Aufgabe erforderlich ist.

**§ 9a Abs. 1 (geändert)**

[1] Der Regierungsrat kann, nachdem er im Rahmen einer Vorabkonsulation nach § 13 die Beurteilung der oder des Datenschutzbeauftragten eingeholt hat, vor Inkrafttreten eines Gesetzes die Bearbeitung von besonderen Personendaten bewilligen, wenn:

*Aufzählung unverändert.*

**§ 10 Abs. 1 (geändert)**

[1] Ein öffentliches Organ darf Personendaten zu einem nicht personenbezogenen Zweck, namentlich für Statistik, Planung oder Forschung, bearbeiten, wenn es

*Aufzählung unverändert.*

**§ 11 Abs. 2 (neu)**, **Abs. 3 (neu)**

[2] Wer Personendaten bearbeitet, hat sich über deren Richtigkeit zu vergewissern.

[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.

**§ 12a (neu)**

**Datenschutz-Folgenabschätzung**

[1] Das verantwortliche öffentliche Organ prüft bei jedem Vorhaben für eine Personendatenbearbeitung, ob voraussichtlich ein hohes Risiko für die Grundrechte der betroffenen Personen besteht. Das hohe Risiko ergibt sich, insbesondere bei Verwendung neuer Technologien, aus der Art, dem Umfang, den Umständen und dem Zweck der Bearbeitung.

[2] Besteht voraussichtlich ein hohes Risiko, ist eine Datenschutz-Folgenabschätzung durchzuführen.

[3] Die Folgenabschätzung enthält mindestens:

a) eine allgemeine Beschreibung der geplanten Bearbeitungsvorgänge;
b) eine Bewertung der in Bezug auf die Grundrechte der betroffenen Personen bestehende Risiken sowie
c) eine Darstellung und Bewertung der geplanten Abhilfemassnahmen, Garantien, Sicherheitsvorkehren und Verfahren, durch die der Schutz der Grundrechte der Personen sichergestellt und der Nachweis erbracht werden soll, dass dieses Gesetz eingehalten wird.

**§ 13 Abs. 1 (geändert)**, **Abs. 2 (geändert)**

**Vorabkonsultation der oder des Datenschutzbeauftragten (Überschrift geändert)**

[1] Das verantwortliche öffentliche Organ legt der oder dem Datenschutzbeauftragten frühzeitig zur Vorabkonsultation vor:

a) **(neu)** Rechtsetzungsprojekte, die das Bearbeiten von Personendaten betreffen oder die für den Umgang mit Informationen erheblich sind, und
b) **(neu)** Vorhaben zur Bearbeitung von Personendaten, die aufgrund der Art der Bearbeitung oder der zu bearbeitenden Daten zu einem hohen Risiko für die Grundrechte der betroffenen Personen führen.

[2] Die oder der Datenschutzbeauftragte erstellt eine Liste der Bearbeitungsvorgänge, die zur Vorabkonsultation zu unterbreiten sind.

**§ 14 Abs. 1 (geändert)**, **Abs. 2 (geändert)**

**Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Überschrift geändert)**

[1] Das öffentliche Organ trifft bei Datenbearbeitungen von Anfang an Massnahmen, die das Risiko von Verletzungen der Grundrechte verringern und solchen Verletzungen vorbeugen.

[2] Es stellt mittels geeigneter Voreinstellungen sicher, dass standardmässig nur diejenigen Personendaten bearbeitet werden, die für den jeweiligen Verwendungszweck erforderlich sind.

**§ 15 Abs. 1 (geändert)**, **Abs. 2 (geändert)**, **Abs. 3 (geändert)**, **Abs. 4 (neu)**

**Informationspflicht bei der Beschaffung (Überschrift geändert)**

[1] Das verantwortliche öffentliche Organ informiert die betroffene Person über jede Beschaffung von Personendaten. Diese Informationspflicht gilt auch, wenn die Daten bei Dritten beschafft werden.

[2] Die Information umfasst insbesondere Angaben über:

a) **(neu)** das verantwortliche öffentliche Organ samt Kontaktdaten;
b) **(neu)** die bearbeiteten Daten oder die Kategorien der bearbeiteten Daten;
c) **(neu)** die Rechtsgrundlage und den Zweck des Bearbeitens;
d) **(neu)** die Datenempfangenden oder die Kategorien der Datenempfangenden, falls die Daten Dritten bekannt gegeben werden, und
e) **(neu)** die Rechte der betroffenen Person.

[3] Die Informationspflicht entfällt, wenn

a) **(neu)** die betroffene Person bereits über die Informationen nach Abs. 2 verfügt;
b) **(neu)** wenn das Bearbeiten der Personendaten gesetzlich ausdrücklich vorgesehen ist oder
c) **(neu)** die Information nicht oder nur mit unverhältnismässigem Aufwand möglich ist.

[4] Die Übermittlung der Informationen kann unter denselben Voraussetzungen eingeschränkt werden wie der Zugang zu den eigenen Personendaten.

**§ 16 Abs. 2 (neu)**

[2] Für Informationsbestände, die Personendaten enthalten, sind Fristen für die Vernichtung beziehungsweise für die Überprüfung, ob die Daten zur Aufgabenerfüllung noch erforderlich sind, festzulegen.

**§ 16a (neu)**

**Meldung von Datenschutzverletzungen**

[1] Das verantwortliche öffentliche Organ meldet der oder dem Datenschutzbeauftragten ohne unangemessene Verzögerung eine Datenschutzverletzung.

[2] Die Auftragsdatenbearbeiterin oder der Auftragsdatenbearbeiter informiert das auftraggebende öffentliche Organ unverzüglich über eine Datenschutzverletzung.

[3] Eine Datenschutzverletzung liegt vor, wenn durch eine Verletzung der Informationssicherheit bearbeitete Personendaten unwiederbringlich vernichtet werden oder verloren gehen, unbeabsichtigt oder unrechtmässig verändert oder offenbart werden oder Unbefugte Zugang zu solchen Personendaten erhalten.

[4] Eine Meldepflicht besteht nicht, wenn die Datenschutzverletzung voraussichtlich nicht zu einem Risiko für die Grundrechte der betroffenen Person führt.

[5] Das öffentliche Organ informiert die betroffenen Personen, wenn die Umstände dies erfordern oder der oder die Datenschutzbeauftragte es verlangt.

[6] Die Benachrichtigung der betroffenen Personen kann ganz oder teilweise unterbleiben oder aufgeschoben werden, wenn eine Einschränkung gemäss § 29 zulässig ist.

**§ 18 Abs. 4 (geändert), Abs. 4$^{bis}$ (neu), Abs. 4$^{ter}$ (neu)**

[4] Vor dem Erlass und der Verlängerung eines Reglements ist das Vorhaben der oder dem Datenschutzbeauftragten zur Vorabkonsultation vorzulegen.

[4bis] Die Reglemente sind der Öffentlichkeit leicht zugänglich zu machen.

[4ter] Soweit durch die Bekanntgabe der Kamerastandorte oder anderer Einsatzdetails die Zweckerreichung verunmöglicht wird, kann auf deren Veröffentlichung verzichtet werden.

**§ 21 Abs. 2 (geändert)**

[2] Besondere Personendaten oder Resultate eines Profilings gibt das öffentliche Organ bekannt, wenn

*Aufzählung unverändert.*

**§ 22 Abs. 1 (geändert), Abs. 4 (geändert), Abs. 5 (geändert)**

[1] Das öffentliche Organ kann anderen öffentlichen Organen im Kanton, in anderen Kantonen oder im Bund Personendaten zur Bearbeitung für einen nicht personenbezogenen Zweck, namentlich für Statistik, Planung oder Forschung, bekannt geben, sofern dies nicht durch eine besondere Geheimhaltungsbestimmung ausgeschlossen ist.

[4] Privaten kann das öffentliche Organ Personendaten zur Bearbeitung für Zwecke der Forschung bekannt geben, sofern dies nicht durch eine besondere Geheimhaltungsbestimmung ausgeschlossen ist und sich die Empfängerin oder der Empfänger zusätzlich zu den Anforderungen von Abs. 2 verpflichtet,

*Aufzählung unverändert.*

[5] Unter den gleichen Voraussetzungen kann die richterliche Behörde den in einem kantonalen Anwaltsregister nach dem Bundesgesetz über die Freizügigkeit der Anwältinnen und Anwälte (Anwaltsgesetz, BGFA) vom 23. Juni 2000 eingetragenen Advokatinnen und Advokaten zum Zweck der Berufsausübung Urteile mit Personendaten bekannt geben, sofern die Urteile nicht bereits in anonymisierter Form vorliegen.

**§ 26 Abs. 2 (neu)**

[2] Der Zugang umfasst:

a) alle Personendaten zur gesuchstellenden Person;
b) alle verfügbaren Informationen über die Herkunft der Personendaten, wenn sie nicht bei der betroffenen Person erhoben worden sind und
c) die weiteren Angaben nach § 15 Abs. 2.

**§ 27 Abs. 1 (geändert), Abs. 1$^{bis}$ (neu), Abs. 1$^{ter}$ (neu)**

[1] Jede betroffene Person kann vom öffentlichen Organ verlangen, dass es kostenlos

c) **(geändert)** die Folgen des widerrechtlichen Bearbeitens von Personendaten beseitigt, insbesondere die sie betreffenden Personendaten löscht oder ihre Bekanntgabe an Dritte sperrt;

[1bis] Das schutzwürdige Interesse der betroffenen Person wird vermutet.

[1ter] Die Berichtigung, Vernichtung oder Löschung von Personendaten und die Sperrung der Bekanntgabe an Dritte ist ausserdem jenen Personen oder Stellen, denen die Daten zuvor bekannt gegeben worden sind, mitzuteilen, soweit dies nicht unmöglich oder mit unverhältnismässigem Aufwand verbunden ist.

