Verordnung zum Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (VIDAG)

Änderung vom 23. Mai 2018

Der Regierungsrat des Kantons Aargau

beschliesst:

I.

Der Erlass SAR 150.711 (Verordnung zum Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen [VIDAG] vom 26. September 2007) (Stand 1. Juli 2008) wird wie folgt geändert:

Ingress (geändert)
Der Regierungsrat des Kantons Aargau,
gestützt auf § 13 Abs. 4 des Gesetzes über die Organisation des Regierungsrates und der kantonalen Verwaltung (Organisationsgesetz) vom 26. März 1985 [1)] und die §§ 12, 21, 27, 30, 40, 43 und 45 des Gesetzes über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (IDAG) vom 24. Oktober 2006 [2)],
beschliesst:

§ 1 Abs. 4 (geändert)
[4] Das öffentliche Organ weist die Gesuchstellerin oder den Gesuchsteller darauf hin, dass auf das Gesuch nicht eingetreten wird, wenn sie oder er innert einer Frist von 20 Tagen nicht die für die Identifizierung des verlangten Dokuments erforderliche Präzisierung macht (§ 36 Abs. 1 IDAG).

§ 2 Abs. 3 (aufgehoben)
[3] *Aufgehoben.*

1) SAR 153.100
2) SAR 150.700

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

[1] Die öffentlichen Organe haben bei der elektronischen Bearbeitung von Personendaten zur Einhaltung der Vertraulichkeit, Integrität, Verfügbarkeit, Zurechenbarkeit und Nachvollziehbarkeit sowie der Löschfristen insbesondere folgende Massnahmen zu ergreifen:

a) **(geändert)** Zugangskontrolle: unbefugten Personen ist der Zugang zu Einrichtungen, in denen Personendaten verarbeitet werden, zu verwehren,
b) **(geändert)** Datenträgerkontrolle: unbefugten Personen ist das Lesen, Kopieren, Verändern oder Entfernen von Datenträgern zu verunmöglichen,
c) **(geändert)** Transportkontrolle: bei der Bekanntgabe von Personendaten sowie beim Transport von Datenträgern ist zu verhindern, dass die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können,
d) **(geändert)** Bekanntgabekontrolle: Datenempfänger, denen Personendaten mittels Einrichtungen zur Datenübertragung bekannt gegeben werden, müssen identifiziert werden können,
e) **(geändert)** Speicherkontrolle: unbefugte Eingabe in den Speicher sowie unbefugte Einsichtnahme, Veränderung oder Löschung gespeicherter Personendaten sind zu verhindern,
f) **(geändert)** Benutzerkontrolle: die Benutzung von automatisierten Datenverarbeitungssystemen mittels Einrichtungen zur Datenübertragung durch unbefugte Personen ist zu verhindern,
g) **(neu)** Zugriffskontrolle: der Zugriff der berechtigten Personen ist auf diejenigen Personendaten zu beschränken, die sie für die Erfüllung ihrer Aufgabe benötigen,
h) **(neu)** Eingabekontrolle: in elektronischen Systemen muss nachträglich überprüft werden können, welche Personendaten zu welcher Zeit und von welcher Person eingegeben wurden,
i) **(neu)** Wiederherstellung: Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können,
j) **(neu)** Zuverlässigkeit, Integrität: Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen, auftretende Fehlfunktionen gemeldet werden und gespeicherte Personendaten nicht durch Fehlfunktionen des Systems beschädigt werden können.

[3] Öffentliche Organe legen ihr Datensicherheitskonzept fest und bestimmen die Aufbewahrungsfristen der von ihnen bearbeiteten Daten unter Beachtung der Anbietepflichten gemäss Archivgesetzgebung.

[4] Spätestens ein Jahr nach Ablauf einer befristeten Anbietepflicht gemäss Archivgesetzgebung oder zehn Jahre nach ihrer Anlage sind vom Archiv nicht übernommene Personendaten zu löschen, ausser sie werden aufgrund einer nachweisbaren Überprüfung für die Aufgabenerfüllung oder zu Beweiszwecken weiterhin benötigt. Die Überprüfung ist spätestens nach zehn Jahren zu wiederholen. Sonderbestimmungen in anderen Erlassen bleiben vorbehalten.

§ 5 Abs. 1 (geändert), **Abs. 2 (geändert)**, **Abs. 2bis (neu)**, **Abs. 3 (aufgehoben)**

Elektronische Systeme (Überschrift geändert)

[1] Öffentliche Organe dokumentieren beim Betrieb eines elektronischen Systems zur Bearbeitung von Personendaten die zur Gewährleistung der Datensicherheit getroffenen Massnahmen sowie deren Überprüfung und Aktualisierung.

