PD/P241328

Erläuterungen zur Änderung der Verordnung über die Information und den Datenschutz vom 9. August 2011 (Informations- und Datenschutzverordnung, IDV; SG 153.270)

Inhalt

1. Ausgangslage

Der Grosse Rat hat am 20. Oktober 2022 eine umfassende Revision des Gesetzes über die Information und den Datenschutz vom 9. Juni 2010 (Informations- und Datenschutzgesetz, IDG) und weiterer Gesetze beschlossen. Diese Gesetzesanpassung geht ihrerseits weitgehend auf Reformen von datenschutzrechtlichen Erlassen des Europarates und der Europäischen Union zurück, zu deren Umsetzung die Schweiz verpflichtet ist:

- Der Europarat hat 2016 die Konvention zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten[1] modernisiert. Am 18. Mai 2018 hat das Ministerkomitee das Protokoll zur Änderung dieses Übereinkommens[2] beschlossen. Die Bundesversammlung hat das Protokoll am 19. Juni 2020 genehmigt[3]. Dadurch wurden Bund und Kantone verpflichtet, den Minimalstandard gemäss dem revidierten Übereinkommen in ihrem Recht umzusetzen.
- Die EU-Datenschutz-Richtlinie 2016/680[4] regelt das Datenbearbeiten im Rahmen der justiziellen und polizeilichen Zusammenarbeit. Sie wurde als Schengen-relevant erklärt und der Schweiz am 1. August 2016 notifiziert. Aufgrund des Schengen-Assoziierungsabkommens[5] muss diese Richtlinie auf Bundes- und kantonaler Ebene umgesetzt werden.

Nicht zur Umsetzung verpflichtet ist die Schweiz bezüglich der EU-Datenschutz-Grundverordnung 2016/679[6] (DSGVO). Allerdings sieht Art. 45 DSGVO vor, dass Datenübermittlungen in Drittstaaten nur dann ohne weiteres zulässig sind, wenn dieser Drittstaat ein angemessenes Datenschutzniveau bietet. Die EU-Kommission fällt entsprechende Angemessenheitsbeschlüsse aufgrund einer Evaluation des Rechts des Bundes und der Kantone. Da ein solcher Angemessenheitsbeschluss für die Schweiz von grosser Bedeutung ist, war bei dem Revisionsprojekt auch der DSGVO die nötige Beachtung zu schenken.

Zur Erfüllung dieses gesetzgeberischen Auftrages hat der Regierungsrat am 29. September 2021 dem Grossen Rat einen 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) (21.1239.01; im Weiteren «Ratschlag Änderung IDG») vorgelegt. Der Grosse Rat beauftragte seinerseits die Justiz-, Sicherheits- und Sportkommission (JSSK) mit der Berichterstattung zu dem Reformprojekt. Die JSSK legte ihren Bericht zum Ratschlag zu einer Änderung des Gesetzes über die Information und Datenschutz vom 9. Juni 2010 (Informations- und Datenschutzgesetz, IDG) und weiterer Gesetze (Anpassung an die europäischen Datenschutzreformen und weitere Anpassungen) sowie zum Anzug Thomas Gander und Konsorten zur Schaffung von rechtlichen Grundlagen für die Anwendung von algorithmus-basierter Instrumente in der Polizeiarbeit (21.1239.02; im Weiteren «Bericht JSSK») am 15. September 2022 vor.

Die vom Grossen Rat beschlossenen Änderungen des IDG bedingen eine Reihe von Anpassungen der zugehörigen Verordnung über die Information und den Datenschutz vom 9. August 2011 (Informations- und Datenschutzverordnung, IDV; SG 153.270). Der Regierungsrat setzt daher die Änderung des IDG vom 20. Oktober 2022 zusammen mit der vorliegenden Revision der IDV in Kraft.

Zugleich wird eine Anpassung der IDV vorgenommen, welche sich aufgrund von Erfahrungen in der Rechtsanwendung der letzten Jahre ergeben hat: Neu wird der Anwendungsbereich der Bestimmungen über die Klassifizierung von Informationen auf die Berichte und Beschlussentwürfe der Departemente zuhanden des Regierungsrates eingegrenzt, da sich in der Praxis gezeigt hat, dass eine generelle Klassifizierungspflicht weder nötig noch umsetzbar ist.

---

[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] 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.
[5] Abkommen vom 26. Oktober 2004 zwischen der Schweizerischen Eidgenossenschaft, der Europäischen Union und der Europäischen Gemeinschaft über die Assoziierung dieses Staates bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands, SR 0.362.31.
[6] 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.

2. Erläuterungen zu den einzelnen Bestimmungen

2.1 Rechtliche Grundlagen von Datenpools (§ 1b IDV; geändert)

Informations- und Datenschutzverordnung vom 9. August 2011	**Änderungen**
§ 1b Rechtliche Grundlagen	**§ 1b Rechtliche Grundlagen**
[1] Zugriffe auf den Informationsbestand eines Datenpools setzen das Vorhandensein von rechtlichen Grundlagen nach den Vorgaben von § 9 und § 21 IDG voraus.	[1] *unverändert*
[2] Für die Errichtung, den Betrieb und die Organisation eines Datenpools sind rechtliche Grundlagen mindestens auf Verordnungsstufe zu schaffen.	[2] *unverändert*
[3] Sie regeln insbesondere	[3] Sie regeln insbesondere:
a) den Zweck des Datenpools,	a) den Zweck des Datenpools;
b) den Inhalt des Datenpools,	b) den Inhalt des Datenpools;
c) das verantwortliche Organ und dessen Aufgaben (§ 6 Abs. 2 IDG),	c) das ~~verantwortliche~~ öffentliche Organ, das die Gesamtverantwortung trägt, und dessen Aufgaben (§ 6 Abs. 2 IDG);
d) die Rechte und Pflichten der informationenliefernden öffentlichen Organe und/oder Dritten,	d) die Rechte und Pflichten der informationenliefernden öffentlichen Organe ~~und/~~oder Dritten;
e) die Rechte und Pflichten der informationenbeziehenden öffentlichen Organe und/oder Dritten,	e) die Rechte und Pflichten der informationenbeziehenden öffentlichen Organe ~~und/~~oder Dritten;
f) den Umgang mit nicht mehr benötigten Informationen,	f) den Umgang mit nicht mehr benötigten Informationen;
g) die Vorgaben für eine Übertragung der Bearbeitung auf Dritte (§ 7 IDG),	g) die Vorgaben für eine Übertragung der Bearbeitung auf Dritte (§ 7 IDG);
h) die Auflösung des Datenpools unter Beachtung von § 1c dieser Verordnung.	h) die Auflösung des Datenpools unter Beachtung von § 1c dieser Verordnung.

Erläuterungen

Der geänderte § 6 Abs. 2 IDG verlangt neu, dass mehrere öffentliche Organe, die einen gemeinsamen Informationsbestand bearbeiten, festlegen müssen, welches öffentliche Organ die Gesamtverantwortung trägt. Da Datenpools im Sinne von § 1a IDV in der Regel von mehrere öffentlichen Organen bearbeitet werden, sind die in § 1b IDV genannten Anforderungen an die rechtliche Grundlage eines Datenpools entsprechend anzupassen.

In § 1b Abs. 3 lit. d und e IDV wird eine redaktionelle Anpassung, gestützt auf den Rechtsetzungsleitfaden des Kantons Basel-Stadt vom April 2022, vorgenommen («oder» statt «und/oder»). Inhaltlich ändert sich durch diese Anpassung nichts.