**§ 28a (neu)**

**Aufsichtsrechtliche Anzeige an die Datenschutzbeauftragte oder den Datenschutzbeauftragten**

[1] Jede Person hat das Recht, sich mit einer aufsichtsrechtlichen Anzeige an die Datenschutzbeauftragte oder den Datenschutzbeauftragten zu wenden, wenn sie der Ansicht ist, dass ein öffentliches Organ, eine Auftragsbearbeiterin oder ein Auftragsbearbeiter bei der Bearbeitung von sie betreffenden Personendaten gegen die datenschutzrechtlichen Vorschriften verstösst.

[2] Der anzeigenden Person kommt in diesem Verfahren keine Parteistellung zu.

[3] Die oder der Datenschutzbeauftragte informiert sie innert drei Monaten über den Stand beziehungsweise das Ergebnis der Abklärungen und die Erledigung.

**§ 38 Abs. 3**

**Stellung und Aufsichtszuständigkeit (Überschrift geändert)**

[3] Der Kontrolle durch die Datenschutzbeauftragte oder den Datenschutzbeauftragten unterstehen nicht:

b) **(geändert)** der Regierungsrat als Behörde;
c) **(neu)** Datenbearbeitungen in hängigen Verfahren der Zivil- und Strafrechtspflege und
d) **(neu)** Datenbearbeitungen in hängigen Verfahren der Verfassungs- und Verwaltungsgerichtsbarkeit.

**§ 44 Abs. 1**

[1] Die oder der Datenschutzbeauftragte

b) **(geändert)** nimmt Stellung zu Rechtsetzungs- und anderen Vorhaben, die ihr oder ihm nach § 13 zur Vorabkonsultation vorzulegen sind;
f) **(geändert)** behandelt aufsichtsrechtliche Anzeigen nach § 28a;
g) **(neu)** sensibilisiert die öffentlichen Organe für ihre datenschutzrechtlichen Pflichten und die Öffentlichkeit für die Anliegen des Datenschutzes und der Transparenz;
h) **(neu)** verfolgt die für den Schutz von Personendaten und das Öffentlichkeitsprinzip massgeblichen Entwicklungen.

**§ 45 Abs. 1 (geändert), Abs. 2 (geändert)**

[1] Die oder der Datenschutzbeauftragte kann bei öffentlichen Organen, bei Auftragsdatenbearbeiterinnen und Auftragsdatenbearbeitern sowie 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.

[2] Die öffentlichen Organe, die Auftragsdatenbearbeiterinnen und Auftragsdatenbearbeiter sowie Drittpersonen, die von einem öffentlichen Organ Personendaten erhalten haben, sind verpflichtet, die Aufsichtsstelle bei der Erfüllung ihrer Aufgaben zu unterstützen. Sie wirken insbesondere an der Feststellung des Sachverhaltes mit.

**§ 50 Abs. 1 (geändert), Abs. 2 (aufgehoben)**

[1] Die oder der Datenschutzbeauftragte erstattet der Wahlbehörde und der Öffentlichkeit periodisch und bei Bedarf Bericht über Umfang und Schwerpunkte der Tätigkeiten, über wichtige Feststellungen und Beurteilungen sowie über die Wirkung des Gesetzes.

[2] *Aufgehoben.*

**§ 51 Abs. 1 (geändert)**

[1] Mit Busse bestraft wird, wer:

a) **(neu)** als Auftragsdatenbearbeiterin oder Auftragsdatenbearbeiter gemäss § 7 ohne ausdrückliche Ermächtigung des auftraggebenden öffentlichen Organs vorsätzlich oder fahrlässig Personendaten für sich oder andere verwendet oder anderen bekannt gibt oder

b) **(neu)** als Auftragsdatenbearbeiterin oder Auftragsdatenbearbeiter gemäss § 7 ohne vorgängige schriftliche Einwilligung des auftraggebenden öffentlichen Organs die Datenbearbeitung einer weiteren Auftragsdatenbearbeiterin und einem weiteren Auftragsdatenbearbeiter überträgt.

**§ 55 Abs. 1 (geändert)**

[1] Diese Änderung ist zu publizieren; sie unterliegt dem Referendum und der Regierungsrat bestimmt den Zeitpunkt des Inkrafttretens.

II. Änderung anderer Erlasse

**1.**

Gesetz betreffend die Organisation der Gerichte und der Staatsanwaltschaft (Gerichtsorganisationsgesetz, GOG) vom 3. Juni 2015 [2)] (Stand 1. Januar 2021) wird wie folgt geändert:

**Titel nach § 98 (neu)**

*7.5 Datenschutzberatung*

**§ 98a (neu)**

[1] Die Staatsanwaltschaft bezeichnet eine Datenschutzberaterin oder einen Datenschutzberater für die Staats- und Jugendanwaltschaft.

[2] Diese Person hat die folgenden Aufgaben:

1. Sie berät und unterstützt bei der Bearbeitung von Personendaten.
2. Sie nimmt Datenschutz-Folgenabschätzungen gemäss § 12a Abs. 1 des Gesetzes über die Information und den Datenschutz (Informations- und Datenschutzgesetz, IDG) vom 9. Juni 2010 vor.
3. Sie arbeitet mit der oder dem Datenschutzbeauftragten zusammen.

**2.**

Geoinformationsgesetz (KGeoIG) vom 16. November 2011 [3)] (Stand 1. September 2012) wird wie folgt geändert:

**§ 12 Abs. 3 (geändert)**

[3] Werden die Geodaten gemäss § 3 mit Downloaddienst zugänglich gemacht, ist vorab die oder der Datenschutzbeauftragte gemäss § 13 des Informations- und Datenschutzgesetzes (Informations- und Datenschutzgesetz, IDG) vom 9. Juni 2010 zu konsultieren.

---

2) SG 154.100

3) SG 214.300

**3.**
Gesetz über den Justizvollzug (Justizvollzugsgesetz, JVG) vom 13. November 2019 [4)] (Stand 1. Juli 2020) wird wie folgt geändert:

**§ 28a (neu)**

**Datenschutzberatung**

[1] Die Vollzugsbehörde bezeichnet eine Datenschutzberaterin oder einen Datenschutzberater.

[2] Diese Person hat die folgenden Aufgaben:

a) sie berät und unterstützt bei der Bearbeitung von Personendaten;
b) sie nimmt Datenschutz-Folgenabschätzungen gemäss § 12a Abs. 1 des Gesetzes über die Information und den Datenschutz (Informations- und Datenschutzgesetz, IDG) vom 9. Juni 2010 vor;
c) sie arbeitet mit der oder dem Datenschutzbeauftragten zusammen.

**4.**
Gesetz betreffend die Kantonspolizei des Kantons Basel-Stadt (Polizeigesetz, PolG [5)]) vom 13. November 1996 [6)] (Stand 1. Januar 2021) wird wie folgt geändert:

**§ 57 Abs. 5 (neu)**

[5] Die Kantonspolizei darf besondere Personendaten bearbeiten sowie Profiling vornehmen, soweit es zur Erfüllung ihrer gesetzlichen Aufgaben zwingend notwendig ist.

**§ 57a (neu)**

**Datenschutzberatung**

[1] Die Kantonspolizei bezeichnet eine Datenschutzberaterin oder einen Datenschutzberater.

[2] Diese Person hat die folgenden Aufgaben:

a) sie berät und unterstützt bei der Bearbeitung von Personendaten;
b) sie nimmt Datenschutz-Folgenabschätzungen gemäss § 12a Abs. 1 des Gesetzes über die Information und den Datenschutz (Informations- und Datenschutzgesetz, IDG) vom 9. Juni 2010 vor;
c) sie arbeitet mit der oder dem Datenschutzbeauftragten zusammen.

**5.**
Finanz- und Verwaltungskontrollgesetz (FVKG) vom 17. September 2003 [7)] (Stand 1. Juli 2016) wird wie folgt geändert:

**§ 22 Abs. 2 (geändert)**

[2] Die Finanzkontrolle hat das Recht, die für die Wahrnehmung der Finanzaufsicht erforderlichen Personendaten aus den Datensammlungen der Departemente und Dienststellen, der Gerichte sowie der selbständigen öffentlich-rechtlichen und privatrechtlichen Anstalten abzurufen. Soweit die Daten für die Aufgabenerfüllung geeignet und erforderlich sind, erstreckt sich das Zugriffsrecht auch auf besondere Personendaten. Die Finanzkontrolle unterliegt dabei der gleichen Geheimhaltungspflicht wie die geprüfte Stelle. Die Finanzkontrolle darf die ihr derart zur Kenntnis gebrachten Personendaten nur bis zum Abschluss des Revisionsverfahrens aufbewahren oder speichern. Die Zugriffe auf die verschiedenen Datensammlungen und die damit verfolgten Zwecke müssen dokumentiert sein.

**6.**
Gesetz über die direkten Steuern (Steuergesetz, StG) vom 12. April 2000 [8)] (Stand 1. Januar 2021) wird wie folgt geändert:

---

4) SG 258.200
5) Titel: Abkürzung redaktionell ergänzt.
6) SG 510.100
7) SG 610.200
8) SG 640.100

**§ 141a Abs. 1 (geändert)**

[1] Die Steuerverwaltung betreibt zur Erfüllung ihrer Aufgaben ein Informationssystem. Dieses kann auch besondere Personendaten über administrative und strafrechtliche Sanktionen enthalten, die steuerrechtlich wesentlich sind.

**7.**

Gesetz über die Industriellen Werke Basel (IWB-Gesetz) vom 11. Februar 2009 [9)] (Stand 1. Juli 2020) wird wie folgt geändert:

**§ 35a Abs. 3 (geändert)**

[3] Die Einzelheiten der Datenbearbeitung gemäss Abs. 1 und 2 werden in vom Verwaltungsrat zu erlassenden und vom Regierungsrat zu genehmigenden Ausführungsbestimmungen für jedes Medium (Elektrizität, Erdgas, Fernwärme und Wasser) separat geregelt. Diese Ausführungsbestimmungen zur Datenbearbeitung sind der oder dem kantonalen Datenschutzbeauftragten im Rahmen einer Vorabkonsultation vorzulegen.

