

**Gesetzentwurf  
der Landesregierung**

**Gesetz zur Anpassung des allgemeinen Datenschutzrechts  
und sonstiger Vorschriften an die Verordnung (EU) 2016/679**

A. Zielsetzung

In allen Mitgliedstaaten der Europäischen Union gilt ab dem 25. Mai 2018 die 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. Mai 2016, S. 1, ber. ABl. L 314 vom 22. November 2016, S. 72) unmittelbar. Die Verordnung (EU) 2016/679 schafft damit ein verbindliches Schutzniveau für die Rechte und Freiheiten von natürlichen Personen bei der Verarbeitung von personenbezogenen Daten in allen Mitgliedstaaten, das auch alle öffentlichen Stellen zu beachten haben, soweit sie personenbezogene Daten im Anwendungsbereich der Verordnung (EU) 2016/679 verarbeiten.

Wegen des Anwendungsvorrangs des europäischen Rechts ergibt sich die Notwendigkeit, die landesrechtlichen Datenschutzregelungen an die Verordnung (EU) 2016/679 anzupassen.

B. Wesentlicher Inhalt

Der Gesetzentwurf sieht folgende Gesetzesänderungen vor:

1. Neufassung des Landesdatenschutzgesetzes

Das neue Landesdatenschutzgesetz (LDSG) gilt im Anwendungsbereich der Verordnung (EU) 2016/679 wie bisher für alle öffentlichen Stellen des Landes. Wegen der unmittelbaren Geltung der Verordnung enthält es nur noch ergänzende Regelungen, soweit diese aufgrund der verbliebenen Regelungsspielräume möglich sind. Das bisherige Landesdatenschutzgesetz enthielt eine vollständige Regelung der allgemeinen datenschutzrechtlichen Anforderungen.

Bei der Neuregelung wird im öffentlichen Interesse insbesondere von der Öffnungsklausel in der Verordnung (EU) 2016/679 zur Beschränkung der Zweckbindung sowie der Betroffenenrechte Gebrauch gemacht.

Die oder der Landesbeauftragte für den Datenschutz wird als oberste Landesbehörde eingerichtet, um die geforderte völlige Unabhängigkeit der Aufsichtsbehörde herzustellen. Die bisherige Anbindung an den Landtag wird aufgelöst. Die Ausgestaltung des Dienstverhältnisses als öffentlich-rechtliches Amtsverhältnis eigener Art sichert die Unabhängigkeit ab.

## 2. Weitere Änderungen

Infolge der Verordnung (EU) 2016/679 sind Anpassungen des Landesinformationsfreiheitsgesetzes erforderlich, um das Informationsrecht in Einklang mit dem Schutz personenbezogener Daten zu bringen (Artikel 5).

Mit Artikel 15 und 16 werden das Abschiebungshaftvollzugsgesetz und die Abschiebungshaftvollzugsverordnung an die Verordnung (EU) 2016/679 angepasst. Zusätzlich wird in das Abschiebungshaftvollzugsgesetz eine Regelung aufgenommen, wonach dieses zukünftig auch auf den Vollzug des Ausreisegewahrsams im Sinne des § 62 b des Aufenthaltsgesetzes entsprechende Anwendung findet. Außerdem wird eine erweiterte Beschränkungsbefugnis für Fälle vorgesehen, in denen von Untergebrachten eine erhebliche Gefahr für Leib oder Leben Dritter oder bedeutende Rechtsgüter der inneren Sicherheit ausgeht.

Im Landesbeamtengesetz, im Landesdisziplinargesetz und im Landespersonalvertretungsgesetz werden in Artikel 17 bis 19, neben den erforderlichen Anpassungen an die Verordnung (EU) 2016/679, für den Bereich des Dienstrechts bereichsspezifische Regelungen zur Datenverarbeitung im Beschäftigungskontext getroffen.

## C. Alternativen

Keine. Dem Systemwechsel im Datenschutzrecht durch die ab dem 25. Mai 2018 unmittelbar geltende Verordnung (EU) 2016/679 wird nur eine Neufassung des Landesdatenschutzgesetzes gerecht.

## D. Kosten für die öffentlichen Haushalte

Die datenschutzrechtlichen Betroffenenrechte und damit die Pflichten des Verantwortlichen gegenüber der betroffenen Person werden durch die Verordnung (EU) 2016/679 gestärkt. Darüber hinaus ist jede öffentliche Stelle verpflichtet, einen Datenschutzbeauftragten zu benennen. Dadurch entstehen zusätzliche Kosten für die Landesverwaltung und die kommunalen Haushalte, die aber durch die Verordnung (EU) 2016/679 und nicht durch dieses Gesetz verursacht werden.

Da die Verordnung (EU) 2016/679 der Aufsichtsbehörde zusätzliche Aufgaben auferlegt, wird bei der oder dem Landesbeauftragten für den Datenschutz erhöhter Personalbedarf entstehen. Die daraus folgenden Personal- und Sachkosten sind ebenfalls allein auf die europäischen Bestimmungen zurückzuführen.

## E. Kosten für Private

Für Private ergeben sich aus der Anwendung dieses Gesetzes keine zusätzlichen Kosten. Für privatrechtlich organisierte öffentliche Stellen gelten die oben unter D. gemachten Ausführungen.

**Staatsministerium  
Baden-Württemberg  
Ministerpräsident**

Stuttgart, 19. April 2018

An die  
Präsidentin des Landtags  
von Baden-Württemberg

Sehr geehrte Frau Landtagspräsidentin,

in der Anlage übersende ich Ihnen gemäß Artikel 59 Absatz 1 der Landesverfassung den von der Landesregierung beschlossenen Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679. Ich bitte, die Beschlussfassung des Landtags herbeizuführen. Federführend ist das Innenministerium zuständig. Beteiligt waren alle Ministerien des Landes.

Mit freundlichen Grüßen

Kretschmann  
Ministerpräsident

Der Landtag wolle beschließen,  
dem nachstehenden Gesetzentwurf seine Zustimmung zu erteilen:

**Gesetz zur Anpassung des allgemeinen  
Datenschutzrechts und sonstiger  
Vorschriften an die Verordnung  
(EU) 2016/679**

Artikel 1

Landesdatenschutzgesetz (LDSG)

INHALTSÜBERSICHT

Abschnitt 1: Allgemeine Bestimmungen

- § 1 Zweck des Gesetzes
- § 2 Anwendungsbereich
- § 3 Sicherstellung des Datenschutzes

Abschnitt 2: Rechtsgrundlagen der Verarbeitung personenbezogener Daten

- § 4 Zulässigkeit der Verarbeitung personenbezogener Daten
- § 5 Datenverarbeitung zu anderen Zwecken (Ergänzung zu Artikel 6 Absatz 3 und 4 der Verordnung [EU] 2016/679)
- § 6 Übermittlung personenbezogener Daten
- § 7 Datenverarbeitung in der gemeinsamen Dienststelle

Abschnitt 3: Rechte der betroffenen Person

- § 8 Beschränkung der Informationspflicht (Ergänzung zu Artikel 13 und 14 der Verordnung [EU] 2016/679)
- § 9 Beschränkung des Auskunftsrechts (Ergänzung zu Artikel 15 der Verordnung [EU] 2016/679)
- § 10 Beschränkung des Rechts auf Löschung (Ergänzung zu Artikel 17 der Verordnung [EU] 2016/679)
- § 11 Beschränkung der Benachrichtigungspflicht (Ergänzung zu Artikel 34 der Verordnung [EU] 2016/679)

## Abschnitt 4: Besondere Verarbeitungssituationen

- § 12 Verarbeitung personenbezogener Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen
- § 13 Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken
- § 14 Datenverarbeitung zu im öffentlichen Interesse liegenden Archivzwecken
- § 15 Datenverarbeitung bei Dienst- und Arbeitsverhältnissen
- § 16 Öffentliche Auszeichnungen und Ehrungen
- § 17 Verarbeitung personenbezogener Daten im öffentlichen Interesse
- § 18 Videoüberwachung öffentlich zugänglicher Räume
- § 19 Verarbeitung personenbezogener Daten zu künstlerischen und literarischen Zwecken

## Abschnitt 5: Unabhängige Aufsichtsbehörden

- § 20 Errichtung
- § 21 Unabhängigkeit
- § 22 Ernennung und Amtszeit
- § 23 Amtsverhältnis
- § 24 Rechte und Pflichten
- § 25 Aufgaben und Befugnisse
- § 26 Pflicht zur Unterstützung
- § 27 Rundfunkbeauftragte oder Rundfunkbeauftragter für den Datenschutz

## Abschnitt 6: Sanktionen

- § 28 Ordnungswidrigkeiten (Ergänzung zu Artikel 83 Absatz 7 der Verordnung [EU] 2016/679)
- § 29 Strafvorschrift (Ergänzung zu Artikel 84 der Verordnung [EU] 2016/679)

## Abschnitt 7: Übergangsbestimmungen

- § 30 Polizeibehörden und Polizeivollzugsdienst, Justizbehörden, Landesamt für Verfassungsschutz und Vollzug des Landessicherheitsüberprüfungsgesetzes
- § 31 Überleitungsvorschriften

## Abschnitt 1

## Allgemeine Bestimmungen

## § 1

*Zweck des Gesetzes*

Dieses Gesetz trifft ergänzende Regelungen zur Durchführung der 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. Mai 2016, S. 1, ber. ABl. L 314 vom 22. November 2016, S. 72) in der jeweils geltenden Fassung sowie Regelungen für die Verarbeitung personenbezogener Daten im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt.

## § 2

*Anwendungsbereich*

(1) Dieses Gesetz gilt nach Maßgabe von Absatz 2 bis 7 für die Verarbeitung personenbezogener Daten durch Behörden und sonstige Stellen des Landes, der Gemeinden und Gemeindeverbände und der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts (öffentliche Stellen). Die öffentliche Stelle ist zugleich Verantwortlicher nach Artikel 4 Nummer 7 der Verordnung (EU) 2016/679, soweit dieses Gesetz nichts anderes bestimmt. Dieses Gesetz gilt nicht für die Verarbeitung personenbezogener Daten

1. durch das Landesamt für Verfassungsschutz im Rahmen der Erfüllung seiner Aufgaben nach § 3 des Landesverfassungsschutzgesetzes,
2. beim Vollzug des Landessicherheitsüberprüfungsgesetzes,
3. durch die Polizei sowie die Gerichte, Staatsanwaltschaften, das Justizministerium und die Justizvollzugsbehörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten und Ordnungswidrigkeiten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit und
4. durch andere für die Verfolgung und Ahndung von Ordnungswidrigkeiten zuständige Stellen,

soweit besondere Rechtsvorschriften keine abweichenden Regelungen treffen. § 30 gilt auch für die Verarbeitung personenbezogener Daten nach Satz 3.

(2) Als öffentliche Stellen gelten auch juristische Personen und sonstige Vereinigungen des privaten Rechts, die Aufgaben der öffentlichen Verwaltung wahrnehmen und

an denen eine oder mehrere der in Absatz 1 genannten juristischen Personen des öffentlichen Rechts mit absoluter Mehrheit der Anteile oder absoluter Mehrheit der Stimmen beteiligt sind. Beteiligt sich eine juristische Person oder sonstige Vereinigung des privaten Rechts nach Satz 1 an einer weiteren Vereinigung des privaten Rechts, findet Satz 1 entsprechende Anwendung. Nehmen nichtöffentliche Stellen hoheitliche Aufgaben der öffentlichen Verwaltung wahr, sind sie insoweit öffentliche Stellen im Sinne dieses Gesetzes.

(3) Soweit besondere Rechtsvorschriften des Bundes oder des Landes auf personenbezogene Daten anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor. Die Vorschriften dieses Gesetzes gehen denen des Landesverwaltungsverfahrensgesetzes vor, soweit bei der Ermittlung des Sachverhalts personenbezogene Daten verarbeitet werden.

(4) Soweit die Verarbeitung personenbezogener Daten im Rahmen einer Tätigkeit stattfindet, die nicht in den sachlichen Anwendungsbereich der Verordnung (EU) 2016/679 oder der 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. Mai 2016, S. 89) fällt, gelten die Regelungen der Verordnung (EU) 2016/679 und dieses Gesetz entsprechend, sofern die Verarbeitung nicht in besonderen Rechtsvorschriften geregelt ist. Die Artikel 30, 35 und 36 der Verordnung (EU) 2016/679 gelten nur, soweit die Verarbeitung personenbezogener Daten automatisiert erfolgt oder die Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Auf die Prüfungstätigkeit des Rechnungshofs und der staatlichen Rechnungsprüfungsämter finden Artikel 30 und Kapitel VI der Verordnung (EU) 2016/679 sowie §§ 25 und 26 dieses Gesetzes keine Anwendung.

(5) Dieses Gesetz gilt für den Landtag sowie unbeschadet des Absatz 1 Nummer 3 für die Gerichte nur, soweit sie in Verwaltungsangelegenheiten tätig werden.

(6) Soweit öffentliche Stellen als Unternehmen mit eigener Rechtspersönlichkeit am Wettbewerb teilnehmen, sind die für nichtöffentliche Stellen geltenden datenschutzrechtlichen Vorschriften entsprechend anzuwenden. Satz 1 gilt nicht für Zweckverbände.

(7) Die Vorschriften dieses Gesetzes gelten nicht für die Verarbeitung personenbezogener Daten zur Ausübung des Begnadigungsrechts.

## § 3

*Sicherstellung des Datenschutzes*

(1) Bei der Datenverarbeitung sind angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen. Dabei sind der Stand der Technik, die Implementierungskosten, die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen. Zu den Maßnahmen können insbesondere gehören:

1. technische und organisatorische Maßnahmen, um sicherzustellen, dass die Verarbeitung gemäß der Verordnung [EU] 2016/679 erfolgt,
2. Maßnahmen, die die nachträgliche Überprüfung und Feststellung gewährleisten, ob und von wem personenbezogene Daten erfasst, verändert oder gelöscht worden sind,
3. die Sensibilisierung und Schulung der an Verarbeitungsvorgängen Beteiligten,
4. die Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der öffentlichen Stelle und von Auftragsverarbeitern,
5. die Pseudonymisierung personenbezogener Daten,
6. die Verschlüsselung personenbezogener Daten,
7. die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten auf Dauer sicherzustellen, einschließlich der Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen,
8. die Einrichtung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung und
9. spezifische Verfahrensregelungen, die im Fall einer Übermittlung oder Verarbeitung personenbezogener Daten für andere Zwecke die Einhaltung der Vorgaben dieses Gesetzes sowie der Verordnung [EU] 2016/679 sicherstellen.

(2) Den bei öffentlichen Stellen beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu verarbeiten (Datengeheimnis). Das Datengeheimnis besteht nach Beendigung ihrer Tätigkeit fort.

## Abschnitt 2

Rechtsgrundlagen der Verarbeitung  
personenbezogener Daten

## § 4

*Zulässigkeit der Verarbeitung  
personenbezogener Daten*

Die Verarbeitung personenbezogener Daten ist unbeschadet sonstiger Bestimmungen zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der öffentlichen Stelle liegenden Aufgabe oder in Ausübung öffentlicher Gewalt, die der öffentlichen Stelle übertragen wurde, erforderlich ist.

## § 5

*Datenverarbeitung zu anderen Zwecken  
(Ergänzung zu Artikel 6 Absatz 3 und 4  
der Verordnung [EU] 2016/679)*

(1) Die Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem sie erhoben wurden, ist unbeschadet der Bestimmungen der Verordnung [EU] 2016/679 zulässig, wenn

1. sie zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer unmittelbar drohenden Gefahr für die öffentliche Sicherheit oder zur Wahrung erheblicher Belange des Gemeinwohls erforderlich ist,
2. sie zum Schutz der betroffenen Person oder zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte und Freiheiten einer anderen Person erforderlich ist,
3. sich bei der rechtmäßigen Aufgabenerfüllung Anhaltspunkte für Straftaten oder Ordnungswidrigkeiten von erheblicher Bedeutung ergeben und die Unterrichtung der für die Verhütung, Verfolgung oder Vollstreckung zuständigen Behörden erforderlich ist oder
4. Angaben der betroffenen Person überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,

soweit die Verarbeitung notwendig und verhältnismäßig ist.