2.2 Nachweis für die Einhaltung der Datenschutzbestimmungen (§ 1d IDV; neu)

Informations- und Datenschutzverordnung vom 9. August 2011	Änderungen
	I.1b. Nachweis für die Einhaltung der Datenschutzbestimmungen **§ 1d Dokumentation** [1] Der Nachweis für die Einhaltung der Datenschutzbestimmungen (§ 6 Abs. 3 IDG) wird durch eine Dokumentation erbracht und umfasst: a) eine Beschreibung der Bearbeitung der Personendaten; b) eine Darstellung der Rechtslage; c) eine Beschreibung der Risiken und Abhilfemassnahmen; d) eine Beschreibung der Prozesse und Verantwortlichkeiten. [2] Die Dokumentation kann in einem strukturierten Datenschutz- oder Informationssicherheits-Managementsystem erfolgen.

Erläuterungen

§ 6 Abs. 3 IDG verlangt neu, dass öffentliche Organe nachweisen können müssen, dass sie die Bestimmungen des Datenschutzgesetzes einhalten. Der Nachweis erfolgt in Form einer Dokumentation, deren Mindestgehalt nun in § 1d Abs. 1 definiert wird.

Die Dokumentation umfasst erstens eine Beschreibung der Bearbeitung von Personendaten. Es soll verständlich beschrieben werden, welche «gewöhnlichen» oder besonderen Personendaten (und welche Personendaten, die einem Berufs- oder Amtsgeheimnis unterstehen) von wem zu welchem Zweck bearbeitet werden. Insbesondere sollen die Datenflüsse ersichtlich sein. Zweitens enthält die Dokumentation eine Darstellung der Rechtslage. Es ist aufzuzeigen, dass die jeweilige Datenbearbeitung (Erheben, Weiterbearbeiten, Bekanntgeben, Aufbewahren, Archivieren oder Vernichten von Daten) rechtmässig ist. Das ist vor allem bei bloss mittelbaren gesetzlichen Grundlagen (§ 9 Abs. 1 und 2, jeweils lit. b IDG) wichtig. Drittens sind die Risiken für die Grundrechte der betroffenen Personen, insbesondere für den Anspruch auf informationelle Selbstbestimmung, sowie die getroffenen Abhilfemassnahmen zu nennen. Viertens sind die Prozesse darzustellen, mittels welchen sichergestellt wird, dass die anwendbaren Bestimmungen des IDG eingehalten werden, beispielsweise Erteilung und Entzug von Zugriffsberechtigungen, Einhaltung der Archivierungs- und Vernichtungspflichten, Behandlung von Datenschutzverletzungen, Gewährung der Rechte der betroffenen Personen etc. Zudem sind die Verantwortlichkeiten bei diesen Prozessen zu benennen.

Der Nachweis kann in einer separaten Dokumentation, in einem Datenschutz-Managementsystem (DSMS) oder in einem um Datenschutzaspekte angereicherten Informationssicherheits-Managementsystem (ISMS) erbracht werden. Insbesondere bei grösseren Datenbearbeitungssystemen oder Systemen mit besonders heiklen oder schutzwürdigen Daten ist es aus Compliance-Gründen unumgänglich, die Einhaltung von Informationssicherheit und Datenschutz mit einem Informationssicherheits- und Datenschutz-Managementsystem zu kontrollieren. Solche Managementsysteme sind digitale Organisations-Tools, mit denen die Umsetzung gesetzlicher Anforderungen systematisch geplant, organisiert, gesteuert und kontrolliert werden. Mit «strukturiert» wird ausgedrückt, dass es sich um ein methodisches, fachliches System handeln muss. Diese Managementsysteme basieren auf den ISO-Standards des Qualitätsmanagements (ISO 9001) und der Informationssicherheit (ISO 27001 usw.) und/oder Frameworks (BSI, COBIT usw.). Der Kanton erfasst seine

Datenbearbeitungssysteme in einem Informationssicherheits-Managementsystem, welches zur Umsetzung der neuen, mit der Änderung des IDG vom 20. Oktober 2022 hinzugekommenen Anforderungen um die entsprechenden Aspekte des Datenschutzes erweitert wird. In der IDV soll vorerst nur festgelegt werden, dass der Nachweis der Datenschutzkonformität mit einem solchen System erbracht werden *kann*.

Vgl. auch die Übergangsbestimmung in § 35a IDV.

2.3 Hohes Risiko (§ 2 IDV; geändert)

Informations- und Datenschutzverordnung vom 9. August 2011	**Änderungen**
I. 2. Vorabkontrolle (§ 13 IDG) **§ 2 Pflicht zur Vorlage zur Vorabkontrolle** [1] Das Vorhaben der Bearbeitung von Personendaten unterliegt insbesondere dann der Vorabkontrolle durch die oder den Datenschutzbeauftragen: a) wenn sie ein Abrufverfahren vorsieht, b) wenn sie besondere Personendaten betrifft, c) wenn sie mit dem Einsatz neuer Technologie verbunden ist, d) wenn sie eine grosse Anzahl Personen betrifft, e) wenn ein Datenpool im Sinn von § 1a errichtet werden soll, oder f) wenn ein Gesetz oder eine Verordnung es vorsieht.	~~***I. 2. Vorabkontrolle (§ 13 IDG)***~~ ~~**§ 2 Pflicht zur Vorlage zur Vorabkontrolle**~~ ~~[1] Das Vorhaben der Bearbeitung von Personendaten unterliegt insbesondere dann der Vorabkontrolle durch die oder den Datenschutzbeauftragen:~~ ~~a. wenn sie ein Abrufverfahren vorsieht,~~ ~~b. wenn sie besondere Personendaten betrifft,~~ ~~c. wenn sie mit dem Einsatz neuer Technologie verbunden ist,~~ ~~d. wenn sie eine grosse Anzahl Personen betrifft,~~ ~~e. wenn ein Datenpool im Sinn von § 1a errichtet werden soll, oder~~ ~~f. wenn ein Gesetz oder eine Verordnung es vorsieht.~~ ~~[2] Ein Vorhaben muss nicht zur Vorabkontrolle vorgelegt werden, wenn die oder der Datenschutzbeauftragte bereits in der Projektorganisation des Vorhabens mitwirkt.~~ **I. 2. <u>Datenschutz-Folgeabschätzung und Vorabkonsultation (§§ 12a und 13 IDG)</u>** **§ 2 <u>Hohes Risiko</u>** [1] <u>Ein hohes Risiko für die Grundrechte der betroffenen Personen im Sinn von § 12a Abs. 1 und § 13 Abs. 1 lit. b IDG liegt insbesondere vor, wenn ein Vorhaben zur Bearbeitung von Personendaten:</u> a) <u>ein Abrufverfahren vorsieht;</u> b) <u>besondere Personendaten oder Personendaten, die einem Berufs- oder Amtsgeheimnis unterstehen, betrifft;</u> c) <u>ein Profiling umfasst;</u> d) <u>eine grosse Anzahl von Personen betrifft;</u> e) <u>eine Auftragsdatenbearbeitung durch Dritte im Ausland in einem Staat ohne angemessenen Datenschutz umfasst oder</u> f) <u>die Errichtung eines Datenpools im Sinn von § 1a umfassen soll.</u> [2] *aufgehoben*

[2] Ein Vorhaben muss nicht zur Vorabkontrolle vorgelegt werden, wenn die oder der Datenschutzbeauftragte bereits in der Projektorganisation des Vorhabens mitwirkt.	