**8.**

Gesetz betreffend die Tagesbetreuung von Kindern (Tagesbetreuungsgesetz) vom 17. September 2003 [10)] (Stand 1. Januar 2016) wird wie folgt geändert:

**§ 15 Abs. 1 (geändert)**

[1] Für die Bearbeitung der Daten, einschliesslich besonderer Personendaten, ist das Gesetz über die Harmonisierung und Koordination von bedarfsabhängigen Sozialleistungen im Kanton Basel-Stadt (Harmonisierungsgesetz Sozialleistungen, SoHaG) vom 25. Juni 2008 massgebend.

**9.**

Gesetz über die Harmonisierung und Koordination von bedarfsabhängigen Sozialleistungen (Harmonisierungsgesetz Sozialleistungen, SoHaG) vom 25. Juni 2008 [11)] (Stand 1. Juli 2015) wird wie folgt geändert:

**§ 25 Abs. 2 (geändert)**, **Abs. 3 (geändert)**

[2] Die Bekanntgabe von Daten für einen nicht personenbezogenen Zweck, namentlich für Planung und Forschung, an andere öffentliche Organe im Kanton sowie an öffentliche Organe in anderen Kantonen oder des Bundes richtet sich nach § 22 IDG.

[3] Die Bekanntgabe von Daten an Private kann zum Zweck der Forschung ausschliesslich in anonymisierter Form erfolgen.

III. Aufhebung anderer Erlasse

*Keine Aufhebung anderer Erlasse.*

IV. Schlussbestimmung

Diese Änderung ist zu publizieren; sie unterliegt dem Referendum und der Regierungsrat bestimmt den Zeitpunkt des Inkrafttretens.

---

9) SG 772.300
10) SG 815.100
11) SG 890.700

[Behörde]

[Funktion 1]
[NAME 1]

[Funktion 2]
[NAME 2]

**Synopse**

**Änderung des Gesetzes über die Information und den Datenschutz vom 9. Juni 2010**

| Geltendes Recht | Arbeitsversion (Stempel: 16.06.2021) |
|---|---|
| | **Gesetz über die Information und den Datenschutz (Informations- und Datenschutzgesetz, IDG)** |
| | *Der Grosse Rat des Kantons Basel-Stadt,*<br><br>nach Einsichtnahme in den Ratschlag des Regierungsrates Nr. [Nr. eingeben] vom [Datum eingeben] sowie in den Bericht der Justiz-, Sicherheits- und Sportkommission Nr. [Nr. eingeben] vom [Datum eingeben],<br><br>*beschliesst:* |
| | **I.** |
| | Gesetz über die Information und den Datenschutz (Informations- und Datenschutzgesetz, IDG) vom 9. Juni 2010 (Stand 4. Januar 2018) wird wie folgt geändert: |
| **§ 1**<br>Gegenstand und Zweck<br><br>[1] Dieses Gesetz regelt den Umgang der öffentlichen Organe mit Informationen.<br><br>[2] Es bezweckt,<br><br>a) das Handeln der öffentlichen Organe transparent zu gestalten und damit die freie Meinungsbildung und die Wahrnehmung der demokratischen Rechte zu fördern, soweit nicht überwiegende öffentliche oder private Interessen entgegenstehen, und<br><br>b) die Grundrechte von Personen zu schützen, über welche die öffentlichen Organe Personendaten bearbeiten. | [2] Es bezweckt~~,~~:<br><br>b) die Grundrechte von natürlichen Personen zu schützen, über welche die öffentlichen Organe Personendaten bearbeiten. |
| **§ 2**<br>Geltungsbereich<br><br>[1] Dieses Gesetz gilt für alle öffentlichen Organe gemäss § 3 Abs. 1. | |

| Geltendes Recht | Arbeitsversion (Stempel: 16.06.2021) |
|---|---|
| [2] Es findet keine Anwendung: | [2] Es findet keine Anwendung~~:~~, soweit ein öffentliches Organ am wirtschaftlichen Wettbewerb teilnimmt und dabei privatrechtlich handelt. Für das Bearbeiten von Personendaten ist das Bundesgesetz über den Datenschutz (DSG) vom 19. Juni 1992 sinngemäss anwendbar. |
| a) soweit ein öffentliches Organ am wirtschaftlichen Wettbewerb teilnimmt und dabei privatrechtlich handelt; | a) *Aufgehoben.* |
| b) in hängigen Verfahren der Zivil- und Strafrechtspflege; | b) *Aufgehoben.* |
| c) in hängigen Verfahren der Verfassungs- und Verwaltungsgerichtsbarkeit. | c) *Aufgehoben.* |
| | [2bis] In hängigen Verfahren der Zivil- und Strafrechtspflege sowie der Verfassungs- und Verwaltungsgerichtsbarkeit richten sich die Rechte und Ansprüche der betroffenen Person, die Informationspflicht des öffentlichen Organs bei der Beschaffung von Personendaten, die Bekanntgabe von Personendaten an Verfahrensbeteiligte, die Information der Öffentlichkeit und der allgemeine Informationszugangsanspruch der Öffentlichkeit ausschliesslich nach dem anwendbaren Verfahrensrecht. |
| [3] Abweichende und ergänzende Bestimmungen in anderen Gesetzen bleiben vorbehalten, sofern sie den Schutz der Grundrechte von Personen, über welche die öffentlichen Organe Personendaten bearbeiten, im Sinne dieses Gesetzes sicherstellen. | |
| [4] Der Regierungsrat sorgt dafür, dass interkantonale Institutionen mit baselstädtischer Beteiligung einen gleichwertigen Datenschutz gewährleisten. | |
| **§ 3**<br>Begriffe | |
| [1] Öffentliche Organe im Sinne dieses Gesetzes sind: | |
| a) die Organisationseinheiten des Kantons und der Gemeinden, die eine öffentliche Aufgabe erfüllen; | |
| b) die Organisationseinheiten der juristischen Personen des kantonalen und kommunalen öffentlichen Rechts, die eine öffentliche Aufgabe erfüllen; | |

| Geltendes Recht | Arbeitsversion (Stempel: 16.06.2021) |
|---|---|
| c) Private, soweit ihnen von Kanton oder Gemeinden die Erfüllung öffentlicher Aufgaben übertragen ist. | |
| [2] Informationen im Sinne dieses Gesetzes sind alle Aufzeichnungen, welche die Erfüllung einer öffentlichen Aufgabe betreffen, unabhängig von ihrer Darstellungsform und ihrem Informationsträger. | |
| [3] Personendaten sind Informationen, die sich auf eine bestimmte oder bestimmbare natürliche oder juristische Person beziehen. | [3] Personendaten sind Informationen, die sich auf eine bestimmte oder bestimmbare natürliche ~~oder juristische~~ Person beziehen. |
| [4] Besondere Personendaten sind: | |
| a) Personendaten, bei deren Bearbeitung eine besondere Gefahr der Grundrechtsverletzung besteht, insbesondere Angaben über: | a) Personendaten, bei deren Bearbeitung eine besondere Gefahr der Grundrechtsverletzung besteht~~,~~ (sensitive Personendaten), insbesondere ~~Angaben über~~: |
| 1. die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten, | 1. Angaben über die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten~~,~~; |
| 2. die Gesundheit, das Erbgut, die persönliche Geheimsphäre oder die ethnische Herkunft, | 2. Angaben über die Gesundheit, das Erbgut (genetische Daten), die persönliche Geheimsphäre, das Sexualleben, die sexuelle Orientierung oder die ethnische Herkunft~~,~~; |
| 3. Massnahmen der sozialen Hilfe und | 3. Angaben über Massnahmen der sozialen Hilfe ~~und~~; |
| 4. administrative oder strafrechtliche Verfolgungen und Sanktionen. | 4. Angaben über administrative oder strafrechtliche Verfolgungen und Sanktionen~~.~~ und |
| | 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) Zusammenstellungen von Informationen, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlauben (Persönlichkeitsprofil). | |

| Geltendes Recht | Arbeitsversion (Stempel: 16.06.2021) |
|---|---|
| [5] Bearbeiten ist jeder Umgang mit Informationen wie das Beschaffen, Aufbewahren, Verwenden, Verändern, Bekanntgeben oder Vernichten, unabhängig von den angewandten Mitteln und Verfahren. | [5] Bearbeiten ist jeder Umgang mit Informationen ~~wie~~, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten~~, unabhängig von den angewandten Mitteln und Verfahren.~~ sowie das Durchführen logischer oder rechnerischer Operationen mit diesen Informationen. |
| [6] Bekanntgeben ist jedes Zugänglichmachen von Informationen wie das Einsichtgewähren, Weitergeben oder Veröffentlichen. | |
| | [7] Profiling ist jede Auswertung von Informationen, um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen, insbesondere bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Geheimsphäre oder Mobilität, vorherzusagen. |
| | [8] Auftragsdatenbearbeiterin oder Auftragsdatenbearbeiter ist die private Person oder das öffentliche Organ, die oder das im Auftrag des für die Bearbeitung veröffentlichen öffentlichen Organs Informationen bearbeitet. |
| **§ 6**<br>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. | [2] Bearbeiten mehrere öffentliche Organe einen gemeinsamen Informationsbestand, regeln sie die Verantwortung~~.~~ und legen fest, welches öffentliche Organ die Gesamtverantwortung trägt. |
| | [3] Das öffentliche Organ muss nachweisen können, dass es die Datenschutzbestimmungen einhält. Der Regierungsrat regelt das Nähere für die kantonale Verwaltung, der Gemeinderat für die kommunale Verwaltung. Für die Gerichte und die selbständigen Anstalten und Körperschaften gilt die Regelung des Kantons sinngemäss. |
| **§ 7**<br>Bearbeiten im Auftrag | |