(2) Eine Verarbeitung gilt als mit den ursprünglichen Zwecken vereinbar, wenn sie

1. für die Wahrnehmung von Aufsichts- und Kontrollbefugnissen benötigt wird oder
2. der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen oder der Prüfung und Wartung von automatisierten Verfahren dient.

Dies gilt auch für die Verarbeitung zu eigenen Aus- und Fortbildungszwecken, soweit schutzwürdige Belange der betroffenen Person nicht entgegenstehen.

(3) Abweichend von Artikel 13 der Verordnung [EU] 2016/679 erfolgt eine Information der betroffenen Person über die Datenverarbeitung nach Absatz 1 Nummern 1 bis 4 nicht, soweit und solange hierdurch der Zweck der Verarbeitung gefährdet würde und die Interessen der öffentlichen Stelle an der Nichterteilung der Information die Interessen der betroffenen Person überwiegen.

(4) Personenbezogene Daten, die ausschließlich zum Zweck der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage verarbeitet werden, dürfen nur für diesen Zweck und hiermit in Zusammenhang stehende Maßnahmen gegenüber Beschäftigten verarbeitet werden oder soweit dies zur Verhütung oder Verfolgung von Straftaten gegen Leib, Leben oder Freiheit einer Person erforderlich ist.

## § 6

### *Übermittlung personenbezogener Daten*

(1) Die Übermittlung personenbezogener Daten zu anderen als ihren Erhebungszwecken ist zulässig, wenn

1. sie zur Erfüllung einer der übermittelnden oder der empfangenden öffentlichen Stelle obliegenden Aufgabe erforderlich ist und die Voraussetzungen vorliegen, die eine Verarbeitung nach § 5 zulassen würden oder
2. der Empfänger eine nichtöffentliche Stelle ist, die ein berechtigtes Interesse an ihrer Kenntnis glaubhaft darlegt und die betroffene Person kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat; dies gilt auch, soweit die Daten zu anderen Zwecken als denjenigen, zu denen sie erhoben wurden, übermittelt werden.

(2) Die Verantwortung für die Zulässigkeit der Übermittlung personenbezogener Daten trägt die übermittelnde öffentliche Stelle. Erfolgt die Übermittlung an eine öffentliche Stelle im Geltungsbereich des Grundgesetzes auf deren Ersuchen, trägt diese die Verantwortung und erteilt die Informationen nach Artikel 14 der Verordnung [EU] 2016/679. Die übermittelnde öffentliche Stelle hat im Falle des Satzes 2 lediglich zu prüfen, ob das Übermittlungsersuchen im Rahmen der Aufgaben der ersuchenden öffentlichen Stelle liegt. Die Rechtmäßigkeit des Ersuchens prüft sie nur, wenn im Einzelfall hierzu Anlass besteht.

(3) Erfolgt die Übermittlung aufgrund eines automatisierten Verfahrens, welches die Übermittlung personenbezogener Daten durch Abruf ermöglicht, trägt die Verantwortung für die Rechtmäßigkeit des Abrufs der Dritte, an den übermittelt wird. Die übermittelnde Stelle prüft die Zulässigkeit des Abrufs nur, wenn dazu Anlass besteht. Sie hat zu gewährleisten, dass die Übermittlung personenbezogener Daten zumindest durch geeignete

Stichprobenverfahren festgestellt und überprüft werden kann.

### § 7

#### *Datenverarbeitung in der gemeinsamen Dienststelle*

(1) Die örtlich zuständige öffentliche Stelle darf personenbezogene Daten nur den in einer gemeinsamen Dienststelle nach § 16 Absatz 1 des Landesverwaltungsgesetzes beschäftigten eigenen Bediensteten zur Verarbeitung für eigene Aufgaben überlassen. Durch technische und organisatorische Maßnahmen ist sicherzustellen, dass ein Zugriff auf die Daten nach Satz 1 durch Bedienstete anderer Behörden nicht möglich ist. Soweit dies zur Sicherstellung einer sachgerechten Erledigung der eigenen Aufgaben erforderlich ist, darf die örtlich zuständige öffentliche Stelle auch Bediensteten anderer Behörden, die in der gemeinsamen Dienststelle beschäftigt sind, personenbezogene Daten zur Verarbeitung überlassen. Im Rahmen einer solchen Datenverarbeitung unterliegen die Bediensteten anderer Behörden den Weisungen der örtlich zuständigen öffentlichen Stelle. Hinsichtlich der Daten, die sie im Rahmen ihrer Tätigkeit für die fremde Behörde zur Kenntnis nehmen, haben sie das Datengeheimnis gegenüber ihrer eigenen Dienststelle zu wahren. Das Nähere ist durch gemeinsame interne Dienst-Anweisungen zu regeln. Verantwortlicher bleibt die örtlich zuständige öffentliche Stelle.

(2) Für gemeinsame Dienststellen nach § 27 des Gesetzes über kommunale Zusammenarbeit gilt Absatz 1 entsprechend.

### Abschnitt 3

#### Rechte der betroffenen Person

### § 8

#### *Beschränkung der Informationspflicht (Ergänzung zu Artikel 13 und 14 der Verordnung [EU] 2016/679)*

(1) Eine Pflicht zur Information der betroffenen Person besteht nicht, soweit und solange

1. die Information die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde,
2. die Information die Verhütung oder Verfolgung von Straftaten oder Ordnungswidrigkeiten gefährden würde,
3. die Information die Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche beeinträchtigen würde,
4. die Daten oder die Tatsache der Verarbeitung nach einer Rechtsvorschrift oder zum Schutze der betroffe-

nen Person oder der Rechte und Freiheiten anderer Personen geheim gehalten werden müssen oder

5. die Information voraussichtlich die Verwirklichung des wissenschaftlichen oder historischen Forschungszwecks unmöglich macht oder ernsthaft beeinträchtigt

und deswegen das Interesse der betroffenen Person an der Informationserteilung zurücktreten muss.

(2) Bezieht sich die Informationserteilung auf die Übermittlung personenbezogener Daten an Staatsanwaltschaften, Polizeibehörden oder den Polizeivollzugsdienst, Verfassungsschutzbehörden und, soweit sie in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung personenbezogener Daten speichern, an Behörden der Finanzverwaltung, ist diesen Behörden vorab Gelegenheit zur Stellungnahme zu geben. Satz 1 findet auch Anwendung auf die Übermittlung personenbezogener Daten an den Bundesnachrichtendienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, an andere Behörden des Bundesministers der Verteidigung. Satz 1 und 2 gelten entsprechend für die Information über die Herkunft der Daten von den genannten Behörden.

(3) Die Gründe für das Absehen von der Information sind zu dokumentieren.

## § 9

### *Beschränkung des Auskunftsrechts (Ergänzung zu Artikel 15 der Verordnung [EU] 2016/679)*

(1) Die Auskunftserteilung kann aus den in § 8 Absatz 1 Nummern 1 bis 4 genannten Gründen abgelehnt werden. Die betroffene Person kann ferner keine Auskunft verlangen, soweit und solange die personenbezogenen Daten ausschließlich zu Zwecken der Datensicherung oder der Datenschutzkontrolle gespeichert sind und eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist und deswegen das Interesse der betroffenen Person an der Auskunftserteilung zurücktreten muss.

(2) Sofern die öffentliche Stelle eine große Menge von Informationen über die betroffene Person verarbeitet, kann sie sich auf die Benennung der Verarbeitungsvorgänge und der Art der verarbeiteten Daten beschränken, wenn sie im Übrigen von der betroffenen Person eine Präzisierung verlangt, auf welche Information oder welche Verarbeitungsvorgänge sich ihr Auskunftersuchen bezieht. Kommt die betroffene Person dem Verlangen nicht nach, kann die Auskunft verweigert werden, soweit die Auskunftserteilung einen unzumutbaren Aufwand auslösen würde.

(3) § 8 Absatz 2 gilt entsprechend.

(4) Die Ablehnung der Auskunftserteilung ist zu begründen, es sei denn, durch die Mitteilung der Gründe würde der mit der Auskunftsverweigerung verfolgte Zweck gefährdet. In diesem Fall sind die Gründe der Auskunftsverweigerung zu dokumentieren. Die betroffene Person ist auf die Möglichkeit der Beschwerde bei der oder dem Landesbeauftragten für den Datenschutz hinzuweisen.

(5) Wird der betroffenen Person keine Auskunft erteilt, ist sie auf ihr Verlangen der oder dem Landesbeauftragten für den Datenschutz zu erteilen, soweit nicht die jeweils zuständige oberste Landesbehörde im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. Die Mitteilung der oder des Landesbeauftragten für den Datenschutz an die betroffene Person über das Ergebnis der datenschutzrechtlichen Prüfung darf keine Rückschlüsse auf den Erkenntnisstand der öffentlichen Stelle zulassen, sofern diese nicht einer weiter gehenden Auskunft zustimmt.

#### § 10

*Beschränkung des Rechts auf Löschung  
(Ergänzung zu Artikel 17 der Verordnung  
[EU] 2016/679)*

(1) Die Bestimmungen des Landesarchivgesetzes zur Anbietungspflicht sowie sonstige gesetzliche oder satzungsmäßige Dokumentations- und Aufbewahrungspflichten bleiben unberührt.

(2) Die Pflicht zur Löschung personenbezogener Daten nach Artikel 17 der Verordnung [EU] 2016/679 besteht nicht, wenn Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen der betroffenen Person beeinträchtigt würden. In diesem Fall tritt an die Stelle einer Löschung eine Einschränkung der Verarbeitung nach Artikel 18 der Verordnung [EU] 2016/679. Die öffentliche Stelle unterrichtet die betroffene Person über das Absehen von der Löschung und die Einschränkung der Verarbeitung. Widerspricht die betroffene Person dem Absehen von der Löschung, sind die Daten zu löschen.

(3) Ist eine Löschung im Falle nichtautomatisierter Datenverarbeitung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich und ist das Interesse der betroffenen Person an der Löschung als gering anzusehen, besteht das Recht der betroffenen Person auf und die Pflicht der öffentlichen Stelle zur Löschung personenbezogener Daten nicht. In diesem Fall tritt an die Stelle einer Löschung eine Einschränkung der Verarbeitung nach Artikel 18 der Verordnung [EU] 2016/679. Satz 1 und 2 finden keine Anwendung, wenn die personenbezogenen Daten unrechtmäßig verarbeitet wurden.

## § 11

*Beschränkung der Benachrichtigungspflicht  
(Ergänzung zu Artikel 34 der Verordnung  
[EU] 2016/679)*

Die öffentliche Stelle kann von der Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person absehen, soweit und solange

1. die Benachrichtigung die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde,
2. die Daten oder die Tatsache der Verarbeitung nach einer Rechtsvorschrift oder zum Schutze der betroffenen Person oder der Rechte anderer Personen geheim gehalten werden müssen oder
3. die Benachrichtigung die Sicherheit von Systemen der Informationstechnologie gefährden würde

und deswegen das Interesse der betroffenen Person an der Benachrichtigung zurücktreten muss.

## Abschnitt 4

## Besondere Verarbeitungssituationen

## § 12

*Verarbeitung personenbezogener Daten,  
die einem Berufs- oder besonderen  
Amtsgeheimnis unterliegen*

(1) Personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen und die der öffentlichen Stelle in Ausübung einer Berufs- oder Amtspflicht übermittelt worden sind, dürfen von der öffentlichen Stelle nur für den Zweck verarbeitet werden, für den sie die Daten erhalten hat. Artikel 9 der Verordnung (EU) 2016/679 bleibt unberührt.

(2) Für einen anderen Zweck dürfen die Daten nur verarbeitet werden, wenn

1. die Änderung des Zwecks durch besonderes Gesetz zugelassen ist oder
2. die Voraussetzungen des § 5 Absatz 1 Nummern 1 bis 3, § 13 Absatz 1 oder § 14 Absatz 1 vorliegen und die zur Verschwiegenheit verpflichtete Stelle zugestimmt hat.

## § 13

*Datenverarbeitung zu wissenschaftlichen  
oder historischen Forschungszwecken  
und zu statistischen Zwecken*

(1) Öffentliche Stellen dürfen personenbezogene Daten einschließlich besonderer Kategorien personenbezogener

Daten für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke verarbeiten, wenn die Zwecke auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden können und die Interessen der öffentlichen Stelle an der Durchführung des Forschungs- oder Statistikvorhabens die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung überwiegen. Besondere Kategorien personenbezogener Daten sind die in Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 genannten Daten.

(2) Die personenbezogenen Daten sind zu anonymisieren, sobald dies nach dem Forschungs- oder Statistikzweck möglich ist, es sei denn, berechnete Interessen der betroffenen Person stehen dem entgegen. Bis zur Anonymisierung sind die Merkmale gesondert zu speichern, mit denen Einzelangaben einer bestimmten oder bestimmbarer Person zugeordnet werden können. Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungs- oder Statistikzweck dies erfordert.

(3) Die wissenschaftliche oder historische Forschung betreibenden öffentlichen Stellen dürfen personenbezogene Daten außer bei Einwilligung nur veröffentlichen, soweit dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist.

(4) Die in Artikel 15, 16, 18 und 21 der Verordnung (EU) 2016/679 vorgesehenen Rechte der betroffenen Person sind insoweit beschränkt, als diese Rechte voraussichtlich die Verwirklichung der jeweiligen Forschungs- oder Statistikzwecke unmöglich machen oder ernsthaft beeinträchtigen und die Beschränkung für die Erfüllung der jeweiligen Forschungs- oder Statistikzwecke notwendig ist. Das Recht auf Auskunft gemäß Artikel 15 der Verordnung (EU) 2016/679 besteht darüber hinaus nicht, wenn die Daten für Zwecke der wissenschaftlichen Forschung erforderlich sind und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde.

#### § 14

##### *Datenverarbeitung zu im öffentlichen Interesse liegenden Archivzwecken*

(1) Die Verarbeitung besonderer Kategorien personenbezogener Daten ist zulässig, wenn sie für im öffentlichen Interesse liegende Archivzwecke erforderlich ist.

(2) Das Recht auf Auskunft der betroffenen Person gemäß Artikel 15 der Verordnung (EU) 2016/679 besteht nicht, wenn das Archivgut nicht durch den Namen der Person erschlossen ist oder keine Angaben gemacht werden, die das Auffinden des betreffenden Archivguts mit vertretbarem Verwaltungsaufwand ermöglichen.

(3) Das Recht auf Berichtigung der betroffenen Person gemäß Artikel 16 der Verordnung (EU) 2016/679 be-

steht nicht, wenn die personenbezogenen Daten zu Archivzwecken im öffentlichen Interesse verarbeitet werden. Bestreitet die betroffene Person die Richtigkeit der personenbezogenen Daten, ist ihr die Möglichkeit einer Gegendarstellung einzuräumen. Das zuständige Archiv ist verpflichtet, die Gegendarstellung den Unterlagen hinzuzufügen.

(4) Die in Artikel 18, 19, 20 und 21 der Verordnung (EU) 2016/679 vorgesehenen Rechte bestehen nicht, soweit diese Rechte voraussichtlich die Verwirklichung der im öffentlichen Interesse liegenden Archivzwecke unmöglich machen oder ernsthaft beeinträchtigen und die Ausnahmen für die Erfüllung dieser Zwecke erforderlich sind.

(5) Soweit öffentliche Stellen verpflichtet sind, Unterlagen einem öffentlichen Archiv zur Übernahme anzubieten, ist eine Löschung erst zulässig, nachdem die Unterlagen dem öffentlichen Archiv angeboten und von diesem nicht als archivwürdig übernommen worden sind oder über die Übernahme nicht innerhalb der gesetzlichen Frist entschieden worden ist.