Erläuterungen

Bei neuen Vorhaben zu Personendatenbearbeitungen muss das verantwortliche öffentliche Organ gemäss der neuen Bestimmung von § 12a Abs. 1 IDG in einem ersten Schritt prüfen, ob voraussichtlich ein hohes Risiko für die Grundrechte, d.h. eine hohe Wahrscheinlichkeit einer Grundrechtsverletzung der betroffenen Personen besteht. Ergibt diese sogenannte Schwellwertanalyse, dass voraussichtlich ein hohes Risiko für die Grundrechte der betroffenen Personen besteht, ist in einem zweiten Schritt eine Datenschutz-Folgeabschätzung (DSFA) durchzuführen (§ 12a Abs. 2 IDG). Führt die DSFA zum Ergebnis, dass ein hohes Risiko gegeben ist, muss das verantwortliche öffentliche Organ in einem dritten Schritt das Vorhaben der oder dem Datenschutzbeauftragten zur Vorabkonsultation gemäss dem neu gefassten § 13 Abs. 1 lit. b IDG vorlegen.

Die Vorabkonsultation ersetzt die frühere Vorabkontrolle. Der bisherige § 2 IDV umfasste eine (nicht abschliessende) Liste von alternativen Anlasstatbeständen, bei deren Vorliegen eine Vorabkontrolle vorzunehmen war. Schon die Vorabkontrolle musste durchgeführt werden, wenn aufgrund gewisser Indikatoren abzusehen war, dass besondere Gefahren für die Grundrechte der Betroffenen drohten. Daher kann für die Konkretisierung des in diesem Zusammenhang zentralen Begriffs des hohen Risikos gemäss § 12a Abs. 1 und 2 und § 13 Abs. 1 lit. b IDG im neuen § 2 IDV teilweise auf den Anlass-Katalog der Vorabkontrolle im bisherigen § 2 IDV zurückgegriffen werden.

Gemäss Ratschlag IDG ist dabei zu beachten, dass unter «Vorhaben», die einer DSFA zu unterziehen sind (und eventuell zur Vorabkonsultation der oder des Datenschutzbeauftragten nach § 13 IDG führen), nicht einzelne, konkrete Bearbeitungen wie beispielsweise eine Einzelbekanntgabe von Personendaten zu verstehen sind, 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.[7]

Ein hohes Risiko für die Grundrechte der Betroffenen besteht gemäss § 2 lit. a IDV erstens bei einer Datenbearbeitung, die ein Abrufverfahren vorsieht. Dabei ermöglicht ein öffentliches Organ einer anderen Stelle oder Privaten Zugriffe auf einen eigenen Informationsbestand mit Personendaten. Charakteristisch für Abrufverfahren ist, dass die Daten nach dem «Selbstbedienungsprinzip» bezogen werden können. Das bedeutet, dass das bekanntgebende öffentliche Organ im Einzelfall nicht mehr prüfen kann, ob die Voraussetzungen für die Bekanntgabe erfüllt sind. Dies birgt ein gesteigertes Risiko für den Verlust der Vertraulichkeit der Personendaten.

Zweitens liegt der wohl wesentlichste Fall einer Datenbearbeitung, welche ein hohes Risiko für die Grundrechte der Betroffenen mit sich bringt, bei der Bearbeitung von besonderen Personendaten vor. Dies hielt in Bezug auf die Vorabkontrolle schon der bisherige § 2 Abs. 1 lit. b IDV fest. Zu einem hohen Risiko für die betroffenen Personen führt auch das Bearbeiten von Personendaten, die einem Berufs- oder Amtsgeheimnis unterstehen. Dabei handelt es sich in vielen Fällen um besondere Personendaten. Keine besonderen Personendaten sind aber beispielsweise Steuerdaten, für welche das Steuergeheimnis dennoch einen besonderen Schutz vorsieht, der die Aufnahme in den Tatbestandskatalog von § 2 IDV rechtfertigt. Bereits heute werden solche Daten bei der Schutzbedarfsanalyse wie besondere Personendaten behandelt, weil letztlich die gleichen Massnahmen zu einer Risikominderung oder -vermeidung führen.

[7] Ratschlag IDG, S. 23

Da neu in § 9 Abs. 2 IDG die Vornahme eines Profilings auf dieselbe Gefahrenstufe wie die Bearbeitung von besonderen Personendaten gestellt wird, ist drittens in § 2 lit. c IDV festzuhalten, dass auch das Profiling zu einem hohen Risiko führt, das eine Vorabkonsultationspflicht nach sich zieht.

Viertens ist auch von einem hohen Risiko für die Grundrechte auszugehen, wenn eine Datenbearbeitung eine grosse Anzahl von Personen betrifft. Auch für diesen Fall sah der bisherige § 2 Abs. 1 IDV in lit. d bereits die Vornahme einer Vorabkontrolle vor. Eine «grosse Zahl» meint praxisgemäss 10'000 oder mehr Personen. Zu beachten wird sein, dass das öffentliche Organ schon bei einer kleineren Zahl in einer Datenschutz-Folgenabschätzung prüfen muss, ob das Risiko für die Betroffenen durch Schutzmassnahmen zu verringern ist. Allerdings sind diese Projekte dann nicht der oder dem Datenschutzbeauftragten zu unterbreiten.

Auch wenn fünftens eine Auftragsdatenbearbeitung durch Dritte im Ausland in einem Staat vorgesehen ist, welcher kein angemessenes Niveau im Bereich des Datenschutzes erreicht, kann ein hohes Risiko für die Grundrechte der Betroffenen entstehen, das durch entsprechende Massnahmen zu vermeiden oder zu verringern ist. Auch in diesem Fall ist ein Vorhaben der oder dem Datenschutzbeauftragten zur Vorabkonsultation vorzulegen (§ 2 Abs. 1 lit. e IDV). Zur Bestimmung solcher Staaten kann das öffentliche Organ auf die Liste der Staaten, Gebiete, spezifischen Sektoren in einem Staat und internationalen Organisationen in Anhang 1 der Verordnung des Bundesrates über den Datenschutz vom 31. August 2022 (SR 235.11) abstellen (siehe auch § 11).

Wie im bisherigen § 2 IDV wird sechstens die Errichtung eines Datenpools im Sinne von § 1a IDV im Tatbestandskatalog aufgeführt. Datenpools stellen ein erhöhtes Risiko für die Grundrechte von betroffenen Personen dar, da die datenschutzrechtliche Verantwortung teilweise auf mehrere öffentliche Organe verteilt ist. Vorzulegen ist das Vorhaben, das die Schaffung eines Datenpools vorsieht, durch das öffentliche Organ, das die Gesamtverantwortung trägt (§ 1b Abs. 3 lit. c IDV).

Nicht mehr separat erwähnt werden muss in der IDV, dass eine Vorabkonsultationspflicht auch besteht, wenn sie spezialgesetzlich (in einem Gesetz oder in einer Verordnung) vorgesehen ist.

Aufgrund des übergeordneten internationalen Rechts, welches bei bestimmten Vorhaben eine Vorabkonsultation zwingend vorschreibt, muss der Ausnahmetatbestand des bisherigen § 2 Abs. 2 IDV aufgehoben werden (vgl. Ratschlag Änderung IDG, Kommentierung zu § 13 IDG).