| Geltendes Recht | Arbeitsversion (Stempel: 16.06.2021) |
|---|---|
| [1] Das öffentliche Organ kann das Bearbeiten von Informationen Dritten übertragen, wenn:<br><br>a) keine rechtliche Bestimmung oder vertragliche Vereinbarung entgegensteht und<br><br>b) sichergestellt wird, dass die Informationen nur so bearbeitet werden, wie es das öffentliche Organ tun dürfte.<br><br>[2] Es bleibt für den Umgang mit Informationen nach diesem Gesetz verantwortlich. | [3] Eine Auftragsdatenbearbeiterin beziehungsweise ein Auftragsdatenbeauftragter darf ohne vorgängige schriftliche Zustimmung des auftraggebenden öffentlichen Organs die Datenbearbeitung keiner weiteren Auftragsdatenbearbeiterin und keinem weiteren Auftragsdatenbearbeiter übertragen. |
| **§ 8**<br>Informationssicherheit<br><br>[1] Das öffentliche Organ schützt Informationen durch angemessene organisatorische und technische Massnahmen.<br><br>[2] Die Massnahmen richten sich nach den folgenden Schutzzielen:<br><br>a) Informationen dürfen nicht unrechtmässig zur Kenntnis gelangen (Vertraulichkeit);<br><br>b) Informationen müssen richtig und vollständig sein (Integrität);<br><br>c) Informationen müssen bei Bedarf vorhanden sein (Verfügbarkeit);<br><br>d) Informationsbearbeitungen müssen einer Person zugerechnet werden können (Zurechenbarkeit);<br><br>e) Veränderungen von Informationen müssen erkennbar und nachvollziehbar sein (Nachvollziehbarkeit). | |

| Geltendes Recht | Arbeitsversion (Stempel: 16.06.2021) |
|---|---|
| [3] Die zu treffenden Massnahmen richten sich nach der Art der Information, nach Art und Zweck der Verwendung und nach dem jeweiligen Stand der Technik.<br><br>[4] Der Regierungsrat regelt das Nähere für die kantonale Verwaltung, der Gemeinderat für die kommunale Verwaltung. | [4] Der Regierungsrat regelt das Nähere für die kantonale Verwaltung, der Gemeinderat für die kommunale Verwaltung. Für die Gerichte und die selbständigen Anstalten und Körperschaften gilt die Regelung des Kantons sinngemäss. |
| **§ 9**<br>Voraussetzungen für das Bearbeiten von Personendaten<br><br>[1] Ein öffentliches Organ darf Personendaten bearbeiten, wenn<br><br>a) dafür eine gesetzliche Grundlage besteht oder<br><br>b) dies zur Erfüllung einer gesetzlichen Aufgabe erforderlich ist.<br><br>[2] Besondere Personendaten dürfen bearbeitet werden, wenn<br><br>a) ein Gesetz dazu ausdrücklich ermächtigt oder verpflichtet oder<br><br>b) es für eine in einem Gesetz klar umschriebene Aufgabe zwingend notwendig ist.<br><br>[3] Das Bearbeiten von Personendaten hat nach Treu und Glauben zu erfolgen und muss verhältnismässig sein. | [2] Besondere Personendaten dürfen bearbeitet und ein Profiling darf vorgenommen werden, wenn<br><br>[4] Personendaten dürfen nur so lange bearbeitet werden, als es zur Erfüllung der gesetzlichen Aufgabe erforderlich ist. |
| **§ 9a**<br>Voraussetzungen für das Bearbeiten von besonderen Personendaten im Rahmen von Pilotversuchen<br><br>[1] Der Regierungsrat kann, nachdem er im Rahmen einer Vorabkontrolle nach § 13 die Beurteilung der oder des Datenschutzbeauftragten eingeholt hat, vor Wirksamwerden eines Gesetzes die Bearbeitung von besonderen Personendaten bewilligen, wenn: | [1] Der Regierungsrat kann, nachdem er im Rahmen einer ~~Vorabkontrolle~~ Vorabkonsulation nach § 13 die Beurteilung der oder des Datenschutzbeauftragten eingeholt hat, vor ~~Wirksamwerden~~Inkrafttreten eines Gesetzes die Bearbeitung von besonderen Personendaten bewilligen, wenn: |

| Geltendes Recht | Arbeitsversion (Stempel: 16.06.2021) |
|---|---|
| a) die Aufgaben, die diese Bearbeitung erforderlich machen, in einem Gesetz geregelt sind,<br><br>b) ausreichende Massnahmen zur Verhinderung von Persönlichkeitsverletzungen getroffen werden und<br><br>c) die praktische Umsetzung einer Datenbearbeitung eine Testphase vor dem Wirksamwerden des Gesetzes zwingend erfordert.<br><br>[2] Die praktische Umsetzung einer Datenbearbeitung kann eine Testphase dann zwingend erfordern, wenn:<br><br>a) die Erfüllung einer Aufgabe technische Neuerungen erfordert, deren Auswirkungen zunächst evaluiert werden müssen,<br><br>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<br><br>c) sie die Übermittlung von besonderen Personendaten an Dritte mittels eines Abrufverfahrens erfordert.<br><br>[3] Pilotprojekte sind auf maximal fünf Jahre zu befristen.<br><br>[4] Jedes Pilotprojekt ist zu evaluieren.<br><br>[5] Der Regierungsrat regelt die Modalitäten der Datenbearbeitung in einer Verordnung. | |
| **§ 10**<br>Voraussetzungen für das Bearbeiten von Personendaten zu einem nicht personenbezogenen Zweck<br><br>[1] Ein öffentliches Organ darf Personendaten zu einem nicht personenbezogenen Zweck, namentlich für Statistik, Planung, Wissenschaft oder Forschung, bearbeiten, wenn es | [1] Ein öffentliches Organ darf Personendaten zu einem nicht personenbezogenen Zweck, namentlich für Statistik, Planung~~, Wissenschaft~~ oder Forschung, bearbeiten, wenn es |

| Geltendes Recht | Arbeitsversion (Stempel: 16.06.2021) |
|---|---|
| a) diese Daten nicht mehr für einen personenbezogenen Zweck verwendet oder weitergibt und<br><br>b) diese Daten anonymisiert oder pseudonymisiert, sobald es der Bearbeitungszweck erlaubt, und<br><br>c) die Ergebnisse der Bearbeitung nur so bekannt gibt, dass keine Rückschlüsse auf betroffene Personen möglich sind.<br><br>2 … | |
| **§ 11**<br>Richtigkeit<br><br>1 Personendaten müssen richtig und, soweit es der Verwendungszweck erfordert, vollständig sein. | 2 Wer Personendaten bearbeitet, hat sich über deren Richtigkeit zu vergewissern.<br><br>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. |
| | **§ 12a**<br>Datenschutz-Folgenabschätzung<br><br>1 Das verantwortliche öffentliche Organ prüft bei jedem Vorhaben für eine Personendatenbearbeitung, ob voraussichtlich ein hohes Risiko für die Grundrechte der betroffenen Personen besteht. Das hohe Risiko ergibt sich, insbesondere bei Verwendung neuer Technologien, aus der Art, dem Umfang, den Umständen und dem Zweck der Bearbeitung.<br><br>2 Besteht voraussichtlich ein hohes Risiko, ist eine Datenschutz-Folgenabschätzung durchzuführen.<br><br>3 Die Folgenabschätzung enthält mindestens: |

| Geltendes Recht | Arbeitsversion (Stempel: 16.06.2021) |
|---|---|
| | a) eine allgemeine Beschreibung der geplanten Bearbeitungsvorgänge;<br><br>b) eine Bewertung der in Bezug auf die Grundrechte der betroffenen Personen bestehende Risiken sowie<br><br>c) eine Darstellung und Bewertung der geplanten Abhilfemassnahmen, Garantien, Sicherheitsvorkehren und Verfahren, durch die der Schutz der Grundrechte der Personen sichergestellt und der Nachweis erbracht werden soll, dass dieses Gesetz eingehalten wird. |
| **§ 13**<br>Vorabkontrolle<br><br>[1] Wenn eine Bearbeitung von Personendaten aufgrund der Art der Bearbeitung oder der zu bearbeitenden Daten geeignet ist, besondere Risiken für die Rechte und Freiheit der betroffenen Personen mit sich zu bringen, muss diese Bearbeitung vorab der oder dem Datenschutzbeauftragten zur Kontrolle vorgelegt werden.<br><br>[2] Die oder der Datenschutzbeauftragte gibt die Beurteilung in Form einer Empfehlung gemäss § 46 ab. | **§ 13**<br>~~Vorabkontrolle~~Vorabkonsultation der oder des Datenschutzbeauftragten<br><br>[1] ~~Wenn eine Bearbeitung von Personendaten aufgrund~~ Das verantwortliche öffentliche Organ legt ~~der Art der Bearbeitung oder der zu bearbeitenden Daten geeignet ist, besondere Risiken für die Rechte und Freiheit der betroffenen Personen mit sich zu bringen, muss diese Bearbeitung vorab~~ der oder dem Datenschutzbeauftragten frühzeitig zur ~~Kontrolle vorgelegt werden.~~Vorabkonsultation vor:<br><br>a) Rechtsetzungsprojekte, die das Bearbeiten von Personendaten betreffen oder die für den Umgang mit Informationen erheblich sind, und<br><br>b) Vorhaben zur Bearbeitung von Personendaten, die aufgrund der Art der Bearbeitung oder der zu bearbeitenden Daten zu einem hohen Risiko für die Grundrechte der betroffenen Personen führen.<br><br>[2] Die oder der Datenschutzbeauftragte ~~gibt~~ erstellt eine Liste der Bearbeitungsvorgänge, die ~~Beurteilung in Form einer Empfehlung gemäss § 46 ab.~~zur Vorabkonsultation zu unterbreiten sind. |
| **§ 14**<br>Datenvermeidung und Datensparsamkeit bei IT-Systemen | **§ 14**<br>~~Datenvermeidung~~ Datenschutz durch Technikgestaltung und ~~Datensparsamkeit bei IT-Systemen~~durch datenschutzfreundliche Voreinstellungen |