## § 15

### *Datenverarbeitung bei Dienst- und Arbeitsverhältnissen*

(1) Personenbezogene Daten von Bewerberinnen und Bewerbern sowie Beschäftigten dürfen verarbeitet werden, soweit dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des jeweiligen Dienst- oder Arbeitsverhältnisses oder zur Durchführung innerdienstlich planerischer, organisatorischer, personeller, sozialer oder haushalts- und kostenrechnerischer Maßnahmen, insbesondere zu Zwecken der Personalplanung und des Personaleinsatzes, erforderlich oder in einer Rechtsvorschrift, einem Tarifvertrag oder einer Dienst- oder Betriebsvereinbarung (Kollektivvereinbarung) vorgesehen ist. Die Verarbeitung ist auch zulässig, wenn sie zur Ausübung oder Erfüllung der sich aus einem Gesetz, einem Tarifvertrag oder einer Kollektivvereinbarung ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist.

(2) Besondere Kategorien personenbezogener Daten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, soweit die Verarbeitung erforderlich ist, um den Rechten und Pflichten der öffentlichen Stellen oder der betroffenen Person, auch aufgrund von Kollektivvereinbarungen, auf dem Gebiet des Dienst- und Arbeitsrechts sowie des Rechts der sozialen Sicherheit und des Sozialschutzes zu genügen und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt.

(3) Im Zusammenhang mit der Begründung eines Dienst- oder Arbeitsverhältnisses ist die Erhebung personenbe-

zogener Daten einer Bewerberin oder eines Bewerbers bei dem bisherigen Dienstherrn oder Arbeitgeber nur zulässig, wenn die betroffene Person eingewilligt hat. Satz 1 gilt entsprechend für die Übermittlung personenbezogener Daten an künftige Dienstherrn oder Arbeitgeber.

(4) Auf die Verarbeitung von Personalaktendaten von Arbeitnehmerinnen und Arbeitnehmern sowie Auszubildenden in einem privatrechtlichen Ausbildungsverhältnis finden die für Beamtinnen und Beamte geltenden Vorschriften des § 50 des Beamtenstatusgesetzes und der §§ 83 bis 88 des Landesbeamtengesetzes entsprechende Anwendung, es sei denn, besondere Rechtsvorschriften oder tarifliche Vereinbarungen gehen vor.

(5) Zur Aufdeckung von Straftaten und schwerwiegenden Pflichtverletzungen dürfen personenbezogene Daten von Beschäftigten nur dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat oder schwerwiegende Pflichtverletzung begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

(6) Die Verarbeitung biometrischer Daten von Beschäftigten zu Authentifizierungs- und Autorisierungszwecken ist untersagt, es sei denn, die betroffene Person hat ausdrücklich eingewilligt oder sie ist durch Dienst- oder Betriebsvereinbarung geregelt und für die Datenverarbeitung besteht jeweils ein dringendes dienstliches Bedürfnis.

(7) Eine Überwachung von Beschäftigten mit Hilfe optisch-elektronischer Einrichtungen zum Zwecke der Verhaltens- und Leistungskontrolle ist unzulässig. Absatz 5 bleibt unberührt. Für sonstige technische Einrichtungen gilt Absatz 1 entsprechend; die öffentliche Stelle muss geeignete Maßnahmen treffen, um sicherzustellen, dass insbesondere die in Artikel 5 der Verordnung (EU) 2016/679 dargelegten Grundsätze für die Verarbeitung personenbezogener Daten eingehalten werden.

(8) Beschäftigte sind alle bei öffentlichen Stellen beschäftigten Personen unabhängig von der Rechtsform des Beschäftigungsverhältnisses. Die Beteiligungsrechte der Interessenvertretungen der Beschäftigten bleiben unberührt.

## § 16

### *Öffentliche Auszeichnungen und Ehrungen*

(1) Zur Entscheidung über öffentliche Auszeichnungen und Ehrungen dürfen personenbezogene Daten einschließlich besonderer Kategorien personenbezogener Daten verarbeitet werden; die öffentlichen Stellen sind

insofern nicht zur Informations- und Auskunftserteilung gemäß Artikel 13 bis 15 der Verordnung (EU) 2016/679 verpflichtet.

(2) Zu anderen Zwecken dürfen die Daten nicht verarbeitet werden, es sei denn, sie werden für protokollarische Zwecke benötigt.

#### § 17

##### *Verarbeitung personenbezogener Daten im öffentlichen Interesse*

(1) Für die Überprüfung der Zuverlässigkeit von Besuchern, Mitarbeitern von Unternehmen und anderen Organisationen sowie sonstigen Personen, die in sicherheits- oder sicherheitstechnisch relevante Bereiche gelangen sollen, für die öffentliche Stellen Verantwortung tragen, gilt § 15 Absatz 1 Satz 1 entsprechend mit der Maßgabe, dass zusätzlich die Einwilligung der betroffenen Person erforderlich ist. Besondere Kategorien personenbezogener Daten sowie Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßnahmen dürfen nur aufgrund einer ausdrücklichen Einwilligung verarbeitet werden.

(2) Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten zulässig, wenn die Verarbeitung aus Gründen eines erheblichen öffentlichen Interesses oder zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist und die Interessen der öffentlichen Stelle an der Datenverarbeitung die Interessen der betroffenen Person überwiegen.

#### § 18

##### *Videoüberwachung öffentlich zugänglicher Räume*

(1) Die Beobachtung öffentlich zugänglicher Räume mit Hilfe optisch-elektronischer Einrichtungen (Videoüberwachung) sowie die Verarbeitung der dadurch erhobenen personenbezogenen Daten ist zulässig, soweit dies im Rahmen der Erfüllung öffentlicher Aufgaben oder in Ausübung des Hausrechts im Einzelfall erforderlich ist,

1. um Leben, Gesundheit, Freiheit oder Eigentum von Personen, die sich in öffentlichen Einrichtungen, öffentlichen Verkehrsmitteln, Amtsgebäuden oder sonstigen baulichen Anlagen öffentlicher Stellen oder in deren unmittelbarer Nähe aufhalten, oder
2. um Kulturgüter, öffentliche Einrichtungen, öffentliche Verkehrsmittel, Amtsgebäude oder sonstige bauliche Anlagen öffentlicher Stellen sowie die dort oder in deren unmittelbarer Nähe befindlichen Sachen

zu schützen und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der betroffenen Personen überwiegen.

(2) Die Videoüberwachung ist durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt erkennbar zu machen; dabei ist der Verantwortliche mitzuteilen.

(3) Für einen anderen Zweck dürfen die Daten nur weiterverarbeitet werden, soweit dies zur Abwehr von Gefahren für die öffentliche Sicherheit oder zur Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung oder von Straftaten erforderlich ist.

(4) Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, besteht die Pflicht zur Information der betroffenen Person über diese Verarbeitung nach Artikel 13 und 14 der Verordnung (EU) 2016/679. § 8 gilt entsprechend.

(5) Die Videoaufzeichnungen und daraus gefertigte oder sich auf die Videoüberwachung beziehende Unterlagen sind unverzüglich, spätestens jedoch vier Wochen nach der Datenerhebung zu löschen, soweit sie nicht zur Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung oder von Straftaten oder zur Geltendmachung von Rechtsansprüchen benötigt werden.

(6) Öffentliche Stellen haben ihren jeweiligen Datenschutzbeauftragten unbeschadet des Artikels 35 Absatz 2 der Verordnung (EU) 2016/679 rechtzeitig vor dem erstmaligen Einsatz einer Videoüberwachungseinrichtung den Zweck, die räumliche Ausdehnung und die Dauer der Videoüberwachung, den betroffenen Personenkreis, die Maßnahmen nach Absatz 2 und die vorgesehenen Auswertungen mitzuteilen und ihm Gelegenheit zur Stellungnahme zu geben.

## § 19

### *Verarbeitung personenbezogener Daten zu künstlerischen und literarischen Zwecken*

(1) Werden personenbezogene Daten zu künstlerischen und literarischen Zwecken verarbeitet, gelten neben Absatz 2 und 3 nur Artikel 5 Absatz 1 Buchstabe f in Verbindung mit Absatz 2, Artikel 24 und 32, sowie Kapitel I, VI, VIII, X und XI der Verordnung (EU) 2016/679. Artikel 82 der Verordnung (EU) 2016/679 gilt mit der Maßgabe, dass nur für unzureichende Maßnahmen nach Artikel 5 Absatz 1 Buchstabe f, Artikel 24 und 32 der Verordnung (EU) 2016/679 gehaftet wird. Den betroffenen Personen stehen nur die in Absatz 2 und 3 genannten Rechte zu.

(2) Führt die künstlerische oder literarische Offenlegung oder Verbreitung personenbezogener Daten zu hierauf bezogenen Maßnahmen wie Gegendarstellungen, Verpflichtungserklärungen, Gerichtsentscheidungen oder Widerrufen sind diese Maßnahmen zu den gespeicherten Daten zu nehmen und dort für dieselbe Zeitdauer aufzubewahren wie die Daten selbst und bei einer Übermittlung der Daten gemeinsam mit diesen zu übermitteln.

(3) Wird jemand durch die künstlerische oder literarische Offenlegung oder Verbreitung personenbezogener Daten in seinem Persönlichkeitsrecht beeinträchtigt, kann er Auskunft über die zugrunde liegenden, zu seiner Person gespeicherten Daten verlangen.

#### Abschnitt 5

#### Unabhängige Aufsichtsbehörden

#### § 20

##### *Errichtung*

(1) Die oder der Landesbeauftragte für den Datenschutz ist eine unabhängige, nur dem Gesetz unterworfen oberste Landesbehörde. Der Dienstsitz ist Stuttgart.

(2) Die oder der Landesbeauftragte für den Datenschutz ist Dienstvorgesetzte oder Dienstvorgesetzter der Beamtinnen und Beamten der Behörde. Die Beschäftigten der oder des Landesbeauftragten für den Datenschutz sind ausschließlich an ihre oder seine Weisungen gebunden.

(3) Die oder der Landesbeauftragte für den Datenschutz kann Aufgaben der Personalverwaltung und Personalwirtschaft auf andere Stellen des Landes übertragen, soweit hierdurch ihre oder seine Unabhängigkeit nicht beeinträchtigt wird. Diesen Stellen dürfen personenbezogene Daten der Beschäftigten übermittelt werden, soweit deren Kenntnis zur Erfüllung der übertragenen Aufgaben erforderlich ist. Die Aufgabenübertragung nach Satz 1 kann nur im Einvernehmen mit der anderen Stelle erfolgen.

#### § 21

##### *Unabhängigkeit*

(1) Die oder der Landesbeauftragte für den Datenschutz handelt bei der Erfüllung ihrer oder seiner Aufgaben und bei der Ausübung ihrer oder seiner Befugnisse völlig unabhängig.

(2) Die oder der Landesbeauftragte für den Datenschutz unterliegt der Rechnungsprüfung durch den Rechnungshof, soweit hierdurch ihre oder seine Unabhängigkeit nicht beeinträchtigt wird.

(3) Die Abgeordneten des Landtags sind berechtigt, Anfragen an die Landesbeauftragte für den Datenschutz oder den Landesbeauftragten für den Datenschutz zu richten, zu deren Beantwortung diese oder dieser nur verpflichtet ist, soweit hierdurch nicht ihre oder seine Unabhängigkeit beeinträchtigt wird.

## § 22

*Ernennung und Amtszeit*

(1) Der Landtag wählt ohne Aussprache auf Vorschlag der Landesregierung mit der Mehrheit seiner Mitglieder die Landesbeauftragte für den Datenschutz oder den Landesbeauftragten für den Datenschutz. Diese oder dieser soll neben der erforderlichen Erfahrung und Sachkunde insbesondere im Bereich des Schutzes personenbezogener Daten die Befähigung zum Richteramt oder zum höheren Verwaltungsdienst haben oder für eine andere Laufbahn des höheren Dienstes befähigt sein.

(2) Die oder der Gewählte wird von der Landtagspräsidentin oder dem Landtagspräsidenten ernannt. Sie oder er wird vor dem Landtag auf das Amt verpflichtet.

(3) Die Amtszeit der oder des Landesbeauftragten für den Datenschutz beträgt sechs Jahre. Die zweimalige Wiederwahl ist zulässig.

## § 23

*Amtsverhältnis*

(1) Die oder der Landesbeauftragte für den Datenschutz steht nach Maßgabe dieses Gesetzes in einem öffentlich-rechtlichen Amtsverhältnis zum Land.

(2) Die Landtagspräsidentin oder der Landtagspräsident kann die Landesbeauftragte für den Datenschutz oder den Landesbeauftragten für den Datenschutz ihres oder seines Amtes entheben, wenn diese oder dieser eine schwere Verfehlung begangen hat oder die Voraussetzungen für die Wahrnehmung ihrer oder seiner Aufgaben nicht mehr erfüllt. Die Amtsenthebung bedarf der Zustimmung von zwei Dritteln der Mitglieder des Landtags. Die Amtsenthebung wird mit der Zustellung der Urkunde durch die Landtagspräsidentin oder den Landtagspräsidenten wirksam.

(3) Die Leitende Beamtin oder der Leitende Beamte der Dienststelle der oder des Landesbeauftragten für den Datenschutz nimmt die Rechte und Pflichten der oder des Landesbeauftragten für den Datenschutz wahr, wenn die oder der Landesbeauftragte für den Datenschutz an der Ausübung ihres oder seines Amtes verhindert ist oder wenn ihr oder sein Amtsverhältnis geendet hat. § 21 Absatz 1 gilt in den genannten Fällen entsprechend.

(4) Die oder der Landesbeauftragte für den Datenschutz erhält vom Beginn des Kalendermonats an, in dem das Amtsverhältnis beginnt, bis zum Schluss des Kalendermonats, in dem das Amtsverhältnis endet, Bezüge in Höhe des Grundgehalts der Besoldungsgruppe B 5. Daneben werden der Familienzuschlag sowie sonstige Besoldungsbestandteile, Trennungsgeld, Reisekostenvergütung, Umzugskostenvergütung und Beihilfen in Krankheits-, Geburts- oder Todesfällen in sinngemäßer An-

wendung der für Beamtinnen und Beamte geltenden Vorschriften gewährt.

(5) Die oder der Landesbeauftragte für den Datenschutz erhält nach dem Ausscheiden aus dem Amt Versorgungsbezüge in sinngemäßer Anwendung der für Beamtinnen und Beamte geltenden Vorschriften.

## § 24

### *Rechte und Pflichten*

(1) Die oder der Landesbeauftragte für den Datenschutz hat von allen mit den Aufgaben ihres oder seines Amtes nicht zu vereinbarenden Handlungen abzusehen und während ihrer oder seiner Amtszeit keine andere mit ihrem oder seinem Amt nicht zu vereinbarende entgeltliche oder unentgeltliche Tätigkeit auszuüben. Insbesondere darf die oder der Landesbeauftragte für den Datenschutz neben ihrem oder seinem Amt kein anderes besoldetes Amt, kein Gewerbe und keinen Beruf ausüben und weder der Leitung, dem Aufsichtsrat oder Verwaltungsrat eines auf Erwerb gerichteten Unternehmens noch einer Regierung oder einer gesetzgebenden Körperschaft des Bundes oder eines Landes angehören. Sie oder er darf nicht gegen Entgelt außergerichtliche Gutachten abgeben.

(2) Die oder der Landesbeauftragte für den Datenschutz hat der Landtagspräsidentin oder dem Landtagspräsidenten Mitteilung über Geschenke zu machen, die sie oder er in Bezug auf das Amt erhält. Die Landtagspräsidentin oder der Landtagspräsident entscheidet über die Verwendung der Geschenke; sie oder er kann Verfahrensvorschriften erlassen.