2.4 Zeitpunkt und Durchführung der Vorabkonsultation (§ 3 IDV; geändert)

Informations- und Datenschutzverordnung vom 9. August 2011	**Änderungen**
§ 3 Zeitpunkt und Durchführung der Vorabkontrolle	**§ 3 Zeitpunkt und Durchführung der ~~Vorabkontrolle~~Vorabkonsultation**
[1] Die erste Kontaktaufnahme mit der oder dem Datenschutzbeauftragten erfolgt zu einem Zeitpunkt, welcher die Berücksichtigung ihrer oder seiner Beurteilung im Vorhaben ermöglicht.	[1] Die erste Kontaktaufnahme mit der oder dem Datenschutzbeauftragten erfolgt zu einem Zeitpunkt, welcher die Berücksichtigung ihrer oder seiner ~~Beurteilung~~ Empfehlungen aus der Vorabkonsultation im Rechtsetzungsprojekt beziehungsweise Vorhaben ermöglicht.
[2] Die Vorabkontrolle findet je nach Grösse des Vorhabens in einem Prüfungsschritt oder in mehreren Prüfungsschritten statt.	[2] Die ~~Vorabkontrolle~~ Vorabkonsultation findet je nach Grösse des Rechtsetzungsprojekts beziehungsweise Vorhabens in einem Prüfungsschritt oder in mehreren Prüfungsschritten statt.

[3] Die oder der Datenschutzbeauftragte nimmt den jeweiligen Prüfungsschritt innert angemessener Frist vor und teilt dem öffentlichen Organ das entsprechende Prüfungsergebnis mit.	[3] *unverändert*

Erläuterungen

Im Rahmen der neuen Vorabkonsultation gemäss § 13 IDG, welche an die Stelle der bisherigen Vorabkontrolle tritt, ist die oder der Datenschutzbeauftragte nicht mehr nur bei Bearbeitungen bzw. Vorhaben zur Bearbeitung von Personendaten einzubeziehen, sondern auch bei Rechtsetzungsprojekten, die das Bearbeiten von Personendaten betreffen oder die für den Umgang mit Informationen erheblich sind. Die ersten beiden Absätze von § 3 IDV sind entsprechend anzupassen und zu ergänzen.

2.5 Inhalt der vorzulegenden Dokumentation (§ 4; geändert)

Informations- und Datenschutzverordnung vom 9. August 2011	**Änderungen**
§ 4 Inhalt der vorzulegenden Dokumentation	**§ 4 Dokumentation bei Vorhaben zur Bearbeitung von Personendaten**
[1] Die vom öffentlichen Organ der oder dem Datenschutzbeauftragten vorzulegende Dokumentation enthält alle für die Beurteilung relevanten Unterlagen, insbesondere:	[1] ~~Die vom öffentlichen~~ Betrifft die Vorabkonsultation ein Vorhaben zur Bearbeitung von Personendaten, legt das öffentliche Organ der oder dem Datenschutzbeauftragten ~~vorzulegende~~ eine Dokumentation ~~enthält~~ vor, die alle für die Beurteilung relevanten Unterlagen enthält, insbesondere:
a) eine Beschreibung des Vorhabens, b) die Darstellung der Rechtslage und c) eine Übersicht über die Massnahmen zur Verhinderung von Persönlichkeitsverletzungen.	a)−c) *unverändert*

Erläuterungen

Schon das bisherige Recht regelte in § 4 IDV den Inhalt der Dokumentation, die der oder dem Datenschutzbeauftragten im Rahmen der Vorabkontrolle vorzulegen war. Diese Regelung kann für vorabkonsultationspflichtige Vorhaben im Sinne von § 13 Abs. 1 lit. b IDG weitgehend unverändert übernommen werden. Bei grösseren Systemen erfolgt die Dokumentation wie schon bisher mittels dem kantonalen Informationssicherheits-Managementsystem, welches zur Umsetzung der neuen, mit der Änderung des IDG vom 20. Oktober 2022 hinzugekommen Anforderungen um die entsprechenden Aspekte des Datenschutzes erweitert wird (vgl. oben Kommentierung zu § 1d). Die Dokumentation stellt zugleich die Grundlage für den Nachweis der Datenschutzkonformität nach § 6 Abs. 3 IDG dar (siehe § 1d IDV). Die Regelung des § 4 IDV gilt, wie im Einleitungssatz klargestellt wird, nicht bei Rechtsetzungsprojekten (§ 13 Abs. 1 lit. a IDG). Diese sind durch das Vorlegen von Projektskizzen und Entwürfen des Erlasstextes sowie des Ratschlags bzw. von Erläuterungen und dergleichen zu dokumentieren.

Aus der Beschreibung des Vorhabens gemäss § 4 lit. a IDV muss hervorgehen, für welche Aufgabe(n) welche Personendaten in welcher Art und durch wen bearbeitet werden.

Die Darstellung der Rechtslage gemäss § 4 lit. b IDV umfasst eine Beschreibung der für das Vorhaben bestehenden oder vorgesehenen Rechtsgrundlagen im Sinne von § 9 IDG im anwendbaren

Fachrecht und den allfälligen Bedarf für deren Änderung. § 9 IDG nennt die entsprechenden Anforderungen an die Rechtsgrundlage, stellt aber selber keine gesetzliche Grundlage für Datenbearbeitungen dar.

Zudem muss die einzureichende Dokumentation gemäss § 4 lit. c IDV aufzeigen, mit welchen technischen, organisatorischen und rechtlichen Massnahmen die Risiken für Persönlichkeitsverletzungen ausgeschlossen oder so weit reduziert werden, dass das Risiko nicht mehr als hoch zu bewerten und somit den betroffenen Personen zuzumuten ist. Der Weg dorthin führt über mehrere Analysen: Mit der Schutzbedarfsanalyse wird der Schutzbedarf bestimmt: Welchen Schutz brauchen die Daten bzw. Datenbearbeitungsprozesse pro Schutzziel: Vertraulichkeit, Integrität (inkl. Zurechenbarkeit und Nachvollziehbarkeit) und Verfügbarkeit. Nach dem Konzept des Grundschutzes wird der Grundschutzbedarf durch die standardmässig zu treffenden Grundschutzmassnahmen erfüllt. Falls in Bezug auf ein Schutzziel ein erhöhter Schutzbedarf besteht, ist diesbezüglich eine Risikoanalyse durchzuführen, um die zusätzlichen Massnahmen zu definieren, mit denen der erhöhte Schutzbedarf abgedeckt werden soll. Die Erkenntnisse aus diesen Analysen sind für das umzusetzende Projekt im Informationssicherheits- und Datenschutz-Konzept (ISDS-Konzept) festzuhalten.

2.6 Umsetzung der Informationspflicht (§ 4a IDV; neu)

Informations- und Datenschutzverordnung vom 9. August 2011	**Änderungen**
	I.2a Informations- und Meldepflicht **§ 4a Umsetzung der Informationspflicht** [1] Die Informationspflicht bei der Beschaffung gemäss § 15 Abs. 1 IDG kann insbesondere auf Erhebungsformularen und durch die Aushändigung eines Informationsblatts erfüllt werden.

Erläuterungen

Der geänderte § 15 IDG statuiert eine Informationspflicht der öffentlichen Organe bei der Beschaffung von Personendaten. Eine Beschaffung von Personendaten liegt vor, wenn ein öffentliches Organ aktiv und gewollt Kenntnis von Daten erlangt oder die Verfügung darüber begründet. Der neue § 4a IDV konkretisiert, in welcher Form die Information erfolgen kann bzw. muss.