| Geltendes Recht | Arbeitsversion (Stempel: 16.06.2021) |
|---|---|
| [1] Das öffentliche Organ gestaltet informationstechnologische Systeme so, dass keine oder möglichst wenig personenbezogene und personenbeziehbare Daten anfallen.<br><br>[2] Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. | [1] Das öffentliche Organ ~~gestaltet informationstechnologische Systeme so, dass keine oder möglichst wenig personenbezogene~~ trifft bei Datenbearbeitungen von Anfang an Massnahmen, die das Risiko von Verletzungen der Grundrechte verringern und ~~personenbeziehbare Daten anfallen~~solchen Verletzungen vorbeugen.<br><br>[2] ~~Insbesondere ist von~~ Es stellt mittels geeigneter Voreinstellungen sicher, dass standardmässig nur diejenigen Personendaten bearbeitet werden, die für den ~~Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.~~jeweiligen Verwendungszweck erforderlich sind. |
| **§ 15**<br>Erkennbarkeit der Beschaffung<br><br>[1] Die betroffene Person muss erkennen können, welche Personendaten über sie beschafft und zu welchem Zweck sie bearbeitet werden, soweit dadurch nicht die Erfüllung der gesetzlichen Aufgabe ernsthaft gefährdet wird.<br><br>[2] Werden Personendaten systematisch, namentlich mit Fragebogen oder Onlineerfassungen, erhoben, so müssen Rechtsgrundlage und Zweck der Bearbeitung angegeben sein. | **§ 15**<br>~~Erkennbarkeit~~Informationspflicht bei der Beschaffung<br><br>[1] ~~Die~~ Das verantwortliche öffentliche Organ informiert die betroffene Person ~~muss erkennen können, welche Personendaten~~ über ~~sie~~ jede Beschaffung von Personendaten. Diese Informationspflicht gilt auch, wenn die Daten bei Dritten beschafft ~~und zu welchem Zweck sie bearbeitet~~ werden~~, soweit dadurch nicht die Erfüllung der gesetzlichen Aufgabe ernsthaft gefährdet wird~~.<br><br>[2] ~~Werden Personendaten systematisch, namentlich mit Fragebogen oder Onlineerfassungen, erhoben, so müssen Rechtsgrundlage und Zweck der Bearbeitung angegeben sein.~~Die Information umfasst insbesondere Angaben über:<br><br>a) das verantwortliche öffentliche Organ samt Kontaktdaten;<br><br>b) die bearbeiteten Daten oder die Kategorien der bearbeiteten Daten;<br><br>c) die Rechtsgrundlage und den Zweck des Bearbeitens;<br><br>d) die Datenempfangenden oder die Kategorien der Datenempfangenden, falls die Daten Dritten bekannt gegeben werden, und<br><br>e) die Rechte der betroffenen Person. |

| Geltendes Recht | Arbeitsversion (Stempel: 16.06.2021) |
|---|---|
| [3] Bei der Beschaffung von besonderen Personendaten ist das öffentliche Organ verpflichtet, die betroffene Person über den Zweck der Bearbeitung zu informieren, soweit dadurch nicht die Erfüllung der gesetzlichen Aufgabe ernsthaft gefährdet wird. | [3] ~~Bei der Beschaffung von besonderen Personendaten ist das öffentliche Organ verpflichtet, die betroffene Person über den Zweck der Bearbeitung zu informieren, soweit dadurch nicht die Erfüllung der gesetzlichen Aufgabe ernsthaft gefährdet wird.~~Die Informationspflicht entfällt, wenn<br><br>a) die betroffene Person bereits über die Informationen nach Abs. 2 verfügt;<br><br>b) wenn das Bearbeiten der Personendaten gesetzlich ausdrücklich vorgesehen ist oder<br><br>c) die Information nicht oder nur mit unverhältnismässigem Aufwand möglich ist.<br><br>[4] Die Übermittlung der Informationen kann unter denselben Voraussetzungen eingeschränkt werden wie der Zugang zu den eigenen Personendaten. |
| **§ 16**<br>Vernichtung<br><br>[1] Nicht mehr benötigte Personendaten, die von der gemäss Archivgesetz zuständigen Stelle als nicht archivwürdig beurteilt werden, sind vom öffentlichen Organ zu vernichten. | [2] Für Informationsbestände, die Personendaten enthalten, sind Fristen für die Vernichtung beziehungsweise für die Überprüfung, ob die Daten zur Aufgabenerfüllung noch erforderlich sind, festzulegen. |
| | **§ 16a**<br>Meldung von Datenschutzverletzungen<br><br>[1] Das verantwortliche öffentliche Organ meldet der oder dem Datenschutzbeauftragten ohne unangemessene Verzögerung eine Datenschutzverletzung.<br><br>[2] Die Auftragsdatenbearbeiterin oder der Auftragsdatenbearbeiter informiert das auftraggebende öffentliche Organ unverzüglich über eine Datenschutzverletzung. |

| Geltendes Recht | Arbeitsversion (Stempel: 16.06.2021) |
|---|---|
| | [3] Eine Datenschutzverletzung liegt vor, wenn durch eine Verletzung der Informationssicherheit bearbeitete Personendaten unwiederbringlich vernichtet werden oder verloren gehen, unbeabsichtigt oder unrechtmässig verändert oder offenbart werden oder Unbefugte Zugang zu solchen Personendaten erhalten.<br><br>[4] Eine Meldepflicht besteht nicht, wenn die Datenschutzverletzung voraussichtlich nicht zu einem Risiko für die Grundrechte der betroffenen Person führt.<br><br>[5] Das öffentliche Organ informiert die betroffenen Personen, wenn die Umstände dies erfordern oder der oder die Datenschutzbeauftragte es verlangt.<br><br>[6] Die Benachrichtigung der betroffenen Personen kann ganz oder teilweise unterbleiben oder aufgeschoben werden, wenn eine Einschränkung gemäss § 29 zulässig ist. |
| **§ 18**<br>Reglement für das Videoüberwachungssystem<br><br>[1] Für jedes Videoüberwachungssystem muss vor seiner Inbetriebnahme ein Reglement erlassen werden, das insbesondere den Zweck des Systems, die Verantwortlichkeit und die Löschungsfrist regelt.<br><br>[2] Zuständig für den Erlass der Reglemente sind:<br><br>a) die Departemente bei Systemen im Verantwortungsbereich kantonaler öffentlicher Organe;<br><br>b) der Gemeinderat bei Systemen im Verantwortungsbereich kommunaler öffentlicher Organe;<br><br>c) der Gerichtsrat bei Systemen im Verantwortungsbereich von Gerichten;<br><br>d) die Direktion selbständiger Anstalten und Körperschaften des öffentlichen Rechts bei Systemen in ihrem Verantwortungsbereich.<br><br>[3] Das Reglement ist jeweils auf eine Dauer von maximal vier Jahren zu befristen. Vor einer allfälligen Verlängerung ist die Wirksamkeit der Videoüberwachung zu evaluieren. | |

| Geltendes Recht | Arbeitsversion (Stempel: 16.06.2021) |
|---|---|
| [4] Vor dem Erlass und der Verlängerung eines Reglements ist das Vorhaben der oder dem Datenschutzbeauftragten zur Vorabkontrolle vorzulegen. | [4] Vor dem Erlass und der Verlängerung eines Reglements ist das Vorhaben der oder dem Datenschutzbeauftragten zur ~~Vorabkontrolle~~Vorabkonsultation vorzulegen.<br><br>[4bis] Die Reglemente sind der Öffentlichkeit leicht zugänglich zu machen.<br><br>[4ter] Soweit durch die Bekanntgabe der Kamerastandorte oder anderer Einsatzdetails die Zweckerreichung verunmöglicht wird, kann auf deren Veröffentlichung verzichtet werden. |
| [5] Der Regierungsrat regelt das Nähere für die kantonale Verwaltung. Für die Gerichte, die Gemeinden und die selbständigen Anstalten und Körperschaften gilt die Regelung des Kantons sinngemäss. | |
| **§ 21**<br>Bekanntgabe von Personendaten<br><br>[1] Das öffentliche Organ gibt Personendaten bekannt, wenn<br><br>a) eine gesetzliche Bestimmung dazu verpflichtet oder ermächtigt, oder<br><br>b) dies zur Erfüllung einer gesetzlichen Aufgabe erforderlich ist oder<br><br>c) im Einzelfall die betroffene Person ausdrücklich zugestimmt hat oder, falls sie dazu nicht in der Lage ist, die Bekanntgabe in ihrem Interesse liegt und ihre Zustimmung in guten Treuen vorausgesetzt werden darf. | |
| [2] Besondere Personendaten gibt das öffentliche Organ bekannt, wenn<br><br>a) ein Gesetz dazu ausdrücklich verpflichtet oder ermächtigt oder<br><br>b) dies zur Erfüllung einer in einem Gesetz klar umschriebenen Aufgabe zwingend notwendig ist oder<br><br>c) im Einzelfall die betroffene Person ausdrücklich zugestimmt hat oder, falls sie dazu nicht in der Lage ist, die Bekanntgabe in ihrem Interesse liegt und ihre Zustimmung in guten Treuen vorausgesetzt werden darf. | [2] Besondere Personendaten <u>oder Resultate eines Profilings</u> gibt das öffentliche Organ bekannt, wenn |