(3) Die oder der Landesbeauftragte für den Datenschutz ist, auch nach Beendigung ihres oder seines Amtsverhältnisses, verpflichtet, über die ihr oder ihm amtlich bekannt gewordenen Angelegenheiten Verschwiegenheit zu bewahren. Dies gilt nicht für Mitteilungen im dienstlichen Verkehr oder Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Die oder der Landesbeauftragte für den Datenschutz entscheidet nach pflichtgemäßem Ermessen, ob und inwieweit sie oder er oder ihre oder seine Beschäftigten über solche Angelegenheiten vor Gericht oder außergerichtlich aussagen oder Erklärungen abgeben. Wenn sie oder er nicht mehr im Amt ist, ist die Genehmigung der oder des amtierenden Landesbeauftragten für den Datenschutz erforderlich. Satz 1, 2 und 4 gelten entsprechend für die Beschäftigten der oder des Landesbeauftragten für den Datenschutz nach Beendigung ihrer Tätigkeit bei ihrer oder seiner Dienststelle.

(4) Die oder der Landesbeauftragte für den Datenschutz hat für die Dauer von zwei Jahren nach der Beendigung ihrer oder seiner Amtszeit von allen mit den Aufgaben ihres oder seines früheren Amtes nicht zu vereinbaren-

den Handlungen und entgeltlichen oder unentgeltlichen Tätigkeiten abzusehen.

(5) Die oder der Landesbeauftragte für den Datenschutz darf als Zeugin oder Zeuge aussagen, es sei denn, die Aussage würde dem Wohle des Bundes oder eines Landes Nachteile bereiten, insbesondere Nachteile für die Sicherheit der Bundesrepublik Deutschland oder eines Landes oder ihre Beziehungen zu anderen Staaten, oder Grundrechte verletzen. Betrifft die Aussage laufende oder abgeschlossene Vorgänge, die dem Kernbereich exekutiver Eigenverantwortung der Landesregierung zuzurechnen sind oder sein könnten, darf die oder der Landesbeauftragte für den Datenschutz nur im Benehmen mit der Landesregierung aussagen.

## § 25

### *Aufgaben und Befugnisse*

(1) Die oder der Landesbeauftragte für den Datenschutz ist zuständige Aufsichtsbehörde im Sinne des Artikels 51 Absatz 1 der Verordnung (EU) 2016/679 im Geltungsbereich dieses Gesetzes, es sei denn, besondere Vorschriften regeln eine andere Zuständigkeit. Sie oder er ist zugleich Aufsichtsbehörde für den Datenschutz für nichtöffentliche Stellen nach § 40 des Bundesdatenschutzgesetzes.

(2) Die oder der Landesbeauftragte für den Datenschutz nimmt auch im Anwendungsbereich des § 2 Absatz 4 die Aufgaben gemäß Artikel 57 der Verordnung (EU) 2016/679 wahr und übt die Befugnisse gemäß Artikel 58 der Verordnung (EU) 2016/679 aus. Bei den Gemeinden, Gemeindeverbänden und den sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts sowie bei den in § 2 Absatz 2 genannten Stellen ist das vertretungsberechtigte Organ der Verantwortliche.

(3) Jede oder jeder kann sich an die Landesbeauftragte für den Datenschutz oder den Landesbeauftragten für den Datenschutz wenden, wenn sie oder er der Ansicht ist, bei der Verarbeitung ihrer oder seiner personenbezogenen Daten durch eine öffentliche Stelle in ihren oder seinen Rechten verletzt worden zu sein. Wer von seinem Recht nach Satz 1 Gebrauch gemacht hat, darf aus diesem Grund nicht benachteiligt oder gemäßregelt werden.

(4) Stellt die oder der Landesbeauftragte für den Datenschutz Verstöße gegen die Vorschriften dieses Gesetzes oder gegen andere Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung oder Nutzung personenbezogener Daten fest, teilt sie oder er dies bei den öffentlichen Stellen des Landes der zuständigen Rechts- oder Fachaufsichtsbehörde mit und gibt dieser vor Ausübung der Befugnisse des Artikels 58 Absatz 2 Buchstaben b bis g und j der Verordnung (EU) 2016/679 Gelegenheit zur Stellungnahme innerhalb einer angemessenen Frist. Bei den Gemeinden, Gemeindeverbän-

den und den sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts sowie den in § 2 Absatz 2 genannten Stellen tritt an die Stelle der Rechts- und Fachaufsichtsbehörde das vertretungsberechtigte Organ; zugleich unterrichtet die oder der Landesbeauftragte für den Datenschutz die zuständige Aufsichtsbehörde. Von der Einräumung der Gelegenheit zur Stellungnahme kann abgesehen werden, wenn eine sofortige Entscheidung wegen Gefahr im Verzug oder im öffentlichen Interesse notwendig erscheint oder ihr ein zwingendes öffentliches Interesse entgegensteht. Die Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die aufgrund der Mitteilung der oder des Landesbeauftragten für den Datenschutz getroffen worden oder beabsichtigt sind.

(5) § 29 Absatz 3 des Bundesdatenschutzgesetzes bleibt unberührt und gilt entsprechend für die Notarinnen und Notare des Landes. Im Übrigen erstreckt sich die Kontrolle der oder des Landesbeauftragten für den Datenschutz auch auf personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen. Erlangt die oder der Landesbeauftragte für den Datenschutz im Rahmen einer Untersuchung Kenntnis von Daten, die einer Geheimhaltungspflicht unterliegen, gilt die Geheimhaltungspflicht auch für die Landesbeauftragte für den Datenschutz oder den Landesbeauftragten für den Datenschutz.

## § 26

### *Pflicht zur Unterstützung*

(1) Die öffentlichen Stellen sind verpflichtet, die Landesbeauftragte für den Datenschutz oder den Landesbeauftragten für den Datenschutz und ihre oder seine Beauftragten bei der Erfüllung ihrer oder seiner Aufgaben zu unterstützen. Ihnen ist im Rahmen ihrer gesetzlichen Befugnisse insbesondere

1. Auskunft zu ihren Fragen sowie Einsicht in alle Unterlagen und Akten, insbesondere in die gespeicherten Daten und die Datenverarbeitungsprogramme zu gewähren, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen und
2. jederzeit Zutritt zu den Diensträumen einschließlich aller Datenverarbeitungsanlagen und -geräte zu gewähren.

(2) Die Ministerien beteiligen die Landesbeauftragte für den Datenschutz oder den Landesbeauftragten für den Datenschutz rechtzeitig bei der Ausarbeitung von Rechts- und Verwaltungsvorschriften, welche die Verarbeitung personenbezogener Daten betreffen.

## § 27

*Rundfunkbeauftragte oder Rundfunkbeauftragter  
für den Datenschutz*

(1) Der Südwestrundfunk ernennt für die Dauer von sechs Jahren eine Rundfunkbeauftragte für den Datenschutz oder einen Rundfunkbeauftragten für den Datenschutz, die oder der für alle Tätigkeiten des Südwestrundfunks und seiner Beteiligungsunternehmen nach § 16 c Absatz 3 Satz 1 des Rundfunkstaatsvertrages an Stelle der oder des Landesbeauftragten für den Datenschutz zuständige Aufsichtsbehörde nach Artikel 51 Absatz 1 der Verordnung (EU) 2016/679 ist. Die Ernennung erfolgt durch den Rundfunkrat mit Zustimmung des Verwaltungsrats. Die zweimalige Wiederernennung ist zulässig.

(2) Die oder der Rundfunkbeauftragte für den Datenschutz muss über die für die Erfüllung der Aufgaben und Ausübung der Befugnisse erforderliche Qualifikation, nachgewiesen durch ein abgeschlossenes Hochschulstudium, sowie über Erfahrung und Sachkunde, insbesondere im Bereich des Schutzes personenbezogener Daten, verfügen.

(3) Die Dienststelle der oder des Rundfunkbeauftragten für den Datenschutz wird bei der Geschäftsstelle des Rundfunk- und Verwaltungsrats eingerichtet. Die oder der Rundfunkbeauftragte für den Datenschutz ist angemessen zu vergüten. Nähere Bestimmungen, insbesondere die Grundsätze der Vergütung, trifft der Rundfunkrat mit Zustimmung des Verwaltungsrats in einer Satzung. Ihr oder ihm ist die für die Erfüllung ihrer oder seiner Aufgaben und Befugnisse notwendige Personal-, Finanz- und Sachausstattung zur Verfügung zu stellen. Die hierfür vorgesehenen Mittel sind jährlich, öffentlich und gesondert im Haushaltsplan des Südwestrundfunks auszuweisen und der oder dem Rundfunkbeauftragten für den Datenschutz im Haushaltsvollzug zuzuweisen. Die oder der Rundfunkbeauftragte für den Datenschutz ist in der Wahl ihrer oder seiner Mitarbeiterinnen oder Mitarbeiter frei. Sie unterstehen allein ihrer oder seiner Leitung.

(4) Das Amt der oder des Rundfunkbeauftragten für den Datenschutz kann nicht neben anderen Aufgaben innerhalb des Südwestrundfunks und seiner Beteiligungs- und Hilfsunternehmen wahrgenommen werden. Sonstige Aufgaben müssen mit dem Amt der oder des Rundfunkbeauftragten für den Datenschutz vereinbar sein und dürfen ihre oder seine Unabhängigkeit nicht gefährden. Das Amt endet mit Ablauf der Amtszeit, mit Rücktritt vom Amt oder mit Erreichen des gesetzlichen oder tarifvertraglich geregelten Renteneintrittsalters. Die oder der Rundfunkbeauftragte für den Datenschutz kann ihres oder seines Amtes nur enthoben werden, wenn sie oder er eine schwere Verfehlung begangen hat oder die Voraussetzungen für die Wahrnehmung ihrer oder seiner

Aufgaben nicht mehr erfüllt. Dies geschieht durch Beschluss des Rundfunkrats auf Vorschlag des Verwaltungsrats; die oder der Rundfunkbeauftragte für den Datenschutz ist vor der Entscheidung zu hören.

(5) Die oder der Rundfunkbeauftragte für den Datenschutz ist in Ausübung ihres oder seines Amtes völlig unabhängig und nur dem Gesetz unterworfen. Sie oder er unterliegt keiner Dienst-, Rechts- und Fachaufsicht. Der Finanzkontrolle des Verwaltungsrats unterliegt sie oder er nur insoweit, als ihre oder seine Unabhängigkeit dadurch nicht beeinträchtigt wird. Die Mitglieder des Rundfunkrats und des Verwaltungsrats sind berechtigt, Anfragen an die Rundfunkbeauftragte für den Datenschutz oder den Rundfunkbeauftragten für den Datenschutz zu richten, soweit hierdurch ihre oder seine Unabhängigkeit nicht beeinträchtigt wird.

(6) Jeder kann sich an die Rundfunkbeauftrage für den Datenschutz oder den Rundfunkbeauftragten für den Datenschutz wenden, wenn sie oder er der Ansicht ist, bei der Verarbeitung ihrer oder seiner personenbezogenen Daten durch den Südwestrundfunk oder eines seiner Beteiligungsunternehmen nach Absatz 1 Satz 1 in seinen Rechten verletzt worden zu sein.

(7) Die oder der Rundfunkbeauftragte für den Datenschutz hat die Aufgaben und Befugnisse entsprechend Artikel 57 und Artikel 58 Absatz 1 bis 5 der Verordnung (EU) 2016/679. Gegen den Südwestrundfunk dürfen keine Geldbußen verhängt werden. § 25 Absatz 4 gilt entsprechend mit der Maßgabe, dass die Mitteilung an die Intendantin oder den Intendanten unter gleichzeitiger Unterrichtung des Verwaltungsrats zu richten ist. Dem Verwaltungsrat ist auch die Stellungnahme der Intendantin oder des Intendanten zuzuleiten. Von einer Beanstandung und Unterrichtung kann abgesehen werden, wenn es sich um unerhebliche Mängel handelt oder wenn ihre unverzügliche Behebung sichergestellt ist.

(8) Die oder der Rundfunkbeauftragte für den Datenschutz hat auch für die Dauer von zwei Jahren nach der Beendigung ihrer oder seiner Amtszeit von allen mit den Aufgaben ihres oder seines früheren Amtes nicht zu vereinbarenden Handlungen und entgeltlichen oder unentgeltlichen Tätigkeiten abzusehen.

(9) Die oder der Rundfunkbeauftragte für den Datenschutz ist während und nach Beendigung ihres oder seines Amtsverhältnisses verpflichtet, über die ihr oder ihm amtlich bekannt gewordenen Angelegenheiten und vertraulichen Informationen Verschwiegenheit zu bewahren. Bei der Zusammenarbeit mit anderen Aufsichtsbehörden ist, soweit die Datenverarbeitung zu journalistischen Zwecken betroffen ist, der Informantenschutz zu wahren.

(10) Die oder der Rundfunkbeauftragte für den Datenschutz erstattet den Organen des Südwestrundfunks jährlich einen Tätigkeitsbericht nach Artikel 59 der Verord-

nung (EU) 2016/679. Der Bericht wird den Landtagen und den Landesregierungen der unterzeichnenden Länder des Staatsvertrags über den Südwestrundfunk übermittelt. Der Bericht wird veröffentlicht.

## Abschnitt 6

### Sanktionen

#### § 28

##### *Ordnungswidrigkeiten*

*(Ergänzung zu Artikel 83 Absatz 7 der Verordnung  
[EU] 2016/679)*

Gegen öffentliche Stellen im Sinne des § 2 Absatz 1 und 2 dürfen keine Geldbußen verhängt werden, es sei denn, die öffentlichen Stellen nehmen als Unternehmen mit eigener Rechtspersönlichkeit am Wettbewerb teil.

#### § 29

##### *Strafvorschrift*

*(Ergänzung zu Artikel 84 der Verordnung  
[EU] 2016/679)*

(1) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer

1. unbefugt von diesem Gesetz oder der Verordnung (EU) 2016/679 geschützte personenbezogene Daten, die nicht allgemein zugänglich sind,
  - a) speichert, nutzt, verändert, übermittelt oder löscht,
  - b) zum Abruf mittels automatisierten Verfahrens bereithält oder
  - c) abrufen oder sich oder einem anderen aus Dateien verschafft oder
2. durch unrichtige Angaben personenbezogene Daten, die durch dieses Gesetz oder die Verordnung (EU) 2016/679 geschützt werden und nicht allgemein zugänglich sind, erschleicht

und hierbei gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.

(2) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind die betroffene Person, die öffentliche Stelle, der Auftragsverarbeiter, die oder der Landesbeauftragte für den Datenschutz, die oder der Rundfunkbeauftragte für den Datenschutz und die Aufsichtsbehörden.

## Abschnitt 7

## Übergangsbestimmungen

## § 30

*Polizeibehörden und Polizeivollzugsdienst, Justizbehörden, Landesamt für Verfassungsschutz und Vollzug des Landessicherheitsüberprüfungsgesetzes*

(1) Für die Verarbeitung personenbezogener Daten durch die Polizeibehörden und den Polizeivollzugsdienst gilt, soweit sie nicht die Verordnung (EU) 2016/679 anzuwenden haben, das Landesdatenschutzgesetz in der am (Tag vor Inkrafttreten einsetzen) geltenden Fassung weiter, bis die Regelungen des Landes Baden-Württemberg zur Umsetzung der Richtlinie (EU) 2016/680 für den Bereich der Polizei in Kraft treten.

(2) Für die Verarbeitung personenbezogener Daten zu den in Artikel 2 Absatz 2 Buchstabe d der Verordnung (EU) 2016/679 genannten Zwecken durch das Justizministerium und die Justizvollzugsbehörden sowie durch die ordentlichen Gerichte und die Staatsanwaltschaften des Landes, soweit sie zu diesen Zwecken in Verwaltungsangelegenheiten tätig werden, sowie für die Behörden des Landes, die personenbezogene Daten zur Verfolgung und Ahndung von Ordnungswidrigkeiten verarbeiten, gilt das Landesdatenschutzgesetz in der am (Tag vor Inkrafttreten einsetzen) geltenden Fassung weiter, bis das Gesetz des Landes Baden-Württemberg zur Anpassung des besonderen Datenschutzrechts an die Verordnung und zur Umsetzung der Richtlinie (EU) 2016/680 für den Geschäftsbereich des Justizministeriums sowie für die zur Ahndung von Ordnungswidrigkeiten zuständigen Behörden des Landes in Kraft tritt.