Der Aufwand für die Umsetzung der neuen Informationspflicht ist in vielen Fällen überschaubar: Überall dort, wo Personendaten systematisch, beispielsweise auf einem Anmelde- oder Gesuchsformular – ob auf Papier oder auf einem Web-Formular – erhoben werden, reicht es, die entsprechenden Angaben auf dem Formular anzubringen. Wo Daten durch Mitarbeiterinnen und Mitarbeiter in einem Gespräch erhoben werden, kann die Information durch die (vorgängige oder gleichzeitige) Aushändigung eines Informationsblatts erfolgen. Dies hält der neue § 4a IDV fest. Nicht ausreichend wäre es hingegen, ein Informationsblatt nur beim Eingang zur Amtsstelle aufzulegen.

2.7 Ausnahmen von der Informationspflicht (§ 4b IDV; neu)

Informations- und Datenschutzverordnung vom 9. August 2011	Änderungen
	§ 4b Ausnahmen von der Informationspflicht [1] Bei Bekanntgaben von Personendaten für nicht personenbezogene Zwecke, insbesondere für Statistik, Forschung und Planung, kann eine Information der betroffenen Personen unterbleiben.

Erläuterungen

Der neue § 15 Abs. 3 IDG hält drei Ausnahmetatbestände fest, bei deren Vorliegen die Informationspflicht der öffentlichen Organe entfällt. Dies ist dann der Fall, wenn die betroffene Person bereits informiert ist, das Bearbeiten der Personendaten gesetzlich ausdrücklich vorgesehen oder nicht oder nur mit unverhältnismässigem Aufwand möglich ist. Der neue § 4b IDV konkretisiert diese gesetzliche Bestimmung für den Bereich der Bekanntgaben von Personendaten für nicht personenbezogene Zwecke.

Die Datengewinnung des Statistischen Amtes aus den vorhandenen Datenbeständen der öffentlichen Organe beispielsweise ist ausdrücklich gesetzlich vorgesehen (§ 6 Abs. 1 des Gesetzes über die öffentliche Statistik, StatG; SG 453.200), weshalb keine Informationspflicht gilt. Ein zweites gesetzlich geregeltes Anwendungsfeld ist die Humanforschung: Hier legt das Humanforschungsgesetz des Bundes (HFG, SR 810.30) fest, unter welchen Voraussetzungen (Einwilligung oder Nichtwiderspruch der Betroffenen) welche Daten in welcher Form (identifizierend, pseudonymisiert, anonymisiert) z.B. von den Spitälern an Forscherinnen und Forscher an öffentlichen oder privaten Forschungseinrichtungen bekanntgegeben werden dürfen. In den Bereichen von Planung und Forschung sowie bei weiteren, nicht personenbezogenen Datenbearbeitungen, ist eine Information der betroffenen Personen bei der Datenbeschaffung aber auch ausserhalb dieser gesetzlich geregelten Bereiche nicht oder nur mit unverhältnismässigem Aufwand möglich. Oftmals ist im Zeitpunkt der Datenerhebung die spätere Verwendung zu diesen nicht personenbezogenen Zwecken nicht absehbar. Zudem ist die Zahl der betroffenen Personen regelmässig sehr hoch. Das IDG privilegiert schon bisher in § 22 die Datenbekanntgabe zu einem nicht personenbezogenen Zweck, da die entsprechenden Datenbearbeitungen einem öffentlichen Interesse entsprechen und weil sie als weniger heikel als andere Datenbearbeitungen erscheinen. Die in § 22 Abs. 2 IDG vorgesehene Verpflichtungserklärung bei Datenbekanntgaben zu einem nicht personenbezogenen Zweck stellt sicher, dass Rückschlüsse auf einzelne betroffene Personen nicht möglich sind. Die öffentlichen Organe sind verpflichtet, die Daten, sobald es der Bearbeitungszweck zulässt, zu anonymisieren oder pseudonymisieren und Rückschlüsse auf einzelne Personen in den Auswertungen auszuschliessen. Diese Umstände rechtfertigen einen Verzicht auf die Information der betroffenen Personen bei der Datenerhebung. Um Ungewissheiten über den Anwendungsbereich von § 15 Abs. 3 IDG zu vermeiden, hält § 4b IDV daher neu ausdrücklich fest, dass bei Bekanntgaben von Personendaten zu nicht personenbezogenen Zwecken wie Statistik, Forschung oder Planung keine Informationspflicht im Sinne von § 15 Abs. 1 IDG besteht. Anderslautende besondere Bestimmungen bleiben vorbehalten.

2.8 Datenschutzberatung (§ 4c IDV; neu)

Informations- und Datenschutzverordnung vom 9. August 2011	Änderungen
	I.2b. Datenschutzberatung (§ 16b IDG) **§ 4c Datenschutzberaterinnen und -berater** [1] Folgende Bereiche, Abteilungen und Stabsstellen bezeichnen eine Datenschutzberaterin oder einen Datenschutzberater: a) der Bereich Bevölkerungsdienste und Migration; b) die Kantonspolizei; c) die Staatsanwaltschaft; d) das Amt für Wirtschaft und Arbeit; e) die Sozialhilfe. [2] Folgende öffentlich-rechtlichen Anstalten bezeichnen eine Datenschutzberaterin oder einen Datenschutzberater: a) die Industriellen Werke Basel; b) die öffentlichen Spitäler; c) die Universität Basel.

Erläuterungen

Mit § 16b IDG hat der Gesetzgeber die neue Funktion einer Datenschutzberaterin oder eines Datenschutzberaters eingeführt (vgl. Ratschlag Änderung IDG, Seiten 50 ff; Bericht JSSK, Seiten 11 ff.). Die neue Gesetzesbestimmung hält in ihrem ersten Absatz fest, dass die Departemente, die Gerichte sowie die Gemeinden Datenschutzberaterinnen und -berater zu bezeichnen haben. Absatz drei benennt die wesentlichen Aufgaben der Datenschutzberaterinnen und Datenschutzberater:

- Beratung und Unterstützung der Mitarbeitenden der jeweiligen Stelle bei Bearbeitungen von Personendaten. Zu denken ist hier etwa an Beratungen bei der Vornahme einer Rechtsgrundlagenanalyse sowie der Erstellung von Schutzbedarfsanalysen, Informationssicherheits- und Datenschutzkonzepten;
- Unterstützung bei der Vornahme der Datenschutz-Folgenabschätzung gemäss § 12a Abs. 1 IDG;
- Zusammenarbeit mit der oder dem kantonalen Datenschutzbeauftragten, etwa im Rahmen von Vorabkonsultationen gemäss § 13 IDG oder bei der Meldung von Datenschutzverletzungen gemäss § 16a IDG.

Der zweite Absatz der gesetzlichen Regelung beauftragt den Regierungsrat, zusätzlich Bereiche, Abteilungen und Stabsstellen der kantonalen Verwaltung sowie öffentlich-rechtlichen Anstalten des kantonalen Rechts zu bestimmen, die eine eigene Datenschutzberaterin oder einen eigenen Datenschutzberater zu bezeichnen haben. Im neuen § 4d IDV wird dies umgesetzt.