| Geltendes Recht | Arbeitsversion (Stempel: 16.06.2021) |
|---|---|
| **§ 22**<br>Bekanntgabe von Personendaten für einen nicht personenbezogenen Zweck | |
| [1] Das öffentliche Organ kann anderen öffentlichen Organen im Kanton, in anderen Kantonen oder im Bund Personendaten zur Bearbeitung für einen nicht personenbezogenen Zweck, namentlich für Statistik, Planung, Wissenschaft oder Forschung, bekannt geben, sofern dies nicht durch eine besondere Geheimhaltungsbestimmung ausgeschlossen ist. | [1] Das öffentliche Organ kann anderen öffentlichen Organen im Kanton, in anderen Kantonen oder im Bund Personendaten zur Bearbeitung für einen nicht personenbezogenen Zweck, namentlich für Statistik, Planung~~, Wissenschaft~~ oder Forschung, bekannt geben, sofern dies nicht durch eine besondere Geheimhaltungsbestimmung ausgeschlossen ist. |
| [2] Die Empfängerin oder der Empfänger hat sich zu verpflichten: | |
| a) die Personendaten zu anonymisieren oder zu pseudonymisieren, sobald es der Bearbeitungszweck zulässt, und | |
| b) die Auswertungen nur so bekannt zu geben, dass keine Rückschlüsse auf betroffene Personen möglich sind. | |
| [3] … | |
| [4] Privaten kann das öffentliche Organ Personendaten zur Bearbeitung für Zwecke der Wissenschaft und Forschung bekannt geben, sofern dies nicht durch eine besondere Geheimhaltungsbestimmung ausgeschlossen ist und sich die Empfängerin oder der Empfänger zusätzlich zu den Anforderungen von Abs. 2 verpflichtet, | [4] Privaten kann das öffentliche Organ Personendaten zur Bearbeitung für Zwecke der ~~Wissenschaft und~~ Forschung bekannt geben, sofern dies nicht durch eine besondere Geheimhaltungsbestimmung ausgeschlossen ist und sich die Empfängerin oder der Empfänger zusätzlich zu den Anforderungen von Abs. 2 verpflichtet, |
| a) die Personendaten nicht für andere Zwecke zu bearbeiten und | |
| b) die Personendaten nicht an Dritte weiterzugeben und | |
| c) für die Informationssicherheit zu sorgen. | |

| Geltendes Recht | Arbeitsversion (Stempel: 16.06.2021) |
|---|---|
| [5] Unter den gleichen Voraussetzungen kann die richterliche Behörde den in einem kantonalen Anwaltsregister nach dem Anwaltsgesetz des Bundes [1)] eingetragenen Advokatinnen und Advokaten zum Zweck der Berufsausübung Urteile mit Personendaten bekannt geben. | [5] Unter den gleichen Voraussetzungen kann die richterliche Behörde den in einem kantonalen Anwaltsregister nach dem ~~Anwaltsgesetz des Bundes~~ Bundesgesetz über die Freizügigkeit der Anwältinnen und Anwälte (Anwaltsgesetz, BGFA) vom 23. Juni 2000 eingetragenen Advokatinnen und Advokaten zum Zweck der Berufsausübung Urteile mit Personendaten bekannt geben~~.~~, sofern die Urteile nicht bereits in anonymisierter Form vorliegen. |
| **§ 26**<br>Zugang zu den eigenen Personendaten<br><br>[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. | [2] Der Zugang umfasst:<br><br>a) alle Personendaten zur gesuchstellenden Person;<br><br>b) alle verfügbaren Informationen über die Herkunft der Personendaten, wenn sie nicht bei der betroffenen Person erhoben worden sind und<br><br>c) die weiteren Angaben nach § 15 Abs. 2. |
| **§ 27**<br>Schutz der eigenen Personendaten<br><br>[1] Jede betroffene Person kann vom öffentlichen Organ verlangen, dass es<br><br>a) unrichtige Personendaten berichtigt oder, falls die Berichtigung nicht möglich ist, vernichtet;<br><br>b) das widerrechtliche Bearbeiten von Personendaten unterlässt; | [1] Jede betroffene Person kann vom öffentlichen Organ verlangen, dass es kostenlos |

[1)] SR 935.61.

| Geltendes Recht | Arbeitsversion (Stempel: 16.06.2021) |
|---|---|
| c) die Folgen des widerrechtlichen Bearbeitens von Personendaten beseitigt;<br><br>d) die Widerrechtlichkeit des Bearbeitens von Personendaten schriftlich feststellt.<br><br>[2] Der Regierungsrat regelt das Nähere. | c) die Folgen des widerrechtlichen Bearbeitens von Personendaten beseitigt, insbesondere die sie betreffenden Personendaten löscht oder ihre Bekanntgabe an Dritte sperrt;<br><br>[1bis] Das schutzwürdige Interesse der betroffenen Person wird vermutet.<br><br>[1ter] Die Berichtigung, Vernichtung oder Löschung von Personendaten und die Sperrung der Bekanntgabe an Dritte ist ausserdem jenen Personen oder Stellen, denen die Daten zuvor bekannt gegeben worden sind, mitzuteilen, soweit dies nicht unmöglich oder mit unverhältnismässigem Aufwand verbunden ist. |
| | **§ 28a**<br>Aufsichtsrechtliche Anzeige an die Datenschutzbeauftragte oder den Datenschutzbeauftragten<br><br>[1] Jede Person hat das Recht, sich mit einer aufsichtsrechtlichen Anzeige an die Datenschutzbeauftragte oder den Datenschutzbeauftragten zu wenden, wenn sie der Ansicht ist, dass ein öffentliches Organ, eine Auftragsbearbeiterin oder ein Auftragsbearbeiter bei der Bearbeitung von sie betreffenden Personendaten gegen die datenschutzrechtlichen Vorschriften verstösst.<br><br>[2] Der anzeigenden Person kommt in diesem Verfahren keine Parteistellung zu.<br><br>[3] Die oder der Datenschutzbeauftragte informiert sie innert drei Monaten über den Stand beziehungsweise das Ergebnis der Abklärungen und die Erledigung. |
| **§ 38**<br>Stellung<br><br>[1] Die oder der Datenschutzbeauftragte erfüllt die Aufgaben weisungsunabhängig.<br><br>[2] Die Aufsichtsstelle ist organisatorisch dem Büro des Grossen Rates zugeordnet. | **§ 38**<br>Stellung und Aufsichtszuständigkeit |

| Geltendes Recht | Arbeitsversion (Stempel: 16.06.2021) |
|---|---|
| [3] Der Kontrolle durch die Datenschutzbeauftragte oder den Datenschutzbeauftragten unterstehen nicht:<br><br>a) die Mitglieder des Grossen Rates und der Grosse Rat als Behörde und<br><br>b) der Regierungsrat als Behörde. | <br><br><br><br>b) der Regierungsrat als Behörde~~.~~;<br><br>c) Datenbearbeitungen in hängigen Verfahren der Zivil- und Strafrechtspflege und<br><br>d) Datenbearbeitungen in hängigen Verfahren der Verfassungs- und Verwaltungsgerichtsbarkeit. |
| **§ 44**<br>Aufgaben<br><br>[1] Die oder der Datenschutzbeauftragte<br><br>a) kontrolliert nach einem autonom aufzustellenden Prüfprogramm die Anwendung der Bestimmungen über den Umgang mit Informationen;<br><br>b) kontrolliert vorab Bearbeitungen von Personendaten gemäss § 13;<br><br>c) berät die öffentlichen Organe in Fragen des Umgangs mit Informationen;<br><br>d) berät die betroffenen Personen über ihre Rechte;<br><br>e) vermittelt zwischen betroffenen Personen und öffentlichen Organen;<br><br>f) nimmt Stellung zu Erlassen, die für den Umgang mit Informationen oder den Datenschutz erheblich sind. | <br><br><br><br><br><br>b) ~~kontrolliert vorab Bearbeitungen von Personendaten gemäss~~ nimmt Stellung zu Rechtsetzungs- und anderen Vorhaben, die ihr oder ihm nach § 13 zur Vorabkonsultation vorzulegen sind;<br><br><br><br><br>f) ~~nimmt Stellung zu Erlassen, die für den Umgang mit Informationen oder den Datenschutz erheblich sind.~~behandelt aufsichtsrechtliche Anzeigen nach § 28a;<br><br>g) sensibilisiert die öffentlichen Organe für ihre datenschutzrechtlichen Pflichten und die Öffentlichkeit für die Anliegen des Datenschutzes und der Transparenz;<br><br>h) verfolgt die für den Schutz von Personendaten und das Öffentlichkeitsprinzip massgeblichen Entwicklungen. |

| Geltendes Recht | Arbeitsversion (Stempel: 16.06.2021) |
|---|---|
| **§ 45**<br>Kontrollbefugnisse<br><br>[1] Die oder der Datenschutzbeauftragte 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.<br><br>[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 Sachverhaltes mit.<br><br>[3] Die Berichte, welche die oder der Datenschutzbeauftragte im Rahmen der Kontrolltätigkeit erstellt, und die ihnen zugrunde liegenden Materialien sind nicht öffentlich zugänglich im Sinne von § 25 Abs. 1. | [1] Die oder der Datenschutzbeauftragte kann bei öffentlichen Organen, 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.<br><br>[2] Die öffentlichen Organe, die Auftragsdatenbearbeiterinnen und Auftragsdatenbearbeiter sowie Drittpersonen, die ~~beauftragten Dritten~~von einem öffentlichen Organ Personendaten erhalten haben, sind verpflichtet, die Aufsichtsstelle bei der Erfüllung ihrer Aufgaben zu unterstützen. Sie wirken insbesondere an der Feststellung des Sachverhaltes mit. |
| **§ 50**<br>Berichterstattung<br><br>[1] Die oder der Datenschutzbeauftragte erstattet der Wahlbehörde periodisch Bericht über Umfang und Schwerpunkte der Tätigkeiten, über wichtige Feststellungen und Beurteilungen sowie über die Wirkung des Gesetzes.<br><br>[2] Der Bericht wird veröffentlicht. | [1] Die oder der Datenschutzbeauftragte erstattet der Wahlbehörde und der Öffentlichkeit periodisch und bei Bedarf Bericht über Umfang und Schwerpunkte der Tätigkeiten, über wichtige Feststellungen und Beurteilungen sowie über die Wirkung des Gesetzes.<br><br>[2] *Aufgehoben.* |
| **§ 51**<br>Vertragswidriges Bearbeiten von Personendaten<br><br>[1] Wer als beauftragte Drittperson gemäss § 7 ohne ausdrückliche Ermächtigung des auftraggebenden öffentlichen Organs vorsätzlich oder fahrlässig Personendaten für sich oder andere verwendet oder anderen bekannt gibt, wird mit Busse bestraft. | [1] ~~Wer als beauftragte Drittperson gemäss § 7 ohne ausdrückliche Ermächtigung des auftraggebenden öffentlichen Organs vorsätzlich oder fahrlässig Personendaten für sich oder andere verwendet oder anderen bekannt gibt, wird mit~~ Mit Busse bestraft~~.~~ wird, wer: |