(3) Für die Verarbeitung personenbezogener Daten durch das Landesamt für Verfassungsschutz im Rahmen der Erfüllung seiner Aufgaben nach § 3 des Landesverfassungsschutzgesetzes und beim Vollzug des Landessicherheitsüberprüfungsgesetzes gilt das Landesdatenschutzgesetz in der am (Tag vor Inkrafttreten einsetzen) geltenden Fassung weiter, bis das Gesetz des Landes Baden-Württemberg zur Änderung des Landesverfassungsschutzgesetzes und anderer Gesetze in Kraft tritt.

## § 31

*Überleitungsvorschriften*

(1) Der zum Zeitpunkt des Inkrafttretens dieses Gesetzes im Amt befindliche Landesbeauftragte für den Datenschutz gilt ab dem Tag des Inkrafttretens dieses Gesetzes als in ein Amt nach § 23 Absatz 1 berufen. Mit der Berufung in dieses Amt endet sein Beamtenverhältnis auf Zeit. Seine Amtszeit endet am 31. Dezember 2022.

(2) Mit Inkrafttreten dieses Gesetzes sind die Angehörigen des öffentlichen Dienstes bei dem Landesbeauftragten für den Datenschutz vom Landtag zu dem Landesbeauftragten für den Datenschutz versetzt.

(3) Der Personalrat bei der Dienststelle des Landesbeauftragten für den Datenschutz besteht ab Inkrafttreten dieses Gesetzes bis zu seiner Neuwahl als Personalrat bei dem Landesbeauftragten für den Datenschutz fort.

## Artikel 2

### Änderung des Landesverwaltungsgesetzes

Das Landesverwaltungsgesetz vom 14. Oktober 2008 (GBl. S. 313, 314), das zuletzt durch Artikel 13 des Gesetzes vom 21. November 2017 (GBl. S. 597, 606) geändert worden ist, wird wie folgt geändert:

1. In § 7 werden die Wörter „und der Rechnungshof“ durch die Wörter „, der Rechnungshof und der Landesbeauftragte für den Datenschutz“ ersetzt.
2. § 8 wird wie folgt geändert:
  - a) Nach Absatz 1 wird folgender Absatz 2 eingefügt:

„(2) Die Aufgaben des Landesbeauftragten für den Datenschutz ergeben sich aus der 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. Mai 2016, S. 1, ber. ABl. L 314 vom 22. November 2016, S. 72) in der jeweils geltenden Fassung und sonstigen Gesetzen.“
  - b) Die bisherigen Absätze 2 und 3 werden Absätze 3 und 4.
  - c) Im neuen Absatz 3 Satz 1 werden die Wörter „obersten Landesbehörden“ durch die Wörter „Landesregierung, des Ministerpräsidenten, der Ministerien und des Rechnungshofs“ ersetzt.
  - d) Es wird folgender Absatz 5 angefügt:

„(5) Dem Landesbeauftragten für den Datenschutz obliegt im Rahmen seines Geschäftsbereichs die Aufgabe der obersten Dienstbehörde auf dem Gebiet des Beamten-, Besoldungs-, Versorgungs- und Tarifrechts, soweit nicht für bestimmte Angelegenheiten eine besondere Regelung getroffen worden ist.“
3. In § 20 Absatz 1 Satz 2 wird die Angabe „§ 8 Absatz 3 Satz 1 Nr. 2“ durch die Wörter „§ 8 Absatz 4 Satz 1 Nummer 2“ ersetzt.

4. § 28 Nummer 1 wird wie folgt gefasst:

„1. von der Landesregierung für die obersten Landesbehörden mit Ausnahme des Landesbeauftragten für den Datenschutz und für die Regierungspräsidien“.

#### Artikel 3

##### Änderung des Landesbesoldungsgesetzes Baden-Württemberg

In Besoldungsgruppe B 5 der Anlage 2 (Landesbesoldungsordnung B) des Landesbesoldungsgesetzes Baden-Württemberg vom 9. November 2010 (GBl. S. 793, 826), das zuletzt durch Artikel 3 des Gesetzes zur Änderung des ADV-Zusammenarbeitsgesetzes und anderer Vorschriften vom 6. März 2018 (GBl. S. 65, 72) geändert worden ist, wird die Amtsbezeichnung „Landesbeauftragter für den Datenschutz“ gestrichen.

#### Artikel 4

##### Änderung des Ernennungsgesetzes

In § 2 Satz 1 des Ernennungsgesetzes in der Fassung vom 29. Januar 1992 (GBl. S. 141), das zuletzt durch Artikel 7 des Gesetzes vom 21. November 2017 (GBl. S. 597, 605) geändert worden ist, werden nach dem Wort „Ministerien“ die Wörter „, dem Landesbeauftragten für den Datenschutz“ eingefügt.

#### Artikel 5

##### Änderung des Landesinformationsfreiheitsgesetzes

Das Landesinformationsfreiheitsgesetz vom 17. Dezember 2015 (GBl. S. 1201) wird wie folgt geändert:

1. § 3 Nummer 4 wird wie folgt gefasst:

„4. geschützte Person: betroffene Person im Sinne des Artikels 4 Nummer 1 der 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. Mai 2016, S. 1, ber. ABl. L 314 vom 22. November 2016, S. 72) in der jeweils geltenden Fassung oder juristische Person, über die amtliche Informationen vorliegen, mit Ausnahme der antragstellenden Person.“

2. In § 4 Absatz 1 Nummer 3 werden die Wörter „Finanz-, Regulierungs-, Sparkassen-, Versicherungs- oder Wettbewerbsaufsichtsbehörden“ durch das Wort „Aufsichtsbehörden“ ersetzt.

3. In § 4 Absatz 1 Nummer 10, § 7 Absatz 4 Satz 2 und Absatz 7 Satz 2, der Überschrift zu § 8, § 8 Absatz 1 Satz 2 und Absatz 2 Satz 1 und 2 wird das Wort „betroffenen“ jeweils durch das Wort „geschützten“ ersetzt.
4. § 5 wird wie folgt geändert:
  - a) In Absatz 1 werden die Wörter „§ 3 Absatz 1 LDSG ist zu gewähren, soweit und solange die Betroffenen entsprechend § 4 Absatz 2 bis 5 LDSG eingewilligt haben“ durch die Wörter „Artikels 4 Nummer 1 der Verordnung (EU) 2016/679 ist zu gewähren, soweit und solange die betroffene Person im Sinne des Artikels 4 Nummer 1 der Verordnung (EU) 2016/679 entsprechend Artikel 7 der Verordnung (EU) 2016/679 eingewilligt hat“ ersetzt.
  - b) Absatz 2 wird wie folgt gefasst:

„(2) Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten im Sinne des Artikels 4 Nummer 13 der Verordnung (EU) 2016/679, biometrische Daten im Sinne des Artikels 4 Nummer 14 der Verordnung (EU) 2016/679 zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten im Sinne des Artikels 4 Nummer 15 der Verordnung (EU) 2016/679 oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person dürfen nur übermittelt werden, wenn die betroffene Person im Sinne des Artikels 4 Nummer 1 der Verordnung (EU) 2016/679 ausdrücklich eingewilligt hat.“
  - c) In Absatz 3 werden die Angabe „§ 3 Absatz 1 LDSG“ durch die Wörter „Artikels 4 Nummer 1 der Verordnung (EU) 2016/679“ sowie das Wort „Betroffenen“ durch die Wörter „betroffenen Person im Sinne des Artikels 4 Nummer 1 der Verordnung (EU) 2016/679“ ersetzt.
  - d) In Absatz 4 Satz 1 werden das Wort „Betroffenen“ durch die Wörter „betroffene Person im Sinne des Artikels 4 Nummer 1 der Verordnung (EU) 2016/679“ sowie das Wort „haben“ durch das Wort „hat“ ersetzt.
5. In § 6 Satz 2, § 7 Absatz 1 Satz 3, § 8 Absatz 1 Satz 1 und 3 sowie § 12 Absatz 2 wird das Wort „betroffene“ jeweils durch das Wort „geschützte“ ersetzt.
6. In § 7 Absatz 1 Satz 4 sowie § 11 Absatz 1 Satz 2 Nummer 2 wird die Angabe „§ 3 Absatz 1 LDSG“ jeweils durch die Wörter „Artikels 4 Nummer 1 der Verordnung (EU) 2016/679“ ersetzt.

7. § 12 wird wie folgt geändert:

a) Absatz 3 wird wie folgt gefasst:

„(3) Die oder der Landesbeauftragte für die Informationsfreiheit kontrolliert bei den informationspflichtigen Stellen die Einhaltung der Vorschriften dieses Gesetzes.“

b) Es werden folgende Absätze 4 bis 9 angefügt:

„(4) Die informationspflichtigen Stellen sind verpflichtet, die Landesbeauftragte oder den Landesbeauftragten für die Informationsfreiheit und ihre oder seine Beauftragten bei der Erfüllung ihrer oder seiner Aufgaben zu unterstützen.

(5) Die oder der Landesbeauftragte für die Informationsfreiheit teilt der informationspflichtigen Stelle das Ergebnis einer Kontrolle mit.

(6) Stellt die oder der Landesbeauftragte für die Informationsfreiheit Verstöße gegen Vorschriften dieses Gesetzes oder aufgrund dieses Gesetzes erlassener Vorschriften fest, so beanstandet sie oder er dies

1. bei den informationspflichtigen Stellen des Landes im Sinne des § 2 Absatz 1 Nummer 1 gegenüber der zuständigen obersten Landesbehörde,

2. bei den sonstigen informationspflichtigen Stellen gegenüber dem vertretungsberechtigten Organ

und fordert zur Stellungnahme innerhalb einer von ihr oder ihm zu bestimmenden angemessenen Frist auf. In den Fällen des Satz 1 Nummer 2 unterrichtet sie oder er gleichzeitig die zuständige Aufsichtsbehörde. Die oder der Landesbeauftragte für die Informationsfreiheit kann von einer Beanstandung absehen oder auf eine Stellungnahme der betroffenen Stelle verzichten, insbesondere wenn es sich um unerhebliche oder inzwischen beseitigte Mängel handelt. Die in Satz 1 Nummer 2 genannten Stellen leiten der zuständigen Aufsichtsbehörde eine Abschrift ihrer Stellungnahme an die Landesbeauftragte oder den Landesbeauftragten für die Informationsfreiheit zu.

(7) Die oder der Landesbeauftragte für die Informationsfreiheit erstattet dem Landtag für jeweils zwei Kalenderjahre zusammen einen Tätigkeitsbericht. Dieser ist jeweils bis zum 15. Februar des Folgejahres vorzulegen. Der nächste Bericht ist bis zum 15. Februar 2020 vorzulegen.

(8) Die oder der Landesbeauftragte für die Informationsfreiheit hat auf Anforderung des Landtags Gutachten zu erstellen und besondere Berichte zu erstatten. Sie oder er hat ferner zu parlamentarischen Anfragen von Abgeordneten Stellung zu

nehmen, die die Informationsfreiheit in dem ihrer oder seiner Kontrolle unterliegenden Bereich betreffen. Sie oder er kann sich jederzeit an den Landtag wenden, damit dieser sie oder ihn bei der Wahrnehmung ihrer oder seiner Aufgaben unterstützt. Sie oder er unterrichtet den Ständigen Ausschuss des Landtags jährlich, aus besonderem Anlass auch unverzüglich, über aktuelle Entwicklungen und Angelegenheiten von grundsätzlicher oder wesentlicher Bedeutung im Bereich der Informationsfreiheit. Eine Unterrichtung erfolgt auch, wenn der Ständige Ausschuss des Landtags darum ersucht.

(9) Die oder der Landesbeauftragte für die Informationsfreiheit kann der Landesregierung und einzelnen Ministerien sowie anderen öffentlichen Stellen Empfehlungen zur Verbesserung der Informationsfreiheit geben. Sie oder er ist bei der Ausarbeitung von Rechts- und Verwaltungsvorschriften zu diesem Gesetz zu beteiligen.“

#### Artikel 6

##### Änderung der Gebührenverordnung Innenministerium

Die Gebührenverordnung Innenministerium vom 12. Juli 2011 (GBl. S. 404), die zuletzt durch Verordnung vom 29. April 2015 (GBl. S. 286) geändert worden ist, wird wie folgt geändert:

1. In der Überschrift werden die Wörter „und des Landesbeauftragten für den Datenschutz im nichtöffentlichen Bereich“ gestrichen.
2. Nummer 10 der Anlage (Gebührenverzeichnis) wird aufgehoben.

#### Artikel 7

##### Änderung der Verordnung der Landesregierung über Zuständigkeiten nach dem Gesetz über Ordnungswidrigkeiten

§ 4 Absatz 2 der Verordnung der Landesregierung über Zuständigkeiten nach dem Gesetz über Ordnungswidrigkeiten in der Fassung vom 2. Februar 1990 (GBl. S. 73, ber. S. 268), die zuletzt durch Artikel 2 der Verordnung vom 12. Dezember 2017 (GBl. S. 669) geändert worden ist, wird wie folgt geändert:

1. Die Nummer 4 wird aufgehoben.
2. Die bisherigen Nummern 5 bis 7 werden die Nummern 4 bis 6.

## Artikel 8

Änderung des Gesetzes zur Ausführung  
des Personalausweisgesetzes

In § 11 Absatz 2 des Gesetzes zur Ausführung des Personalausweisgesetzes vom 16. März 1987 (GBl. S. 61), das zuletzt durch Gesetz vom 19. Oktober 2010 (GBl. S. 748) geändert worden ist, werden die Wörter „die Aufsichtsbehörde für den Datenschutz im nichtöffentlichen Bereich im Rahmen ihrer Zuständigkeit nach dem Bundesdatenschutzgesetz“ durch die Wörter „die oder der Landesbeauftragte für den Datenschutz“ ersetzt.

## Artikel 9

## Änderung des Feuerwehrgesetzes

§ 35 des Feuerwehrgesetzes in der Fassung vom 2. März 2010 (GBl. S. 333), das durch Artikel 1 des Gesetzes vom 17. Dezember 2015 (GBl. S. 1184) geändert worden ist, wird wie folgt geändert:

1. Absatz 1 wird aufgehoben.
2. Die bisherigen Absätze 2 bis 7 werden die Absätze 1 bis 6.
3. Im neuen Absatz 2 Satz 1 wird die Angabe „Absatz 2“ durch die Angabe „Absatz 1“ ersetzt.
4. Im neuen Absatz 3 werden die Wörter „Absätze 2 und 3“ durch die Wörter „Absätze 1 und 2“ ersetzt.
5. Im neuen Absatz 5 Satz 1 wird die Angabe „Absatz 5“ durch die Angabe „Absatz 4“ ersetzt.
6. Im neuen Absatz 6 werden die Angabe „Absatz 5“ durch die Angabe „Absatz 4“ und die Angabe „Absatz 6“ durch die Angabe „Absatz 5“ ersetzt.

## Artikel 10

## Änderung des Rettungsdienstgesetzes

Das Rettungsdienstgesetz in der Fassung vom 8. Februar 2010 (GBl. S. 285), das zuletzt durch Artikel 1 des Gesetzes vom 17. Dezember 2015 (GBl. S. 1182) geändert worden ist, wird wie folgt geändert:

1. § 31 wird wie folgt geändert:
  - a) Absatz 2 Satz 2 wird aufgehoben.
  - b) Absatz 3 wird aufgehoben.

2. § 32 wird wie folgt geändert:

- a) In der Überschrift werden die Wörter „Erhebung, Veränderung, Speicherung, Nutzung und Übermittlung“ durch das Wort „Verarbeitung“ ersetzt.
- b) In Absatz 1 werden die Wörter „erhoben, verändert, gespeichert und genutzt“ durch das Wort „verarbeitet“ ersetzt.
- c) In Absatz 2 wird das Wort „auch“ gestrichen.