Absatz eins der neuen Bestimmung nennt die Stellen der kantonalen Verwaltung, welche – zusätzlich zu den durch das Gesetz eingeführten departementalen Datenschutzberaterinnen und -beratern – eine Datenschutzberatung zu bezeichnen haben. Bei den unter lit. a bis lit. c genannten Stellen handelt es sich um diejenigen, welche die Pflicht zur Einführung dieser neuen Funktion aufgrund der justiziellen und polizeilichen Zusammenarbeit der Schweiz mit der Europäischen Union trifft (Art. 32 Abs. 1 der Richtlinie [EU] 2016/680). Für sie hatte der Ratschlag Änderung IDG die Bezeichnung von Datenschutzberaterinnen und -beratern auf Gesetzesstufe vorgesehen. Der

Grosse Rat entschied indessen, in § 16b IDG die Departemente zur Einführung von Datenschutzberatungen zu verpflichten, nicht aber Polizei, Staatsanwaltschaft und den Bereich Bevölkerungsdienste und Migration. Mit der Aufnahme dieser drei Dienststellen in der Verordnung wird nun dem Auftrag aus dem übergeordneten Recht entsprochen.

Die beiden weiteren Ämter, welche zur Einführung einer eigenen Datenschutzberatung verpflichtet werden, arbeiten mit grossen Mengen besonders sensibler Personendaten: Das Amt für Wirtschaft und Arbeit bearbeitet insbesondere Personendaten von Stellensuchende, arbeitslosen Personen und Arbeitgebenden im schweizerischen und grenzüberschreitenden europäischen Arbeitsmarkt. Ausserdem werden Personendaten von Arbeitnehmerinnen und Arbeitnehmern bearbeitet sowie solche aus (baselstädtischen) Unternehmen (z.B. für die Aufgaben der Schwarzarbeitsbekämpfung, bei Arbeitsbewilligungen, im Arbeitsinspektorat und bei der Standortförderung). Die Sozialhilfe erbringt materielle und persönliche Hilfeleistungen sowie weitere Dienstleitungen gegenüber Bedürftigen und von Bedürftigkeit bedrohten Personen und bearbeitet in diesem Zusammenhang eine Vielzahl besonders sensibler Personendaten, beispielsweise Informationen zum Aufenthaltsstatus, Unterlagen über Einnahmen und Vermögen und weitere bedarfsrelevante Unterlagen wie Mietverträge oder Krankenkassenpolicen sowie Unterlagen von unterhalts- oder unterstützungspflichtigen Dritten.

§ 4d Abs. 2 nennt die selbständigen kantonalen Anstalten, welche ebenfalls eine Datenschutzberatung einrichten müssen. Die Industriellen Werke Basel, die öffentlichen Spitäler sowie die Universität Basel sind öffentliche Organe, die wie die genannten Ämter ebenfalls sehr umfangreiche Bearbeitungen von teilweise sehr sensiblen Personendaten wie Daten zu Gesundheit oder den persönlichen wirtschaftlichen Verhältnissen vornehmen. Der Begriff «öffentliche Spitäler» bezeichnet in diesem Zusammenhang die öffentlichen Spitäler gemäss dem Gesetz über die öffentlichen Spitäler des Kantons Basel-Stadt (ÖSpG; SG 331.100) (Universitätsspital Basel, Universitäre Psychiatrische Kliniken Basel, Universitäre Altersmedizin Felix Platter [Felix Platter-Spital]) sowie das Universitäts-Kinderspital beider Basel.

Die oder der Datenschutzbeauftragte stellt die kantonale Beratungs-, Kontroll- und Aufsichtsstelle für den Datenschutz dar. Er verfolgt die nationale und internationale Rechtsentwicklung im Bereich des Datenschutzes und kennt aufgrund seiner Tätigkeit sowohl die Anliegen betroffener Personen wie auch der öffentlichen Organe. Zur Sicherstellung der Qualität der Aufgabenerfüllung der Datenschutzberaterinnen und -berater bietet die oder der Datenschutzbeauftragte sinnvollweise Schulungen und Weiterbildungen für die Datenschutzberaterinnen und Datenschutzberater an.

2.9 Veröffentlichung der Videoüberwachungsreglemente (§ 6 IDV; aufgehoben)

Informations- und Datenschutzverordnung vom 9. August 2011	**Änderungen**
§ 6 Veröffentlichung der Reglemente [1] Die Reglemente werden der Öffentlichkeit leicht zugänglich gemacht. [2] Wenn durch die Bekanntgabe der Kamerastandorte die Zweckerreichung unmöglich wird, kann auf deren Veröffentlichung verzichtet werden.	**§ 6** *aufgehoben*

Erläuterungen

Die Pflicht zur Veröffentlichung der Reglemente für Videoüberwachungssysteme war bisher auf Verordnungsstufe geregelt. Neu ist diese Pflicht im Gesetz (§ 18 Abs. 4bis IDG) verankert, um deren Bedeutung hervorzuheben. Auch die Ausnahmebestimmung des bisherigen § 6 Abs. 2 IDV, welche von der Publikationspflicht befreite, soweit die Bekanntgabe der Kamerastandorte die Zweck-

erreichung verunmöglicht, wurde ins Gesetz verschoben, wobei der Ausnahmetatbestand erweitert wurde. Daher wird § 6 IDV redundant und kann aufgehoben werden.

2.10 Anpassungen aufgrund der Einführung der Vorabkonsultation (§§ 8, 9 und 9b IDV; geändert)

Informations- und Datenschutzverordnung vom 9. August 2011	Änderungen
§ 8 Vorabkontrolle vor der Inbetriebnahme eines Videoüberwachungssystems [1] Das öffentliche Organ legt der oder dem Datenschutzbeauftragten das Videoüberwachungsvorhaben zur Vorabkontrolle gemäss §§ 2 ff. dieser Verordnung vor. [2] Das öffentliche Organ legt der oder dem Datenschutzbeauftragten die notwendigen Unterlagen vor, insbesondere: a) Ausführungen dazu, mit welchen anderen Massnahmen der Zweck bisher nicht erreicht werden konnte, b) allenfalls Ausführungen dazu, weshalb die Regelaufbewahrungsdauer von einer Woche zur Erreichung des konkreten Zwecks nicht ausreicht und mit welchen technischen und organisatorischen Vorkehren das Risiko einer Persönlichkeitsverletzung minimiert wird, und c) den Entwurf des Reglements, sofern dieser im Zeitpunkt der Einreichung zur Vorabkontrolle schon vorliegt.	**§ 8 ~~Vorabkontrolle~~ Vorabkonsultation vor der Inbetriebnahme eines Videoüberwachungssystems** [1] Das öffentliche Organ legt der oder dem Datenschutzbeauftragten das Videoüberwachungsvorhaben zur ~~Vorabkontrolle~~ Vorabkonsultation gemäss § 13 IDG sowie §§ 2 ff. dieser Verordnung vor. [2] Das öffentliche Organ legt der oder dem Datenschutzbeauftragten die notwendigen Unterlagen vor, insbesondere: a) Ausführungen dazu, mit welchen anderen Massnahmen der Zweck bisher nicht erreicht werden konnte, b) allenfalls Ausführungen dazu, weshalb die Regelaufbewahrungsdauer von einer Woche zur Erreichung des konkreten Zwecks nicht ausreicht und mit welchen technischen und organisatorischen Vorkehren das Risiko einer Persönlichkeitsverletzung minimiert wird, und c) den Entwurf des Reglements, sofern dieser im Zeitpunkt der Einreichung zur ~~Vorabkontrolle~~ Vorabkonsultation schon vorliegt.
§ 9 Vorabkontrolle vor der Verlängerung eines Videoüberwachungsreglements [1] Soll ein Videoüberwachungsreglement verlängert werden, legt das öffentliche Organ das Verlängerungsvorhaben spätestens drei Monate vor Ablauf der Befristung des Reglements der oder dem Datenschutzbeauftragten zur Vorabkontrolle vor. [2] Die Vorlage enthält alle für die Evaluation der Wirksamkeit notwendigen relevanten Angaben, insbesondere zu den Fragen: a) inwieweit der angestrebte Zweck mit der Videoüberwachung und/oder aufgrund anderer Faktoren erreicht werden konnte, und b) inwieweit Änderungen gegenüber der vorgängigen Konfiguration möglich sind oder sich aufdrängen.	**§ 9 ~~Vorabkontrolle~~ Vorabkonsultation vor der Verlängerung eines Videoüberwachungsreglements** [1] Soll ein Videoüberwachungsreglement verlängert werden, legt das öffentliche Organ das Verlängerungsvorhaben spätestens drei Monate vor Ablauf der Befristung des Reglements der oder dem Datenschutzbeauftragten zur ~~Vorabkontrolle~~ Vorabkonsultation vor. [2] *unverändert*
§ 9b Autorisierung [1] Die Bekanntgabe von Personendaten mittels Abrufverfahren bedarf einer Autorisierung durch die Dateneignerin oder den Dateneigner, d.h.	**§ 9b Autorisierung** [1] *unverändert*