| Geltendes Recht | Arbeitsversion (Stempel: 16.06.2021) |
|---|---|
| | a) als Auftragsdatenbearbeiterin oder Auftragsdatenbearbeiter gemäss § 7 ohne ausdrückliche Ermächtigung des auftraggebenden öffentlichen Organs vorsätzlich oder fahrlässig Personendaten für sich oder andere verwendet oder anderen bekannt gibt oder<br><br>b) als Auftragsdatenbearbeiterin oder Auftragsdatenbearbeiter gemäss § 7 ohne vorgängige schriftliche Einwilligung des auftraggebenden öffentlichen Organs die Datenbearbeitung einer weiteren Auftragsdatenbearbeiterin und einem weiteren Auftragsdatenbearbeiter überträgt. |
| [2] Wer Personendaten, die sie oder er von einem öffentlichen Organ zum Bearbeiten zu nicht personenbezogenen Zwecken erhalten hat, vorsätzlich oder fahrlässig entgegen der Verpflichtung gemäss § 22 Abs. 4 für andere Zwecke bearbeitet oder an Dritte weitergibt, wird mit Busse bestraft. | |
| **§ 55**<br>Wirksamkeit<br><br>[1] Dieses Gesetz ist zu publizieren. Der Regierungsrat bestimmt nach Eintritt der Rechtskraft den Zeitpunkt der Wirksamkeit. [2)] | [1] ~~Dieses Gesetz~~Diese Änderung ist zu publizieren~~. Der~~; sie unterliegt dem Referendum und der Regierungsrat bestimmt ~~nach Eintritt der Rechtskraft~~ den Zeitpunkt ~~der Wirksamkeit~~des Inkrafttretens. |
| | **II.** |
| | **1.**<br>Gesetz betreffend die Organisation der Gerichte und der Staatsanwaltschaft (Gerichtsorganisationsgesetz, GOG) vom 3. Juni 2015 (Stand 1. Januar 2021) wird wie folgt geändert: |
| | **7.5 Datenschutzberatung** |
| | **§ 98a**<br><br>[1] Die Staatsanwaltschaft bezeichnet eine Datenschutzberaterin oder einen Datenschutzberater für die Staats- und Jugendanwaltschaft. |

[2)] Wirksam seit 1. 1. 2012.

| Geltendes Recht | Arbeitsversion (Stempel: 16.06.2021) |
|---|---|
| | [2] Diese Person hat die folgenden Aufgaben:<br><br>1. Sie berät und unterstützt bei der Bearbeitung von Personendaten.<br><br>2. Sie nimmt Datenschutz-Folgenabschätzungen gemäss § 12a Abs. 1 des Gesetzes über die Information und den Datenschutz (Informations- und Datenschutzgesetz, IDG) vom 9. Juni 2010 vor.<br><br>3. Sie arbeitet mit der oder dem Datenschutzbeauftragten zusammen. |
| | **2.**<br>Geoinformationsgesetz (KGeoIG) vom 16. November 2011 (Stand 1. September 2012) wird wie folgt geändert: |
| **§ 12**<br>Elektronischer Zugriff<br><br>[1] Bevor der Regierungsrat die Geodaten gemäss § 3 lit. a mittels direktem elektronischen Zugriff als öffentlich zugänglich erklärt, prüft er die daraus entstehenden möglichen Auswirkungen auf die betroffenen Personen.<br><br>[2] Bevor die Gemeinde die Geodaten gemäss § 3 lit. b mittels direktem elektronischen Zugriff als öffentlich zugänglich erklärt, prüft sie die daraus entstehenden möglichen Auswirkungen auf die betroffenen Personen.<br><br>[3] Werden die Geodaten gemäss § 3 mit Downloaddienst zugänglich gemacht, ist eine Vorabkontrolle durch die Beauftragte oder den Beauftragten für den Datenschutz gemäss § 13 des Informations- und Datenschutzgesetzes vom 9. Juni 2010 erforderlich. | [3] Werden die Geodaten gemäss § 3 mit Downloaddienst zugänglich gemacht, ist ~~eine Vorabkontrolle durch~~ vorab die ~~Beauftragte~~ oder ~~den Beauftragten für den Datenschutz~~ der Datenschutzbeauftragte gemäss § 13 des Informations- und Datenschutzgesetzes (Informations- und Datenschutzgesetz, IDG) vom 9. Juni 2010 ~~erforderlich~~zu konsultieren. |
| | **3.**<br>Gesetz über den Justizvollzug (Justizvollzugsgesetz, JVG) vom 13. November 2019 (Stand 1. Juli 2020) wird wie folgt geändert: |
| | **§ 28a**<br>Datenschutzberatung |

| Geltendes Recht | Arbeitsversion (Stempel: 16.06.2021) |
|---|---|
| | [1] Die Vollzugsbehörde bezeichnet eine Datenschutzberaterin oder einen Datenschutzberater.<br><br>[2] Diese Person hat die folgenden Aufgaben:<br><br>a) sie berät und unterstützt bei der Bearbeitung von Personendaten;<br><br>b) sie nimmt Datenschutz-Folgenabschätzungen gemäss § 12a Abs. 1 des Gesetzes über die Information und den Datenschutz (Informations- und Datenschutzgesetz, IDG) vom 9. Juni 2010 vor;<br><br>c) sie arbeitet mit der oder dem Datenschutzbeauftragten zusammen. |
| | **4.**<br>Gesetz betreffend die Kantonspolizei des Kantons Basel-Stadt (Polizeigesetz, PolG [3)]) vom 13. November 1996 (Stand 1. Januar 2021) wird wie folgt geändert: |
| **§ 57**<br>Grundsatz<br><br>[1] Für Akten der Kantonspolizei gelten die Bestimmungen über das Amtsgeheimnis, den Datenschutz und die Akteneinsicht.<br><br>[2] Die Bearbeitung und Weitergabe von Personendaten durch die Kantonspolizei sowie das Einsichtsrecht in polizeiliche Datensammlungen richten sich nach den Bestimmungen der Datenschutzgesetzgebung und im interkantonalen sowie internationalen Verkehr nach den Bestimmungen der Bundesgesetzgebung sowie der internationalen Rechtshilfeabkommen.<br><br>[3] Polizeilich relevante Informationen dürfen weitergegeben werden, sofern diese der Gefahrenabwehr oder dem Schutz der Polizeigüter dient.<br><br>[4] Die Kantonspolizei führt die zur recht- und zweckmässigen Erfüllung ihrer Aufgaben notwendigen Datensammlungen. | |

[3)] Titel: Abkürzung redaktionell ergänzt.

| Geltendes Recht | Arbeitsversion (Stempel: 16.06.2021) |
|---|---|
| | [5] Die Kantonspolizei darf besondere Personendaten bearbeiten sowie Profiling vornehmen, soweit es zur Erfüllung ihrer gesetzlichen Aufgaben zwingend notwendig ist. |
| | **§ 57a**<br>Datenschutzberatung<br><br>[1] Die Kantonspolizei bezeichnet eine Datenschutzberaterin oder einen Datenschutzberater.<br><br>[2] Diese Person hat die folgenden Aufgaben:<br><br>a) sie berät und unterstützt bei der Bearbeitung von Personendaten;<br><br>b) sie nimmt Datenschutz-Folgenabschätzungen gemäss § 12a Abs. 1 des Gesetzes über die Information und den Datenschutz (Informations- und Datenschutzgesetz, IDG) vom 9. Juni 2010 vor;<br><br>c) sie arbeitet mit der oder dem Datenschutzbeauftragten zusammen. |
| | **5.**<br>Finanz- und Verwaltungskontrollgesetz (FVKG) vom 17. September 2003 (Stand 1. Juli 2016) wird wie folgt geändert: |
| **§ 22**<br>Dokumentation und Datenzugriff<br><br>[1] Beschlüsse und Verfügungen des Grossen Rats, der Regierung, der Gerichte, der Departemente und der Dienststellen sowie der selbständigen öffentlich-rechtlichen und privatrechtlichen Anstalten, die den Finanzhaushalt des Kantons betreffen, sind der Finanzkontrolle zugänglich zu machen. | |