#### Artikel 11

##### Änderung des Flüchtlingsaufnahmegesetzes

§ 16 des Flüchtlingsaufnahmegesetzes vom 19. Dezember 2013 (GBl. S. 493), das zuletzt durch Artikel 14 der Verordnung vom 23. Februar 2017 (GBl. S. 99, 101) geändert worden ist, wird wie folgt geändert:

1. In Absatz 1 werden die Wörter „§ 33 Absatz 1 des Landesdatenschutzgesetzes“ durch die Wörter „Artikel 9 Absatz 1 der 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. Mai 2016, S. 1, ber. ABl. L 314 vom 22. November 2016, S. 72) in der jeweils geltenden Fassung“ ersetzt und nach dem Wort „ist“ die Wörter „; die Verarbeitung von genetischen Daten ist ausgeschlossen“ eingefügt.
2. In Absatz 2 Satz 4 wird das Wort „Betroffenen“ durch die Wörter „jeweiligen betroffenen Person“ ersetzt.
3. Absatz 3 wird aufgehoben.

#### Artikel 12

##### Änderung des baden-württembergischen Ausführungsgesetzes zum Bundesmeldegesetz

Das baden-württembergische Ausführungsgesetz zum Bundesmeldegesetz vom 12. Mai 2015 (GBl. S. 320) wird wie folgt geändert:

1. § 2 wird wie folgt geändert:

- a) In der Überschrift wird das Wort „Speicherung“ durch das Wort „Verarbeitung“ ersetzt.
- b) In Absatz 1 werden die Wörter „erheben, verarbeiten und nutzen“ durch das Wort „verarbeiten“ ersetzt.
- c) In Absatz 2 und Absatz 3 Satz 1 wird jeweils das Wort „nutzen“ durch das Wort „verwenden“ ersetzt.
- d) In Absatz 3 Satz 2 wird das Wort „Nutzung“ durch das Wort „Verwendung“ ersetzt.

2. § 5 wird wie folgt geändert:

- a) In Absatz 1 Satz 2 werden die Wörter „und nutzt“ gestrichen.
- b) In Absatz 3 Satz 1 und 2 wird jeweils das Wort „Ergänzung“ durch das Wort „Vervollständigung“ ersetzt.
- c) In Absatz 5 Satz 1 werden die Wörter „und nutzen“ gestrichen.

#### Artikel 13

##### Änderung der Meldeverordnung

Die Meldeverordnung vom 28. September 2015 (GBl. S. 853), die durch Artikel 10 des Gesetzes vom 6. März 2018 (GBl. S. 65, 73) geändert worden ist, wird wie folgt geändert:

1. In § 4 Absatz 3 Satz 1 wird das Wort „ergänzt“ durch das Wort „vervollständigt“ ersetzt.
2. In § 19 Absatz 3 Satz 1 und 2 wird jeweils das Wort „Ergänzung“ durch das Wort „Vervollständigung“ ersetzt.
3. In § 20 Absatz 2 Satz 2 werden die Wörter „§ 9 des Landesdatenschutzgesetzes in der Fassung vom 18. September 2000 (GBl. S. 649)“ durch die Wörter „entsprechend der Verordnung (EU) 2016/679 sowie § 3 des Landesdatenschutzgesetzes“ ersetzt.

#### Artikel 14

##### Änderung des Landesglücksspielgesetzes

Das Landesglücksspielgesetz vom 20. November 2012 (GBl. S. 604), das zuletzt durch Artikel 12 der Verordnung vom 23. Februar 2017 (GBl. S. 99, 100) geändert worden ist, wird wie folgt geändert:

1. § 5 wird wie folgt geändert:
  - a) In Absatz 4 Satz 1 wird das Wort „nutzen“ durch das Wort „verwenden“ ersetzt.
  - b) In Absatz 5 Satz 1 wird das Wort „Datennutzung“ durch die Wörter „Verwendung der Daten“ ersetzt.
2. In § 30 Absatz 1 Satz 2 wird das Wort „genutzt“ durch das Wort „verwendet“ ersetzt.
3. § 32 wird wie folgt geändert:
  - a) In Absatz 4 Satz 1 wird das Wort „Nutzung“ durch das Wort „Verwendung“ ersetzt.
  - b) Absatz 5 wird aufgehoben. Die bisherigen Absätze 6 bis 8 werden die neuen Absätze 5 bis 7.
  - c) Der neue Absatz 6 wird wie folgt gefasst:

„(6) Die Spielbank ist verpflichtet, einen betrieblichen Datenschutzbeauftragten zu bestellen. Dieser hat das Konzept für die Videoüberwachung vor dessen Umsetzung zu überprüfen, anschließend ist es durch die Spielbank als verantwortliche Stelle freizugeben. Der betriebliche Datenschutzbeauftragte prüft insbesondere, ob bei der vorgesehenen Videoüberwachung die nötigen technischen und organisatorischen Maßnahmen getroffen worden sind und ob den schutzwürdigen Interessen der Betroffenen Rechnung getragen wird. Ihm sind die Namen der zugriffsberechtigten Personen mitzuteilen.“

4. In § 45 Absatz 3 Satz 2 wird das Wort „genutzt“ durch das Wort „verwendet“ ersetzt.

#### Artikel 15

##### Änderung des Abschiebungshaftvollzugsgesetzes Baden-Württemberg

Das Abschiebungshaftvollzugsgesetz Baden-Württemberg vom 17. Dezember 2015 (GBl. S. 1187) wird wie folgt geändert:

1. § 1 wird wie folgt geändert:

- a) Der bisherige Wortlaut wird Absatz 1.
- b) Es wird folgender Absatz 2 angefügt:

„(2) Dieses Gesetz findet auf den Vollzug des Ausreisegewahrsams im Sinne des § 62 b des Aufenthaltsgesetzes entsprechende Anwendung.“

2. § 2 wird wie folgt geändert:

Nach dem Wort „Einrichtung“ werden die Wörter „oder die Abwehr einer von den Untergebrachten ausgehenden erheblichen Gefahr für Leib oder Leben Dritter oder bedeutende Rechtsgüter der inneren Sicherheit“ eingefügt.

3. § 3 Absatz 4 Satz 2 wird wie folgt gefasst:

„Die diesbezüglichen Daten im Sinne des Artikels 9 Absatz 1 der 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. Mai 2016, S. 1, ber. ABl. L 314 vom 22. November 2016, S. 72) in der jeweils geltenden Fassung dürfen zum Zwecke des Schutzes der betroffenen Person vor religiös oder rassistisch motivierten Übergriffen und zum Zwecke der Ermöglichung der Religionsausübung verarbeitet werden, wenn die betroffene Person in die Verarbeitung ausdrücklich eingewilligt hat.“

## 4. § 10 wird wie folgt geändert:

## a) Nach Absatz 3 wird folgender Absatz 4 eingefügt:

„(4) Eine Videoüberwachung ist während einer Unterbringung nach Absatz 3 sowie in Räumen, die nur einer vorübergehenden Unterbringung, insbesondere aus medizinischen Gründen, dienen, wie Krisenräume, Beobachtungsräume und medizinische Bettenstation, zulässig, wenn und soweit sie im Einzelfall zur Abwehr gegenwärtiger Gefahren für das Leben oder gegenwärtiger erheblicher Gefahren für die Gesundheit von Untergebrachten oder Dritten erforderlich ist. Die Anfertigung von Aufzeichnungen hiervon ist zulässig, wenn dies zum Zweck der Aufrechterhaltung der Sicherheit und Ordnung der Einrichtung oder zur Verhinderung oder Verfolgung von Straftaten oder Ordnungswidrigkeiten, durch welche die Sicherheit oder Ordnung der Einrichtung gefährdet wird, erforderlich ist. Die Persönlichkeitsrechte, die Würde und das Schamgefühl der Untergebrachten sind zu achten. Untergebrachte sind auf die Videoüberwachung und die Anfertigung von Aufzeichnungen hinzuweisen. Die nach Satz 2 gespeicherten Daten sind unverzüglich, spätestens jedoch drei Werktage nach der Erhebung zu löschen, sofern nicht ihre Speicherung für andere Zwecke als diejenigen, für die sie erhoben wurden, zulässig und weiterhin erforderlich ist. Die nach Satz 2 erhobenen Daten sind unverzüglich zu löschen, soweit schutzwürdige Belange der betroffenen Personen einer weiteren Speicherung entgegenstehen.“

## b) Die bisherigen Absätze 4 bis 6 werden Absätze 5 bis 7.

## 5. Nach § 10 wird folgender § 10 a eingefügt:

## „§ 10 a

*Videoüberwachung*

(1) Das Einrichtungsgelände sowie das Innere des Einrichtungsgebäudes können offen mittels Videotechnik überwacht werden. Die Anfertigung von Aufzeichnungen hiervon sowie die Beobachtung der unmittelbaren Einrichtungsumgebung sind zulässig, sofern dies zum Zweck der Aufrechterhaltung der Sicherheit oder Ordnung der Einrichtung oder zur Verhinderung oder Verfolgung von Straftaten oder Ordnungswidrigkeiten, durch welche die Sicherheit oder Ordnung der Einrichtung gefährdet wird, erforderlich ist. Die Videoüberwachung von Unterbringungsräumen sowie von Räumen, die für Kontakte mit Berufsheimnisträgern, Beiständen und Mitarbeitern von einschlägig tätigen Hilfs- und Unterstützungsorganisationen genutzt werden, ist ausgeschlossen. § 10 Absatz 4 bleibt unberührt.

(2) Auf die Videoüberwachung und die Anfertigung von Aufzeichnungen ist durch geeignete Maßnahmen hinzuweisen. Sie dürfen auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden.

(3) Die nach Absatz 1 gespeicherten Daten sind unverzüglich, spätestens jedoch eine Woche nach der Erhebung zu löschen, sofern nicht ihre Speicherung für andere Zwecke als diejenigen, für die sie erhoben wurden, zulässig und weiterhin erforderlich ist. Sie sind unverzüglich zu löschen, soweit schutzwürdige Belange der betroffenen Personen einer weiteren Speicherung entgegenstehen.“

#### Artikel 16

##### Änderung der Abschiebungshaftvollzugsverordnung

Die Abschiebungshaftvollzugsverordnung vom 7. März 2016 (GBl. S. 219) wird wie folgt geändert:

1. § 1 Absatz 2 Satz 2 wird wie folgt gefasst:

„Die für die Beantragung von Abschiebungshaft zuständige Behörde übermittelt der Einrichtung vor der Aufnahme die ihr vorliegenden vollzugsrelevanten Erkenntnisse.“

2. § 10 wird wie folgt geändert:

a) Absatz 4 Satz 2 bis 4 wird wie folgt gefasst:

„Personenbezogene Daten der Untergebrachten sind vor der Übermittlung zu anonymisieren. Personenbezogene Daten der Untergebrachten dürfen vom Beirat an die Einrichtungsleitung und das Innenministerium nur übermittelt werden, wenn dies zu deren Aufgabenerfüllung oder zur eigenen Aufgabenerfüllung des Beirats erforderlich ist oder die betroffenen Personen im Einzelfall nach Artikel 6 Absatz 1 Buchstabe a der 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. Mai 2016, S. 1, ber. ABl. L 314 vom 22. November 2016, S. 72) in der jeweils geltenden Fassung in die Übermittlung eingewilligt haben. Sofern Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 übermittelt werden, muss sich die Einwilligung der betroffenen Personen auch ausdrücklich darauf beziehen.“

b) Absatz 6 Satz 3 und 4 wird wie folgt gefasst:

„Personenbezogene Daten der Untergebrachten dürfen von der Einrichtungsleitung an den Beirat nur übermittelt werden, wenn dies zur eigenen Aufga-

benerfüllung oder zur Aufgabenerfüllung des Beirats erforderlich ist oder die betroffenen Personen im Einzelfall nach Artikel 6 Absatz 1 Buchstabe a der Verordnung (EU) 2016/679 in die Übermittlung eingewilligt haben. Sofern Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 übermittelt werden, muss sich die Einwilligung der betroffenen Personen auch ausdrücklich darauf beziehen.“

#### Artikel 17

##### Änderung des Landesbeamtengesetzes

Das Landesbeamtengesetz vom 9. November 2010 (GBl. S. 793, 794), das zuletzt durch Artikel 5 des Gesetzes vom 6. März 2018 (GBl. S. 65, 73) geändert worden ist, wird wie folgt geändert:

1. In § 53 Absatz 3 Satz 2 wird die Angabe „§ 84 Absatz 3 Satz 2“ durch die Wörter „§ 83 Absatz 3 Satz 2“ ersetzt.
2. § 83 wird wie folgt gefasst:

„§ 83

##### *Verarbeitung*

(1) Der Dienstherr darf Personalaktendaten verarbeiten, soweit dies zur Begründung, Durchführung, Beendigung oder Abwicklung des Dienstverhältnisses oder zur Durchführung innerdienstlich planerischer, organisatorischer, personeller, sozialer oder haushalts- und kostenrechnerischer Maßnahmen, insbesondere auch zu Zwecken der Personalplanung oder des Personaleinsatzes erforderlich ist oder eine Rechtsvorschrift oder Dienstvereinbarung dies erlaubt. Die Vorschriften des Landesdatenschutzgesetzes (LDSG) zur Verarbeitung besonderer Kategorien personenbezogener Daten sowie zur Sicherstellung des Datenschutzes (§ 3 LDSG) finden entsprechende Anwendung.

(2) Personalaktendaten über Beihilfe dürfen für andere als für Beihilfezwecke nur verarbeitet werden, wenn die Voraussetzungen nach § 85 Absatz 2 oder 3 vorliegen. Satz 1 gilt entsprechend für die Verarbeitung von Personalaktendaten über Heilfürsorge und Heilverfahren.

(3) Über medizinische oder psychologische Untersuchungen und Tests dürfen im Rahmen der Personalverwaltung nur die Ergebnisse verarbeitet werden, soweit sie die Eignung betreffen und ihre Speicherung, Veränderung oder Verwendung dem Schutz der Beamtin oder des Beamten dient. Sonstige Untersuchungsdaten dürfen nur verarbeitet werden, soweit deren Kenntnis zur Entscheidung für die konkrete Maßnahme, zu deren Zweck die Untersuchung durchgeführt worden ist, erforderlich ist.

(4) Absatz 1 gilt für die nach §§ 77 und 96 Landesbeamtenversorgungsgesetz Baden-Württemberg zuständigen Stellen entsprechend.“

3. § 84 wird wie folgt gefasst:

„§ 84

*Vollständig automatisierte Entscheidungen*

Eine beamtenrechtliche Entscheidung darf nur dann auf einer ausschließlich automatisierten Verarbeitung von personenbezogenen Daten beruhen, wenn weder ein Ermessen noch ein Beurteilungsspielraum besteht.“

4. § 85 wird wie folgt geändert:

a) Absatz 1 wird wie folgt geändert:

aa) In Nummer 9 wird das Wort „nutzen“ durch das Wort „verwenden“ ersetzt.

bb) In Nummer 10 werden die Wörter „von der“ durch die Wörter „über die“ und das Wort „unterrichten“ durch das Wort „informieren“ ersetzt.

b) Absatz 3 Satz 1 wird wie folgt gefasst:

„Personalaktendaten über Beihilfe dürfen auch ohne Einwilligung der betroffenen Personen an eine andere Behörde oder Stelle übermittelt werden, wenn sie für die Festsetzung und Berechnung der Besoldung oder Versorgung oder für die Prüfung der Kindergeldberechtigung erforderlich sind.“

5. Nach § 85 wird folgender § 85 a eingefügt:

„§ 85 a

*Verarbeitung von Personalaktendaten im Auftrag*

(1) Die Verarbeitung von Personalaktendaten im Auftrag des Verantwortlichen gemäß Artikel 28 der 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. Mai 2016, S. 1, ber. ABl. L 314 vom 22. November 2016, S. 72) ist zulässig,

1. soweit sie erforderlich ist

a) für die überwiegend automatisierte Erledigung von Aufgaben oder

b) zur Verrichtung technischer Hilfstätigkeiten durch überwiegend automatisierte Einrichtungen, und

2. wenn der Verantwortliche die Einhaltung der beamten- und datenschutzrechtlichen Vorschriften durch den Auftragsverarbeiter regelmäßig kontrolliert.