durch das verantwortliche öffentliche Organ im Sinne von § 6 IDG. [2] Die Autorisierung ist der oder dem Datenschutzbeauftragten zur Vorabkontrolle vorzulegen. [3] Hat das verantwortliche Organ die Personendaten, auf welche sich das Gesuch bezieht, seinerseits vollständig oder teilweise mittels Abrufverfahren bezogen, ist es nicht befugt, diese ohne Einwilligung des öffentlichen Organs, von dem es die beantragten Personendaten bezogen hat, mittels Abrufverfahren weiterzugeben.	[2] Die Autorisierung ist der oder dem Datenschutzbeauftragten zur ~~Vorabkontrolle~~ Vorabkonsultation vorzulegen. [3] *unverändert*

Erläuterungen

Das Verfahren der bisherigen Vorabkontrolle wird ersetzt durch die neue Vorabkonsultation (§ 13 IDG). §§ 8, 9 und 9b welche bisher auf die Vorabkontrolle Bezug nahmen, sind entsprechend begrifflich anzupassen.

2.11 Grenzüberschreitende Bekanntgabe von Personendaten (§ 11 IDV; geändert)

Informations- und Datenschutzverordnung vom 9. August 2011	**Änderungen**
§ 11 Grenzüberschreitende Bekanntgabe von Personendaten (§ 23 IDG) [1] Das öffentliche Organ kann für die Frage, ob die Gesetzgebung eines Empfängerstaates einen angemessenen Schutz im Sinne von § 23 Bst. a IDG gewährleistet, auf die vom Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten gestützt auf Art. 7 der Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz erlassene Liste abstellen. [2] Wenn bei einer Datenbekanntgabe an eine Empfängerin oder einen Empfänger in einem Staat, dessen Gesetzgebung keinen angemessenen Schutz gewährleistet, der Schutz durch vertragliche Vereinbarungen im Sinne von § 23 Bst. b IDG garantiert werden soll, hat das öffentliche Organ die oder den Datenschutzbeauftragten vorab über die vereinbarten Sicherheitsvorkehrungen zu informieren.	**§ 11 Grenzüberschreitende Bekanntgabe von Personendaten (§ 23 IDG)** [1] Das öffentliche Organ kann für die Frage, ob die Gesetzgebung eines Empfängerstaates einen angemessenen Schutz im Sinne von § 23 ~~Bst.~~lit. a IDG gewährleistet, auf die ~~vom Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten gestützt auf Art. 7 der Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz erlassene Liste~~ Liste der Staaten, Gebiete, spezifischen Sektoren in einem Staat und internationalen Organisationen in Anhang 1 der eidgenössischen Verordnung über den Datenschutz vom 31. August 2022 abstellen. [2] *unverändert*

Erläuterungen

§ 23 IDG regelt die Bedingungen, unter denen öffentliche Organe Personendaten an öffentliche Organe oder Private im Ausland bekannt geben dürfen. § 11 IDV verwies bisher für die Frage, ob die Gesetzgebung eines Empfängerstaates einen angemessenen Schutz im Sinne von § 23 lit. a IDG gewährleistet, auf die vom Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) gestützt auf Art. 7 der Verordnung zum Bundesgesetz über den Datenschutz vom

14. Juni 1993 erlassene Liste. Diese Verordnung ist per 1. September 2023 aufgrund der Inkraftsetzung der neuen Verordnung über den Datenschutz vom 31. August 2022 (Datenschutzverordnung, DSV, SR 235.11) ausser Kraft gesetzt worden.

Gemäss Art. 16 Abs. 1 des ebenfalls seit dem 1. September 2023 geltenden Bundesgesetzes über den Datenschutz vom 25. September 2020 (Datenschutzgesetz, DSG; SR 235.1) liegt es für den Geltungsbereich des DSG beim Bundesrat zu entscheiden, ob ein anderer Staat oder ein internationales Organ einen angemessenen Datenschutz gewährleistet. Art. 8 der neuen DSV legt mehrere Kriterien fest, die bei der Beurteilung der Angemessenheit des Datenschutzes eines Staates, eines Gebiets, eines spezifischen Sektors in einem Staat oder eines internationalen Organs besonders zu berücksichtigen sind, nämlich:

a. die internationalen Verpflichtungen des Staates oder internationalen Organs, insbesondere im Bereich des Datenschutzes;
b. die Rechtsstaatlichkeit und die Achtung der Menschenrechte;
c. die geltende Gesetzgebung insbesondere zum Datenschutz sowie deren Umsetzung und die einschlägige Rechtsprechung;
d. die wirksame Gewährleistung der Rechte der betroffenen Personen und des Rechtsschutzes;
e. das wirksame Funktionieren einer oder mehrerer unabhängiger Behörden, die im betreffenden Staat für den Datenschutz zuständig sind oder denen ein internationales Organ untersteht und die über ausreichende Befugnisse und Kompetenzen verfügen.

Anhang 1 der DSV enthält eine Liste der Staaten, die über einen angemessenen Datenschutz verfügen. Diese Liste hat die bisherige, vom EDÖB erlassene Liste ersetzt. Da die bisherige Fassung von § 11 Abs. 1 IDV auf die Liste des EDÖB Bezug nahm, ist die Bestimmung entsprechend anzupassen. Die Liste des Bundesrates kann, wie die bisherige Liste des EDÖB, bei der Beurteilung des angemessenen Schutzes als Leitlinie herangezogen werden, ist aber für die kantonalen öffentlichen Organe nicht verbindlich.

2.12 Anspruch auf Unterlassung, Beseitigung oder Feststellung (§ 13 IDV; geändert)

Informations- und Datenschutzverordnung vom 9. August 2011	**Änderungen**
§ 13 Anspruch auf Unterlassung, Beseitigung oder Feststellung (§ 27 Abs. 1 Bst. b–d IDG) [1] Weist ein öffentliches Organ das Begehren auf Unterlassung eines widerrechtlichen Bearbeitens, auf Beseitigung der Folgen eines widerrechtlichen Bearbeitens oder auf Feststellung der Widerrechtlichkeit eines Bearbeitens von Personendaten ab, so teilt es das der gesuchstellenden Person mit, auf Verlangen in Form einer anfechtbaren Verfügung.	**§ 13 Anspruch auf Unterlassung, Beseitigung oder Feststellung (§ 27 Abs. 1 Bst. b–d IDG)** [1] Weist ein öffentliches Organ das Begehren auf Unterlassung eines widerrechtlichen Bearbeitens, auf Beseitigung der Folgen eines widerrechtlichen Bearbeitens, insbesondere auf Datenlöschung, oder auf Feststellung der Widerrechtlichkeit eines Bearbeitens von Personendaten ab, so teilt es das der gesuchstellenden Person mit, auf Verlangen in Form einer anfechtbaren Verfügung.