[2] Zugriffe auf Personendaten sind wie folgt zu protokollieren, wenn die Einhaltung der Schutzziele nicht auf andere Art gewährleistet wird:

a) **(neu)** Zugriffe von Systemadministratoren
b) **(neu)** Zugriffe von Nutzenden zur
   1. Authentifizierung und Autorisierung,
   2. Dateneingabe und -veränderung,
   3. Dateneinsicht,
   4. Datenübermittlung,
   5. Datenlöschung.

[2bis] Die Protokolle sind während eines Jahres revisionsgerecht festzuhalten. Sie dürfen ausschliesslich zur Überprüfung der Rechtmässigkeit der Datenbearbeitung und der Sicherstellung der Informations- und Informatiksicherheit verwendet werden.

[3] *Aufgehoben.*

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

Erhöhte Risiken; Datenschutz-Folgenabschätzung (Überschrift geändert)

[1] Öffentliche Organe führen bei jeder Einführung und Erweiterung einer informatikgestützten Anwendung mit Personendaten oder bei Veränderungen der Technologie, die voraussichtlich zu einem erhöhten Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person führt, eine Datenschutz-Folgenabschätzung durch. Ein erhöhtes Risiko ist insbesondere anzunehmen, wenn

a) **(geändert)** das System Profiling ermöglicht,
b) **(geändert)** besonders schützenswerte Personendaten bearbeitet werden,
c) **(geändert)** Bearbeitungen von Personendaten durch Auftragnehmende durchgeführt werden,
d) **(neu)** zwei oder mehrere öffentliche Organe Personendaten in einem gemeinsamen elektronischen System bearbeiten.

[2] Auf die Datenschutz-Folgenabschätzung kann verzichtet werden, sofern und soweit die Datenbearbeitungen in der gesetzlichen Grundlage ausdrücklich geregelt werden.

[3] Öffentliche Organe halten das Ergebnis der Datenschutz-Folgenabschätzung schriftlich fest (§ 17a Abs. 2 IDAG). Der beauftragten Person für Öffentlichkeit und Datenschutz ist eine Kopie zuzustellen, wenn die Anwendung nicht zur Vorab-Konsultation unterbreitet wird.

§ 6a (neu)

Mindestinhalt der Datenschutz-Folgenabschätzung

[1] Die Datenschutz-Folgenabschätzung enthält mindestens:

a) das verantwortliche öffentliche Organ, die rechtliche Grundlage, den Zweck und eine systematische Beschreibung der geplanten Datenbearbeitungen,
b) eine Bewertung der Notwendigkeit und Verhältnismässigkeit der Datenbearbeitungen in Bezug auf den Zweck,
c) eine Bewertung der Risiken für die Persönlichkeit und die Grundrechte der betroffenen Personen unter Beachtung der Schutzziele gemäss § 4 Abs. 1 und
d) die technischen und organisatorischen Massnahmen, die zur Bewältigung der Risiken geplant sind (§ 4 Abs. 1), unter anderem in Bezug auf Datenbearbeitungen durch beauftragte Dritte.

§ 6b (neu)

Vorab-Konsultation; Ablauf

[1] Mit dem Gesuch um Vorab-Konsultation (§ 17b IDAG) reicht das verantwortliche öffentliche Organ die Dokumentation der Datenschutz-Folgenabschätzung ein.

[2] Das öffentliche Organ führt die geplanten Datenverarbeitungen nicht durch, bis die Konsultation abgeschlossen ist.

[3] Die Konsultation ist abgeschlossen, wenn die beauftragte Person für Öffentlichkeit und Datenschutz die Anwendung für unbedenklich erklärt oder eine Empfehlung gemäss § 17b Abs. 2 IDAG abgegeben hat.

§ 6c (neu)

Verletzung der Datensicherheit; Ausnahme der Meldepflicht

[1] Verletzungen der Datensicherheit sind insbesondere Sicherheitsverletzungen, die zur Vernichtung, zum Verlust, zur Veränderung oder zum unbefugten Zugang zu Personendaten führen.

[2] Der Schutz der betroffenen Person erfordert keine Meldung, wenn

a) die technischen und organisatorischen Massnahmen des öffentlichen Organs eine Kenntnisnahme der Personendaten durch Unbefugte verhindert haben oder

b) das öffentliche Organ durch nachfolgende Massnahmen sichergestellt hat, dass aller Wahrscheinlichkeit nach kein erhöhtes Risiko für die Persönlichkeit und die Grundrechte betroffener Personen mehr besteht oder

c) dies mit einem unverhältnismässigen Aufwand verbunden wäre und stattdessen eine öffentliche Bekanntmachung oder eine andere wirksame Informationsmassnahme erfolgt.

§ 7 Abs. 1 (geändert)

[1] Besonders schützenswerte Personendaten sind insbesondere Daten über:

e) **(neu)** die ererbten oder erworbenen genetischen Eigenschaften einer Person, die eindeutige Informationen über deren Physiologie oder deren Gesundheit liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden Person gewonnen wurden (genetische Daten),

f) **(neu)** die physischen, physiologischen oder verhaltenstypischen Merkmale einer Person, die mit speziellen technischen Verfahren gewonnen werden und die eindeutige Identifizierung dieser Person ermöglichen oder bestätigen (biometrische Daten).