(2) Die Auftragserteilung einschließlich der Unterauftragserteilung bedarf der vorherigen Zustimmung der obersten Dienstbehörde. Zu diesem Zweck hat der Verantwortliche der obersten Dienstbehörde rechtzeitig vor der Auftragserteilung mitzuteilen:

1. den Auftragsverarbeiter, die von diesem getroffenen technischen und organisatorischen Maßnahmen und die ergänzenden Festlegungen nach Artikel 28 der Verordnung (EU) 2016/679,
2. die Aufgabe, zu deren Erfüllung der Auftragsverarbeiter die Daten verarbeiten soll,
3. die Art der Daten, die für den Verantwortlichen verarbeitet werden sollen, und den Kreis der Beschäftigten, auf den sich diese Daten beziehen, sowie
4. die beabsichtigte Erteilung von Unteraufträgen durch den Auftragsverarbeiter.

(3) Eine nichtöffentliche Stelle darf nur beauftragt werden, wenn

1. beim Verantwortlichen sonst Störungen im Geschäftsablauf auftreten können oder der Auftragsverarbeiter die übertragenen Aufgaben erheblich wirtschaftlicher erledigen kann und
2. die beim Auftragsverarbeiter mit der Datenverarbeitung beauftragten Beschäftigten besonders auf den Schutz der Personalaktendaten verpflichtet sind.“

6. § 86 wird wie folgt geändert:

- a) Absatz 1 wird aufgehoben.
- b) Die bisherigen Absätze 2 bis 8 werden die Absätze 1 bis 7.
- c) Im neuen Absatz 1 Satz 3 werden die Wörter „Absatzes 2 Nr. 2 bis 4“ durch die Wörter „Nummern 2 bis 4“ ersetzt.
- d) Im neuen Absatz 3 Satz 3 werden die Wörter „Absatz 3 Satz 2 bis 4“ durch die Wörter „Absatz 2 Satz 2 bis 4“ ersetzt.

7. § 87 wird wie folgt gefasst:

„§ 87

*Auskunft, Anhörung*

(1) Beamtinnen und Beamte können während und nach Beendigung des Beamtenverhältnisses Auskunft über alle über sie gespeicherten Personalaktendaten auch in Form der Einsichtnahme verlangen.

(2) Bevollmächtigten der Beamtin oder des Beamten ist Auskunft zu erteilen, soweit dienstliche Gründe nicht entgegenstehen. Dies gilt auch für Hinterbliebene und deren Bevollmächtigte, wenn ein berechtigtes Interesse glaubhaft gemacht wird. Absatz 1 gilt entsprechend.

(3) Wird die Auskunft in Form der Einsichtnahme verlangt, bestimmt die personalverwaltende Stelle, wo die Einsicht gewährt wird. Auf Verlangen werden Abschriften, Kopien oder Ausdrücke, auch auszugsweise, gefertigt und überlassen.

(4) Die Einsichtnahme ist unzulässig, wenn die Daten der betroffenen Beamtin oder des betroffenen Beamten mit Daten Dritter oder geheimhaltungsbedürftigen nicht personenbezogenen Daten derart verbunden sind, dass ihre Trennung nicht oder nur mit unverhältnismäßig großem Aufwand möglich ist. In diesem Fall ist der Beamtin oder dem Beamten Auskunft zu erteilen.

(5) Ist beabsichtigt, Beschwerden, Behauptungen und Bewertungen, die für die Beamtinnen und Beamten ungünstig sind oder ihnen nachteilig werden können, als Personalaktendaten zu speichern, sind sie hierüber zu informieren und es ist ihnen Gelegenheit zur Stellungnahme, insbesondere auch hinsichtlich einer notwendigen Berichtigung oder Vervollständigung, zu geben. Soweit eine Speicherung erfolgt, ist hierzu die Äußerung der Beamtin oder des Beamten ebenfalls zu den Personalaktendaten zu speichern.“

8. Die Inhaltsübersicht ist entsprechend anzupassen.

#### Artikel 18

##### Änderung des Landesdisziplinargesetzes

Das Landesdisziplinargesetz vom 14. Oktober 2008 (GBl. S. 343, 344), das zuletzt durch Artikel 4 des Gesetzes vom 1. Dezember 2015 (GBl. S. 1035, 1038) geändert worden ist, wird wie folgt geändert:

1. § 19 wird wie folgt geändert:

- a) In Absatz 1 werden die Wörter „die Vorlage“ gestrichen sowie das Wort „Personalakten“ durch das Wort „Personalaktendaten“ und das Wort „Betroffener“ durch die Wörter „betroffener Personen“ ersetzt.
- b) In Absatz 2 wird das Wort „Betroffener“ durch die Wörter „betroffener Personen“ ersetzt.

2. § 42 Absatz 4 Satz 1 bis 3 wird wie folgt gefasst:

„Personalaktendaten über den Disziplinarvorgang sind aufgrund des Verwertungsverbots mit Zustimmung des Beamten zu löschen. Auf Antrag des Beamten un-

terbleibt die Löschung oder erfolgt eine gesonderte Aufbewahrung. Der Antrag ist innerhalb eines Monats zu stellen, nachdem dem Beamten die Lösungsabsicht mitgeteilt und er auf sein Antragsrecht und die Antragsfrist hingewiesen worden ist.“

#### Artikel 19

##### Änderung des Landespersonalvertretungsgesetzes

Das Landespersonalvertretungsgesetz in der Fassung vom 12. März 2015 (GBl. S. 222), das zuletzt durch Artikel 2 des Gesetzes vom 6. Oktober 2015 (GBl. S. 842, 851) geändert worden ist, wird wie folgt geändert:

1. In § 32 Absatz 3 Satz 4 werden die Wörter „schriftlicher Zustimmung“ durch das Wort „Einwilligung“ ersetzt.
2. In § 71 Absatz 1 Satz 3 wird das Wort „Zustimmung“ durch das Wort „Einwilligung“ ersetzt.
3. § 76 wird wie folgt geändert:
  - a) Absatz 2 Satz 1 wird wie folgt gefasst:

„Der Personalrat bestimmt, soweit in § 75 Absatz 5 und 6 nichts anderes bestimmt ist, nur mit

    1. in den Personalangelegenheiten nach § 75 Absatz 1 und 2 der
      - a) in § 9 Absatz 2 Satz 1 Nummern 2 und 3 bezeichneten Beschäftigten,
      - b) der Beamten auf Zeit,
      - c) der Beschäftigten mit überwiegend wissenschaftlicher oder künstlerischer Tätigkeit,
    2. in den Angelegenheiten des § 74 Absatz 1 Nummern 1 und 4,wenn die betroffenen Beschäftigten es beantragen.“
  - b) In Absatz 3 Halbsatz 2 werden die Wörter „Antrags- oder Widerspruchsrecht“ durch das Wort „Antragsrecht“ ersetzt.

#### Artikel 20

##### Inkrafttreten, Außerkrafttreten

Dieses Gesetz tritt am Tag nach der Verkündung in Kraft. Gleichzeitig tritt das Landesdatenschutzgesetz in der Fassung vom 18. September 2000 (GBl. S. 649), das zuletzt durch Artikel 2 des Gesetzes vom 17. Dezember 2015 (GBl. S. 1191, 1198) geändert worden ist, außer Kraft.

## Begründung

### A. Allgemeiner Teil

#### I. Zielsetzung

Das Gesetz zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679 ist notwendig, um das bisher geltende Gesetz zum Schutz personenbezogener Daten (Landesdatenschutzgesetz – LDSG) in der Fassung vom 18. September 2000 (GBl. S. 648), zuletzt geändert durch Artikel 2 des Gesetzes vom 17. Dezember 2015 (GBl. S. 1191, 1198) (LDSG a. F.) sowie sonstige bereichsspezifische Datenschutzregelungen an die Regelungen der 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. Mai 2016 S. 1, ber. ABl. L 314 vom 22. November 2016, S. 72) anzupassen. Da die Verordnung (EU) 2016/679 unmittelbar für alle öffentlichen Stellen gilt, verbleibt dem Landesgesetzgeber nur insofern Regelungsspielraum für landesrechtliche Regelungen, als die Verordnung (EU) 2016/679 Öffnungsklauseln enthält. Eine Wiederholung der Regelungen der Verordnung (EU) 2016/679 verbietet außer in eng begrenzten Ausnahmefällen das europarechtliche Wiederholungsverbot (vgl. Erwägungsgrund 8 der Verordnung [EU] 2016/679).

Das bisherige Landesdatenschutzgesetz wird daher aufgehoben. Das Gesetz zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679 enthält im neu gefassten Landesdatenschutzgesetz (LDSG) ergänzende Regelungen zur Verordnung (EU) 2016/679, sofern diese im Rahmen der Öffnungsklauseln zulässig und nach Auffassung des Landesgesetzgebers geeignet, erforderlich und verhältnismäßig sind. Die europäischen Standards werden nur soweit wie nötig eingeschränkt. Geregelt werden im Wesentlichen folgende Bereiche:

- Zulässigkeit der Datenverarbeitung, insbesondere zu anderen Zwecken
- Einschränkungen der Betroffenenrechte
- Besondere Verarbeitungssituationen, soweit sie nicht bereichsspezifisch geregelt sind; zu diesen zählt auch die Videoüberwachung durch öffentliche Stellen und der Beschäftigtendatenschutz
- Sanktionen bei Verstößen.

Hierbei wird das Recht auf informationelle Selbstbestimmung, wie von der Verordnung (EU) 2016/679 und verfassungsrechtlich gefordert, in Einklang gebracht mit den sonstigen grundrechtlich geschützten Freiheiten (z. B. Rundfunkfreiheit, Berufsfreiheit, Freiheit von Forschung und Lehre) einerseits und den Anforderungen der öffentlichen Sicherheit und der Funktionsfähigkeit der Verwaltung andererseits.

Am 25. Mai 2018 tritt das Datenschutz-Anpassungs- und -Umsetzungsgesetz EU des Bundes (BGBl. S. 2097) in Kraft, welches das an die Verordnung (EU) 2016/679 angepasste Bundesdatenschutzgesetz (im Folgenden: Bundesdatenschutzgesetz) enthält. Als vom Landesgesetzgeber zu beachtende Vorgabe bezüglich der Aufsichtsbehörde des Landes regelt es, dass diese wie bisher neben ihrer Aufsichtstätigkeit über die öffentlichen Stellen des Landes bei den privaten Stellen die Einhaltung des Datenschutzes überwacht.

Aus der Neuregelung der Organisation der oder des Landesbeauftragten für den Datenschutz ergibt sich in weiteren Gesetzen Änderungsbedarf, der in den Artikeln 2 bis 4 sowie Artikel 6 bis 8 geregelt ist.

Im Landesinformationsfreiheitsgesetz (Artikel 5) ist das Informationsrecht in Einklang zu bringen mit dem Schutz personenbezogener Daten nach der Verordnung (EU) 2016/679.

Im bereichsspezifischen Datenschutzrecht (Artikel 9 bis Artikel 16) sind Anpassungen an die Verordnung (EU) 2016/679 vorzunehmen, und zwar mit Inkrafttreten des Gesetzes nicht mehr zutreffende Verweisungen auf das bisher geltende Landesdatenschutzgesetz zu streichen sowie Begriffsbestimmungen anzupassen. Im Bereich der dienstrechtlichen Vorschriften (Artikel 17 bis Artikel 19) werden neben begrifflichen auch inhaltliche Anpassungen vorgenommen, um das Ineinandergreifen von der Verordnung (EU) 2016/679 und dem nationalen Recht zu sichern.

In den Artikeln 15 und 16 werden zusätzlich materielle Änderungen des Abschiebungshaftvollzugsgesetzes und der Abschiebungshaftvollzugsverordnung eingefügt.

Artikel 20 regelt schließlich das Inkrafttreten und Außerkrafttreten.

## II. Inhalt

### 1. Landesdatenschutzgesetz

- a) Wie bisher wird ausschließlich die Verarbeitung personenbezogener Daten durch öffentliche Stellen geregelt. Die öffentliche Stelle ist „Verantwortlicher“ nach Artikel 4 Nummer 7 der Verordnung (EU) 2016/679, soweit nichts anderes bestimmt ist. Die Begriffsbestimmungen sind im Übrigen aus Artikel 4 der Verordnung (EU) 2016/679 zu entnehmen und weichen teilweise von der bisherigen Terminologie ab.
- b) Die Betroffenenrechte ergeben sich direkt aus der Verordnung (EU) 2016/679. Artikel 23 der Verordnung (EU) 2016/679 sieht vor, dass sämtliche Betroffenenrechte durch nationale Gesetze beschränkt werden können, sofern dies zur Wahrung bestimmter öffentlicher Interessen, die in Artikel 23 Absatz 1 Buchstaben a bis j der Verordnung (EU) 2016/679 aufgezählt sind, erforderlich ist. Von dieser Ermächtigung wird Gebrauch gemacht. Zugleich werden der Verhältnismäßigkeitsgrundsatz und der Wesensgehalt der Grundrechte beachtet sowie Schutzmaßnahmen nach Artikel 23 Absatz 2 der Verordnung (EU) 2016/679 angeordnet.
- c) Für die wissenschaftliche Forschung, die in der Verordnung (EU) 2016/679 an mehreren Stellen als privilegiert behandelt wird, soll im Interesse der Wissenschafts- und Forschungsfreiheit auch die Verarbeitung besonderer Kategorien personenbezogener Daten zugelassen werden. Einschränkungen sind soweit vorgesehen, wie es die informationelle Selbstbestimmung gebietet.
- d) Der Beschäftigtendatenschutz wird im Verhältnis zu § 36 LDSG a.F. gestärkt. Der Landesgesetzgeber ist hierzu in Bezug auf die Landesbeschäftigten befugt. Das Beschäftigtenverhältnis ist in besonderer Weise vor Beeinträchtigungen des Rechts auf informationelle Selbstbestimmung zu schützen.

In der Abwägung der widerstreitenden Grundrechtspositionen der Arbeitgeber an der Datenverarbeitung zur Kontrolle der Beschäftigten und des Persönlichkeitsrechts der Beschäftigten ist zugunsten Letzterer dem Schutz vor dauerhafter Überwachung der Vorzug zu geben.

Auch an die Verwendung biometrischer Daten als besonders sensible Daten im Beschäftigungsverhältnis werden enge Voraussetzungen geknüpft, um einen Missbrauch zu verhindern. Eine Einwilligung des Beschäftigten alleine oder eine Dienst- oder Betriebsvereinbarung reicht hierfür nicht aus. Hinzu kommen muss ein dringendes dienstliches Bedürfnis.

Für die Zuverlässigkeitsüberprüfung von Bewerberinnen und Bewerbern für öffentliche Leistungen sowie Besucherinnen und Besuchern wird eine eigene gesetzliche Grundlage geschaffen, da hierfür ein öffentliches Interesse besteht. Die Prüfung wird auf die erforderlichen personenbezogenen Daten beschränkt. Auf eine Einwilligung kann wegen der Eingriffstiefe dennoch nicht verzichtet werden.