| Geltendes Recht | Arbeitsversion (Stempel: 16.06.2021) |
|---|---|
| [2] Die Finanzkontrolle hat das Recht, die für die Wahrnehmung der Finanzaufsicht erforderlichen Personendaten aus den Datensammlungen der Departemente und Dienststellen, der Gerichte sowie der selbständigen öffentlich-rechtlichen und privatrechtlichen Anstalten abzurufen. Soweit die Daten für die Aufgabenerfüllung geeignet und erforderlich sind, erstreckt sich das Zugriffsrecht auch auf besonders schützenswerte Personendaten. Die Finanzkontrolle unterliegt dabei der gleichen Geheimhaltungspflicht wie die geprüfte Stelle. Die Finanzkontrolle darf die ihr derart zur Kenntnis gebrachten Personendaten nur bis zum Abschluss des Revisionsverfahrens aufbewahren oder speichern. Die Zugriffe auf die verschiedenen Datensammlungen und die damit verfolgten Zwecke müssen dokumentiert sein. | [2] Die Finanzkontrolle hat das Recht, die für die Wahrnehmung der Finanzaufsicht erforderlichen Personendaten aus den Datensammlungen der Departemente und Dienststellen, der Gerichte sowie der selbständigen öffentlich-rechtlichen und privatrechtlichen Anstalten abzurufen. Soweit die Daten für die Aufgabenerfüllung geeignet und erforderlich sind, erstreckt sich das Zugriffsrecht auch auf ~~besonders schützenswerte~~besondere Personendaten. Die Finanzkontrolle unterliegt dabei der gleichen Geheimhaltungspflicht wie die geprüfte Stelle. Die Finanzkontrolle darf die ihr derart zur Kenntnis gebrachten Personendaten nur bis zum Abschluss des Revisionsverfahrens aufbewahren oder speichern. Die Zugriffe auf die verschiedenen Datensammlungen und die damit verfolgten Zwecke müssen dokumentiert sein. |
| | **6.**<br>Gesetz über die direkten Steuern (Steuergesetz, StG) vom 12. April 2000 (Stand 1. Januar 2021) wird wie folgt geändert: |
| **§ 141a**<br><br>[1] Die Steuerverwaltung betreibt zur Erfüllung ihrer Aufgaben ein Informationssystem. Dieses kann auch besonders schützenswerte Personendaten über administrative und strafrechtliche Sanktionen enthalten, die steuerrechtlich wesentlich sind.<br><br>[1bis] Die Steuerverwaltung ist berechtigt, die Versichertennummer der Alters- und Hinterlassenenversicherung nach den Bestimmungen des Bundesgesetzes vom 20. Dezember 1946 über die Alters- und Hinterlassenenversicherung für die Erfüllung ihrer gesetzlichen Aufgaben systematisch zu verwenden.<br><br>[2] Zur Gewährung der Amtshilfe im Sinne der §§ 139 bis 141 können Daten einzeln, auf Listen oder auf elektronischen Datenträgern übermittelt werden. Sie können auch mittels eines Abrufverfahrens zugänglich gemacht werden.<br><br>[3] Bei Amtshilfe unter oder an Steuerbehörden sind alle diejenigen Daten von Steuerpflichtigen kostenlos weiterzugeben, die zur Veranlagung und Erhebung der Steuern dienen können, namentlich:<br><br>a) die Personalien; | [1] Die Steuerverwaltung betreibt zur Erfüllung ihrer Aufgaben ein Informationssystem. Dieses kann auch ~~besonders schützenswerte~~besondere Personendaten über administrative und strafrechtliche Sanktionen enthalten, die steuerrechtlich wesentlich sind. |

| Geltendes Recht | Arbeitsversion (Stempel: 16.06.2021) |
|---|---|
| b) Angaben über den Zivilstand, den Wohn- und Aufenthaltsort, die Aufenthaltsbewilligung und die Erwerbstätigkeit;<br><br>c) Rechtsgeschäfte;<br><br>d) Leistungen des Gemeinwesens.<br><br>[4] Im Übrigen sind, soweit dieses Gesetz keine abweichenden Vorschriften enthält, die Bestimmungen des kantonalen Informations- und Datenschutzgesetzes sinngemäss anwendbar. | |
| | **7.**<br>Gesetz über die Industriellen Werke Basel (IWB-Gesetz) vom 11. Februar 2009 (Stand 1. Juli 2020) wird wie folgt geändert: |
| **§ 35a**<br><br>[1] Die IWB sind berechtigt, mit Hilfe intelligenter, fernauslesbarer Messeinrichtungen (Smart Meter) Personendaten ohne Einwilligung der betroffenen Personen zu bearbeiten, soweit dies erforderlich ist für<br><br>a) die Lieferung von Energie und Wasser (insbesondere für die Erstellung von Verbrauchsprognosen, Bilanzgruppenmeldungen, Leistungsnominationen, die Energiebeschaffung und das Portfoliomanagement);<br><br>b) die Messung des Energie- und Wasserverbrauchs, der Energieproduktion und der Einspeisemenge;<br><br>c) die Abrechnung des Energie- und Wasserverbrauchs und die Vergütung von Einspeisemengen;<br><br>d) die Ermittlung des Netzzustandes und die Sicherstellung sicherer, effizienter und leistungsstarker Netze;<br><br>e) das Auffinden und Unterbinden von Leistungserschleichungen. | |

| Geltendes Recht | Arbeitsversion (Stempel: 16.06.2021) |
|---|---|
| [2] Die IWB sind zudem berechtigt, mit Einwilligung der betroffenen Personen Personendaten zum Zwecke der Entwicklung und Bereitstellung von Energiedienstleistungen zu bearbeiten.<br><br>[3] Die Einzelheiten der Datenbearbeitung gemäss Abs. 1 und 2 werden in vom Verwaltungsrat zu erlassenden und vom Regierungsrat zu genehmigenden Ausführungsbestimmungen für jedes Medium (Elektrizität, Erdgas, Fernwärme und Wasser) separat geregelt. Diese Ausführungsbestimmungen zur Datenbearbeitung sind der oder dem kantonalen Datenschutzbeauftragten im Rahmen eines Vorabkontrollverfahrens vorzulegen.<br><br>[4] Ausserhalb ihres öffentlichen Auftrags sind die IWB überdies berechtigt, über die Schnittstellen am Smart Meter Personendaten zu bearbeiten, wenn und soweit die betroffene Person sie dazu beauftragt und nach angemessener Information über den Zweck und Inhalt der Datenbearbeitung darin schriftlich eingewilligt hat. Die IWB haben ausserdem sicherzustellen, dass die erhobenen Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden.<br><br>[5] Die mit Smart Meter erhobenen Personendaten und Persönlichkeitsprofile sind nach zwölf Monaten zu vernichten, sofern sie nicht abrechnungsrelevant oder anonymisiert sind oder die betroffene Person in eine längere Aufbewahrung einwilligt. Vorbehalten bleibt das Bundesrecht. | [3] Die Einzelheiten der Datenbearbeitung gemäss Abs. 1 und 2 werden in vom Verwaltungsrat zu erlassenden und vom Regierungsrat zu genehmigenden Ausführungsbestimmungen für jedes Medium (Elektrizität, Erdgas, Fernwärme und Wasser) separat geregelt. Diese Ausführungsbestimmungen zur Datenbearbeitung sind der oder dem kantonalen Datenschutzbeauftragten im Rahmen ~~eines Vorabkontrollverfahrens~~einer Vorabkonsultation vorzulegen. |
| | **8.**<br>Gesetz betreffend die Tagesbetreuung von Kindern (Tagesbetreuungsgesetz) vom 17. September 2003 (Stand 1. Januar 2016) wird wie folgt geändert: |
| **§ 15**<br>Datenbearbeitung<br><br>[1] Für die Bearbeitung der Daten, einschliesslich besonders schützenswerter Personendaten, ist das Gesetz über die Harmonisierung und Koordination von bedarfsabhängigen Sozialleistungen im Kanton Basel-Stadt vom 25. Juni 2008 (Harmonisierungsgesetz Sozialleistungen) massgebend. | [1] Für die Bearbeitung der Daten, einschliesslich ~~besonders schützenswerter~~ besonderer Personendaten, ist das Gesetz über die Harmonisierung und Koordination von bedarfsabhängigen Sozialleistungen im Kanton Basel-Stadt (Harmonisierungsgesetz Sozialleistungen, SoHaG) vom 25. Juni 2008 ~~(Harmonisierungsgesetz Sozialleistungen)~~ massgebend. |
| | **9.** |

| Geltendes Recht | Arbeitsversion (Stempel: 16.06.2021) |
|---|---|
| | Gesetz über die Harmonisierung und Koordination von bedarfsabhängigen Sozialleistungen (Harmonisierungsgesetz Sozialleistungen, SoHaG) vom 25. Juni 2008 (Stand 1. Juli 2015) wird wie folgt geändert: |
| **§ 25**<br>Bekanntgabe von Daten aus der zentralen Datenbank für statistische und weitere nicht personenbezogene Zwecke<br><br>[1] Die Bekanntgabe von Daten an die zentrale Statistikstelle des Kantons richtet sich nach den Bestimmungen des Gesetzes über die öffentliche Statistik (StatG) vom 21. Mai 2014.<br><br>[2] Die Bekanntgabe von Daten für einen nicht personenbezogenen Zweck, namentlich für Planung, Wissenschaft und Forschung, an andere öffentliche Organe im Kanton sowie an öffentliche Organe in anderen Kantonen oder des Bundes richtet sich nach § 22 IDG.<br><br>[3] Die Bekanntgabe von Daten an Private kann zum Zweck der Wissenschaft und Forschung ausschliesslich in anonymisierter Form erfolgen.<br><br>[4] Anfragen für die Bekanntgabe von Daten sind an das für die zentrale Datenbank zuständige Organ gemäss § 13 dieses Gesetzes zu richten. | [2] Die Bekanntgabe von Daten für einen nicht personenbezogenen Zweck, namentlich für Planung~~, Wissenschaft~~ und Forschung, an andere öffentliche Organe im Kanton sowie an öffentliche Organe in anderen Kantonen oder des Bundes richtet sich nach § 22 IDG.<br><br>[3] Die Bekanntgabe von Daten an Private kann zum Zweck der ~~Wissenschaft und~~ Forschung ausschliesslich in anonymisierter Form erfolgen. |
| | **III.** |
| | *Keine Aufhebung anderer Erlasse.* |
| | **IV.** |
| | Diese Änderung ist zu publizieren; sie unterliegt dem Referendum und der Regierungsrat bestimmt den Zeitpunkt des Inkrafttretens.<br><br>[Behörde] |