§ 7a (neu)

Informationspflicht; Ausnahmen

[1] Bei Datenbekanntgaben für nicht personenbezogene Zwecke, insbesondere für Forschung, Planung und Statistik kann eine Information der betroffenen Personen unterbleiben. Anderslautende gesetzliche Bestimmungen bleiben vorbehalten.

[2] Werden Daten ausschliesslich zur Einhaltung und Kontrolle der Datensicherheit erhoben und gespeichert, besteht keine Pflicht zur Information der betroffenen Personen.

[3] Werden Daten ausschliesslich zur Einhaltung der Aufbewahrungs- und Archivierungsvorschriften erhoben und gespeichert, besteht keine Pflicht zur Information der betroffenen Personen.

§ 12

Aufgehoben.

§ 12a (neu)

Datenverarbeitung im Auftrag

[1] Auftragnehmende für die Bearbeitung von Personendaten sind vom öffentlichen Organ unter besonderer Berücksichtigung der von jenen getroffenen technischen und organisatorischen Massnahmen sorgfältig auszuwählen. Durch Vertrag oder Auflagen sind festzulegen:

a) Gegenstand und Dauer des Auftrags,
b) Umfang, Art und Zweck der vorgesehenen Datenbearbeitung, die Art der Daten und der Kreis der Betroffenen,
c) die zur Einhaltung der Datensicherheit zu treffenden technischen und organisatorischen Massnahmen, deren Kontrolle und Dokumentation,
d) Durchsetzung von Ansprüchen betroffener Personen,
e) Verpflichtung zur Verschwiegenheit und Überbindung dieser Pflicht auf alle Datenbearbeitenden,
f) allfällige Berechtigung zur Vergabe von Unteraufträgen,
g) Kontrollrechte des auftraggebenden öffentlichen Organs und entsprechende Duldungs- und Mitwirkungspflichten des Auftragnehmenden,
h) Mitteilungspflicht des Auftragnehmenden bei Verletzungen der Datensicherheit,
i) Weisungsbefugnis des öffentlichen Organs,
j) die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmenden gespeicherter Daten.

[2] Stellt die Bearbeitung von Personendaten nicht die Hauptpflicht des Auftragnehmenden dar, haben sich die Vereinbarung oder die Auflagen sinngemäss am Inhalt gemäss Abs. 1 zu orientieren.

§ 16
Aufgehoben.

§ 17
Aufgehoben.

§ 18
Aufgehoben.

§ 19 Abs. 1 (geändert), **Abs. 2 (aufgehoben)**, **Abs. 3 (neu)**

[1] Gesuche um Auskunft und/oder Zugang zu amtlichen Dokumenten sind nach Möglichkeit innert 10 Tagen zu erledigen.

[2] *Aufgehoben.*

[3] Öffentliche Organe geben innert 30 Tagen nach Erhalt einer Empfehlung gemäss § 32 Abs. 3 IDAG schriftlich eine Erklärung ab, ob sie die Empfehlung annehmen.

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

Zusammenarbeit; Behördenbeschwerde (Überschrift geändert)

[1] Stellen sich Fragen zur Informatiksicherheit oder andere die Informatik betreffende Fragen, holt die beauftragte Person für Öffentlichkeit und Datenschutz die Stellungnahme des Departements Finanzen und Ressourcen ein.

[2] Die öffentlichen Organe holen vor dem Erlass von Gesetzen, Verordnungen, Richtlinien, Reglementen oder Weisungen im Anwendungsbereich des IDAG die Stellungnahme der beauftragten Person für Öffentlichkeit und Datenschutz ein.

[3] Entscheide im Anwendungsbereich des IDAG sind der beauftragten Person für Öffentlichkeit und Datenschutz zuzustellen, soweit sie nicht ohnehin Partei ist. Sie ist zur Erhebung von Verwaltungs- und von Verwaltungsgerichtsbeschwerden befugt.

[4] Hatte die beauftragte Person für Öffentlichkeit und Datenschutz die Möglichkeit zur Erhebung der Beschwerde, erlässt sie weder Empfehlungen noch Verfügungen in der gleichen Sache, sofern nicht Wiedererwägungsgründe gemäss § 39 Abs. 2 des Gesetzes über die Verwaltungsrechtspflege (Verwaltungsrechtspflegegesetz, VRPG) vom 4. Dezember 2007 [1)] vorliegen.

[1)] SAR 271.200

§ 25
Aufgehoben.

II.

Keine Fremdänderungen.

III.

Keine Fremdaufhebungen.

IV.

Die Änderung unter Ziff. I. tritt am 1. August 2018 in Kraft.

Aarau, 23. Mai 2018

Regierungsrat Aargau

Landammann
HÜRZELER

Staatsschreiberin
TRIVIGNO