Erläuterungen

§ 27 Abs. 1 IDG listet die Ansprüche von Personen auf, die von widerrechtlichen Bearbeitungen ihrer Personendaten betroffen sind. Da Art. 16 Abs. 2 der Richtlinie (EU) 2016/680 und Art. 9 Abs. 1 lit. e der (modernisierten) Europarats-Konvention 108+ neu ein ausdrückliches Recht auf Löschung bzw. Einschränkung der Bearbeitung vorsehen, wurde die Gesetzesbestimmung um

den Löschungsanspruch ergänzt. § 13 Abs. 1 IDV regelt in diesem Zusammenhang den Anspruch der betroffenen Person auf Ausstellung einer Verfügung, wenn das öffentliche Organ ein auf § 27 Abs. 1 IDG gestütztes Begehren abweist. Die Verordnungsbestimmung ist, analog der gesetzlichen Regelung, hinsichtlich des Anspruchs auf Datenlöschung zu ergänzen.

2.13 Klassifizierung (§ 18 IDV; geändert)

Informations- und Datenschutzverordnung vom 9. August 2011	**Änderungen**
§ 18 Klassifizierung [1] Das öffentliche Organ, welches schutzwürdige Informationen verfasst, weist sie entsprechend dem Grad ihrer Schutzwürdigkeit einer der folgenden Klassifizierungsstufen zu: a) geheim, b) vertraulich. [2] Werden Informationsträger physisch zu einem Sammelwerk zusammengefasst, ist zu überprüfen, ob und inwiefern dieses klassifiziert oder einer höheren Klassifizierungsstufe zugeordnet werden muss.	**§ 18 Klassifizierung von schutzwürdigen Informationen** [1] Verfasst ein öffentliches Organ Berichte mit schutzwürdigen Informationen zuhanden des Regierungsrats, weist es diese entsprechend dem Grad ihrer Schutzwürdigkeit einer der folgenden Klassifizierungsstufen zu: a) geheim; b) vertraulich. [1bis] Andere schutzwürdige Informationen können ebenfalls klassifiziert werden. [2] *unverändert*

Erläuterungen

Die 2012 in Kraft getretenen Bestimmungen über die Klassifizierung von schutzwürdigen Informationen (§§ 18–22) sind in der Praxis nur teilweise zur Anwendung gelangt. Die generelle Pflicht zur Klassifizierung von schutzwürdigen Informationen erwies sich als weder erforderlich noch umsetzbar. Von Bedeutung ist die Klassifizierung einzig bei den Geschäften des Regierungsrates und den ihnen zugrundeliegenden Informationen. Daher wird die Pflicht zur Klassifizierung schutzwürdiger Informationen neu eingegrenzt auf die Berichte der Departemente und der Staatskanzlei zuhanden des Regierungsrates einschliesslich ihrer Beilagen sowie die in diesen Berichten enthaltenen Beschlussanträge.

Das bedeutet nicht, dass für alle anderen Informationen keine Einschränkungen bezüglich Veröffentlichung oder Herausgabe gelten. Im Rahmen der Prüfung nach § 29 IDG muss jedes öffentliche Organ weiterhin prüfen, ob die Bekanntgabe von und der Zugang zu Informationen ganz oder teilweise zu verweigern oder aufzuschieben ist, weil eine besondere gesetzliche Geheimhaltungspflicht oder ein überwiegendes öffentliches oder privates Geheimhaltungsinteresse entgegensteht. Ausserdem wird im Zusammenhang mit der Nutzung von Cloud-Diensten die Schaffung einer Klassifizierungsordnung zu prüfen sein.

Abs. 1bis hält fest, dass die Klassifikation anderer schutzwürdiger Informationen weiterhin zulässig ist.

Bei Gelegenheit dieser Revision wurde zudem eine sprachliche Bereinigung der Bestimmung vorgenommen.

2.14 Einschränkungen zum Schutz überwiegender privater Interessen, Anonymisierung (§ 23 IDV; geändert)

Informations- und Datenschutzverordnung vom 9. August 2011	Änderungen
§ 23 Einschränkungen zum Schutz überwiegender privater Interessen, Anonymisierung (§ 29 Abs. 3 und § 30 IDG) [1] Bei besonderen Personendaten wird vermutet, dass das private Interesse der betroffenen Person gegenüber dem Interesse einer Drittperson am Zugang überwiegt.	**§ 23 Einschränkungen zum Schutz überwiegender privater Interessen, Anonymisierung (§ 29 Abs. 3 und § 30 IDG)** [1] Bei besonderen Personendaten und Ergebnissen eines Profilings wird vermutet, dass das private Interesse der betroffenen Person gegenüber dem Interesse einer Drittperson am Zugang überwiegt.

Erläuterungen

Der geänderte § 9 Abs. 2 IDG verlangt neu, dass zur Vornahme eines Profilings im Sinne des neuen § 3 Abs. 7 IDG die gleichen Voraussetzungen erfüllt sein müssen wie zur Bearbeitung besonderer Personendaten. Entsprechend müssen die privaten Interessen von Personen, die von einem Profiling betroffen sind, auch gleichermassen geschützt werden wie diejenigen von Personen, deren besondere Personendaten bearbeitet werden. § 23 IDV statuiert die rechtliche Vermutung, dass bei der Bearbeitung besonderer Personendaten das (Geheimhaltungs-)Interesse betroffener Personen das Interesse am Informationszugang überwiegt. Diese Bestimmung ist aufgrund der Änderung von § 9 Abs. 2 IDG dahingehend zu ergänzen, dass auch bei Profilings vermutet wird, dass die Geheimhaltungsinteressen der betroffenen Person die Zugangsinteressen überwiegen.

2.15 Übergangsbestimmung (§ 35a IDV; neu)

Informations- und Datenschutzverordnung vom 9. August 2011	Änderungen
	§ 35a Übergangsbestimmung zur Änderung vom [Datum des RRB betreffend Änderung IDV] [1] Für bestehende Datenbearbeitungssysteme ist der Nachweis für die Einhaltung der Datenschutzbestimmungen gemäss § 6 Abs. 3 IDG sowie § 1d dieser Verordnung spätestens bis 31. Dezember 2029 zu erbringen.

Erläuterungen

§ 6 Abs. 3 IDG verlangt neu, dass öffentliche Organe nachweisen können müssen, dass sie die Bestimmungen des Datenschutzes einhalten (vgl. auch oben, § 1d IDV). Diese Pflicht gilt nicht nur bezüglich neuen, sondern auch hinsichtlich schon bestehenden Datenbearbeitungssystemen. Daher ist für bestehende Systeme eine Übergansfrist für die Erbringung des Nachweises vorzusehen. Eine Frist bis Ende des Jahres 2029 stellt einen realistischen zeitlichen Rahmen für diese anspruchsvolle Aufgabe dar.