- e) Auch unter Geltung der Verordnung (EU) 2016/679 wird die Videoüberwachung zugelassen. Um der Videoüberwachung in verstärktem Maße präventive Wirkung zukommen zu lassen, wird entgegen dem bisherigen Landesdatenschutzgesetz bereits das Bestehen einer abstrakten Gefahr für die Zulässigkeit der Videoüberwachung als ausreichend erachtet.
- f) Artikel 85 der Verordnung (EU) 2016/679 verpflichtet den Gesetzgeber, im nationalen Recht medienpezifische Bestimmungen zu treffen, um einen Ausgleich zwischen dem Persönlichkeitsrecht einerseits und der Rundfunk- und Pressefreiheit andererseits zu gewährleisten. Dazu sind Bestimmungen zum Medienprivileg nötig sowie aufsichtsrechtliche Vorschriften über die Medien und damit auch zur datenschutzrechtlichen Aufsicht über den öffentlich-rechtlichen Rundfunk. Bereits bisher galt für die Datenverarbeitung durch Presse, Rundfunk und sonstige Medien das sogenannte Medienprivileg, das nur eine eingeschränkte Geltung der materiell-rechtlichen Datenschutzvorschriften vorsah. Statt der Betroffenenrechte aus Kapitel III der Verordnung (EU) 2016/679 stehen den betroffenen Personen besondere Abwehrrechte, insbesondere der Gegendarstellungsanspruch, zu.

Bisher war das Medienprivileg für den Südwestrundfunk (SWR) im Landesdatenschutzgesetz vorgesehen. Der Einundzwanzigste Rundfunkänderungsstaatsvertrag sieht vor, dass dieses Medienprivileg zukünftig einheitlich geregelt werden soll. Künftig regelt also der Rundfunkstaatsvertrag im Rahmen des Medienprivilegs die Verarbeitung personenbezogener Daten durch den SWR zu journalistischen Zwecken und legt fest, ob und inwieweit Normen der Verordnung (EU) 2016/679 gelten.

Regelungen zur datenschutzrechtlichen Aufsicht über den SWR sollen wie bisher landesrechtlich festgelegt werden. Die Regelungen in § 39 des Staatsvertrags über den Südwestrundfunk sind bereits in Einklang mit der Verordnung (EU) 2016/679. Eine Fortschreibung der Regelungen ist jedoch im vorliegenden Gesetz notwendig, da der SWR-Staatsvertrag für den Datenschutz im Weiteren auf das Landesdatenschutzgesetz verweist. Da bereits mit dem Gesetz zu dem Staatsvertrag über den Südwestrundfunk und zur Änderung medienrechtlicher und datenschutzrechtlicher Vorschriften vom 3. Dezember 2013 zum 1. Januar 2014 die nach europäischen Vorgaben erforderlichen Normen zum Rundfunkbeauftragten für den Datenschutz geändert wurden, ist jetzt aufgrund der Verordnung (EU) 2016/679 nur noch eine geringfügige Anpassung notwendig.

- g) Artikel 51 Absatz 1 der Verordnung (EU) 2016/679 gibt vor, dass jeder Mitgliedstaat eine unabhängige Behörde einrichtet, welche für die Überwachung der Anwendung der Verordnung (EU) 2016/679 zuständig ist. Desgleichen sieht Artikel 41 Absatz 1 der 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. Mai 2016, S. 89) die Überwachung der Einhaltung dieser Richtlinie durch eine unabhängige Datenschutzaufsichtsbehörde vor. Beide Aufgaben nimmt – vorbehaltlich der Zuständigkeit sektoraler

Aufsichtsorgane – die oder der Landesbeauftragte für den Datenschutz für die öffentlichen Stellen des Landes wahr.

In diesem Gesetz werden die Einrichtung und die mit dem Amtsverhältnis verbundenen Rechte und Pflichten der oder des Landesbeauftragten für den Datenschutz sowohl aufgrund der Verordnung (EU) 2016/679 wie auch der Richtlinie (EU) 2016/680 geregelt, da diese dieselben Regelungen erfordern. Die Aufgaben und Befugnisse ergeben sich jeweils aus der Verordnung (EU) 2016/679 und ergänzend aus diesem Gesetz sowie für den Bereich der Richtlinie (EU) 2016/680 aus den zu deren Umsetzung ergangenen Gesetzen.

- h) Die oder der Landesbeauftragte für den Datenschutz wird entsprechend den Vorgaben der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 als unabhängige Aufsichtsbehörde eingerichtet. Hierzu wird die bisherige Einrichtung ihrer oder seiner Dienststelle beim Landtag aufgegeben und die oder der Landesbeauftragte für den Datenschutz als oberste Landesbehörde sui generis eingerichtet, entsprechend der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. Die oder der Landesbeauftragte für den Datenschutz erhält damit die Personalhoheit, welche Voraussetzung für die von der Verordnung (EU) 2016/679 geforderte Unabhängigkeit ist. Ihr oder ihm wird die Befugnis zur Ernennung ihrer oder seiner Beamtinnen und Beamten verliehen. Ihre oder seine Mitarbeiter unterliegen nur den Weisungen der oder des Landesbeauftragten für den Datenschutz. Eine Dienstaufsicht über die Landesbeauftragte für den Datenschutz oder den Landesbeauftragten für den Datenschutz ist ausgeschlossen.

Wie bisher ist es auch nach der Verordnung (EU) 2016/679 zulässig, sektorale Aufsichtsorgane zu schaffen. Dies war bislang für den Bereich der Kirchen und der öffentlich-rechtlichen Rundfunkanstalten der Fall und soll beibehalten werden. Es müssen aber detaillierte Regelungen insbesondere zu den Anforderungen der Artikel 51 bis 54 der Verordnung (EU) 2016/679 getroffen werden. Dies betrifft die Aufsicht über den SWR. Die Kirchen regeln ihre Angelegenheiten selbstständig gemäß Artikel 140 Grundgesetz in Verbindung mit Artikel 137 Absatz 3 der deutschen Verfassung vom 11. August 1919.

## 2. Dienstrechtliche Vorschriften

Die Änderungen des Landesbeamtengesetzes – LBG (Artikel 17), des Landesdisziplinalgesetzes – LDG (Artikel 18) und des Landespersonalvertretungsgesetzes – LPVG (Artikel 19) beinhalten die im Dienstrecht notwendigen gesetzlichen Anpassungen an die Verordnung (EU) 2016/679.

Die Verordnung (EU) 2016/679 verdrängt zwar in ihrem Anwendungsbereich entgegenstehendes nationales Datenschutzrecht. Allerdings regelt die Verordnung das Datenschutzrecht nicht abschließend. Im Beschäftigungskontext ermöglicht Artikel 88 der Verordnung (EU) 2016/679 spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Daten. Ergänzt um die Befugnis der Mitgliedstaaten nach Artikel 6 Absatz 2 und 3 der Verordnung (EU) 2016/679, spezifischere Bestimmungen zur Anpassung der Anwendung der Verordnung (EU) 2016/679 in Bezug auf die zur Erfüllung einer rechtlichen Verpflichtung oder zur Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe oder in Ausübung öffentlicher Gewalt erforderlichen Verarbeitung beizubehalten oder zu erlassen, ergibt sich damit weiterhin der nötige Regelungsspielraum, um im Bereich des Dienstrechts den Umgang mit personenbezogenen Daten von Beschäftigten zu regeln bzw. an bestehenden Regelungen festzuhalten. Die Verordnung (EU) 2016/679 wird somit durch bereichsspezifische Regelungen zur Datenverarbeitung, insbesondere im Personalaktendatenrecht (§§ 83 bis 88 LBG), ergänzt. Sofern auch insofern keine speziellen abschließenden Regelungen

gen getroffen werden, finden die Vorschriften des Landesdatenschutzgesetzes oder andere bereichsspezifische datenschutzrechtliche Vorschriften Anwendung.

a) Personalaktendatenrecht

Die Vorschriften zum Personalaktendatenrecht gemäß §§ 83 ff. des Landesbeamtengesetzes vom 9. November 2010 (GBl. S. 793, 794), das zuletzt durch Artikel 8 des Gesetzes vom 21. November 2017 (GBl. S. 597, 605) geändert worden ist (im Folgenden: LBG a. F.) werden an die Verordnung (EU) 2016/679 angepasst.

In § 83 Absatz 1 LBG wird eine zentrale Rechtsgrundlage für jegliche Vorgänge im Zusammenhang mit der Verarbeitung von Personalaktendaten im Beschäftigungsverhältnis geschaffen. Hierbei handelt es sich um eine zulässige spezifischere Regelung der Datenverarbeitung im Beschäftigungskontext im Sinne von Artikel 88 der Verordnung (EU) 2016/679. § 83 Absatz 1 LBG ist Rechtsgrundlage für jegliche Vorgänge im Zusammenhang mit der Verarbeitung von Personalaktendaten im Beschäftigungsverhältnis.

Die Rechtsgrundlage des § 83 Absatz 1 LBG wird durch die nachfolgenden Absätze bzw. Vorschriften für einzelne Konstellationen der Datenverarbeitung teilweise modifiziert. So bestimmt § 83 Absatz 2 LBG spezifische Voraussetzungen hinsichtlich der Verarbeitung von Beihilfedaten zu anderen als Beihilfezwecken. § 85 LBG regelt die Übermittlung von Personalaktendaten als einen Teilschritt der Verarbeitung und ist im Vergleich zu § 83 LBG als speziellere Vorschrift anzusehen. § 85 a LBG regelt, in welchen Fällen Datenverarbeitung im Auftrag zulässig sein soll. § 86 LBG bestimmt Lösungsfristen und besondere Lösungsbedingungen und konkretisiert damit in zeitlicher Hinsicht das Erforderlichkeitsprinzip (Artikel 5 Absatz 1 Buchstaben c und e der Verordnung [EU] 2016/679). § 87 LBG enthält eine spezifische Regelung zur Form der Auskunft an die betroffenen Beamtinnen und Beamten.

Nach § 84 LBG wird eine beamtenrechtliche Entscheidung, die auf einer ausschließlich automatisierten Verarbeitung beruht, zugelassen. Hierdurch wird der zunehmenden Bedeutung automatisierter Verfahren im Bereich der Verwaltungsarbeit, insbesondere im Beihilfe- und Reisekostenbereich, Rechnung getragen.

b) Weitere dienstrechtliche Vorschriften

Im Bereich des Landespersonalvertretungsgesetzes und des Landesdisziplinargesetzes erfolgen Anpassungen an die Begrifflichkeiten der Verordnung (EU) 2016/679.

3. Änderungen sonstiger Vorschriften

Neben notwendigen Folgeänderungen werden im Wesentlichen inhaltliche und begriffliche Anpassungen des bereichsspezifischen Datenschutzrechts an die Verordnung (EU) 2016/679 vorgenommen.

Mit dem Abschiebungshaftvollzugsgesetz Baden-Württemberg (AHaftVollzG BW) vom 17. Dezember 2015 (GBl. S. 1187) wird der Vollzug der Abschiebungshaft in Baden-Württemberg geregelt, soweit diese in einer Abschiebungshafteinrichtung vollzogen wird. Die Abschiebungshaftvollzugsverordnung (AHaftVO) vom 7. März 2016 (GBl. S. 219) beruht auf der Verordnungsermächtigung in § 16 AHaftVollzG BW und enthält Regelungen zur Durchführung der Abschiebungshaft. Neben den Anpassungen an die Verordnung (EU) 2016/679 wird in das Abschiebungshaftvollzugsgesetz zusätzlich eine

Regelung aufgenommen, wonach dieses zukünftig auch auf den Vollzug des Ausreisegewahrsams im Sinne des § 62 b des Aufenthaltsgesetzes (AufenthG) entsprechende Anwendung findet. Außerdem wird eine erweiterte Beschränkungsbefugnis für Fälle vorgesehen, in denen von den Untergebrachten eine erhebliche Gefahr für Leib oder Leben Dritter oder bedeutende Rechtsgüter der inneren Sicherheit ausgeht.

### III. Alternativen

Wegen der grundlegenden strukturellen Änderung des Datenschutzrechts durch die Verordnung (EU) 2016/679 ist eine bloße Änderung des bisherigen Landesdatenschutzgesetzes nicht opportun. Der Neufassung liegt der Systemwechsel im Datenschutzrecht mit dem Primat der Verordnung (EU) 2016/679 und ergänzender Anwendung des Landesrechts zugrunde.

Als Alternative zum Erlass eines eigenständigen Gesetzes kommt ein Verweisungsgesetz auf das Datenschutz-Anpassungs- und -Umsetzungsgesetz EU des Bundes, soweit es die Anpassung an die Verordnung (EU) 2016/679 regelt, in Betracht. Gegen ein Verweisungsgesetz spricht das Erfordernis, die Verordnung (EU) 2016/679 an die landes- und kommunalspezifischen Besonderheiten anzupassen sowie die Rechtsstellung der unabhängigen Aufsichtsbehörden im Land zu normieren. Eine teilweise Verweisung würde zu einer unübersichtlichen Verweiskette führen, die die Rechtsanwendung erschweren würde. Im Übrigen besteht nur eine Teilschnittmenge zum Datenschutz-Anpassungs- und -Umsetzungsgesetz EU des Bundes, da dieses auch das Datenschutzrecht für nichtöffentliche Stellen regelt, während das Landesdatenschutzgesetz ausschließlich das von den öffentlichen Stellen des Landes zu beachtende Datenschutzrecht enthält.

Untergesetzliche Regelungen reichen nicht aus, um die Öffnungsklausel der Verordnung (EU) 2016/679 zu nutzen, da sie keine ausreichende Legitimation für Grundrechtseingriffe in das informationelle Selbstbestimmungsrecht darstellen.

Eine Anpassung der dienstrechtlichen Vorschriften sowie der sonstigen bereichsspezifischen Datenschutzregelungen ist wegen des Anwendungsvorrangs der Verordnung (EU) 2016/679 unumgänglich.

### IV. Finanzielle Auswirkungen

Insbesondere die gegenüber der bisherigen Rechtslage erweiterten Pflichten der öffentlichen Stellen als Verantwortliche führen in der Verwaltung zu höheren Kosten. Nach der Verordnung (EU) 2016/679 ist jede öffentliche Stelle ab dem Inkrafttreten der Verordnung (EU) 2016/679 verpflichtet, einen Datenschutzbeauftragten zu benennen. Eine solche Verpflichtung gab es im bisherigen Landesdatenschutzgesetz nicht. Die dadurch entstehenden zusätzlichen Kosten – auch für die Kommunen – sind jedoch durch die Verordnung (EU) 2016/679 und nicht durch das Gesetz verursacht.

Darüber hinaus sieht die Verordnung (EU) 2016/679 mehr Aufgaben und Befugnisse für die Aufsichtsbehörde der oder des Landesbeauftragten für den Datenschutz vor, für deren Wahrnehmung diese oder dieser langfristig mehr Personal benötigen wird. Der konkrete Personalbedarf und die daraus resultierenden Personal- und Sachkosten der Aufsichtsbehörde werden durch das Gesetz weder ausgelöst noch konkretisiert. Sie sind allein auf die europäischen Vorgaben zurückzuführen.

## V. Ergebnis der Anhörung

### 1. Stellungnahmen zu dem Gesetzentwurf

(Hinweis: Die Stellungnahmen beziehen sich auf den Gesetzentwurf auf dem Stand vom 14. Dezember 2017, der den Verbänden und Institutionen übersandt wurde. Wegen des neu eingefügten § 14 verschieben sich die dort genannten §§ 14 bis 30 jeweils um eine Ziffer und entsprechen nunmehr den §§ 15 bis 31 des Gesetzentwurfs).

Zu dem Gesetzentwurf wurden die kommunalen Landesverbände nach Artikel 71 Absatz 4 der Landesverfassung, der Landesbeauftragte für den Datenschutz nach § 31 Absatz 4 Satz 2 des Landesdatenschutzgesetzes sowie die Beauftragte der Landesregierung für die Belange von Menschen mit Behinderungen nach § 14 Absatz 3 des Landes-Behindertengleichstellungsgesetzes und über 100 weitere Verbände und Institutionen angehört.

Folgende Verbände und Institutionen haben Stellungnahmen abgegeben:

- Anwaltsverband Baden-Württemberg im Deutschen Anwaltsverein e. V. (DAV BW)
- AOK Baden-Württemberg (AOK BW)
- Arbeitsgemeinschaft des Hauptpersonalratsvorsitzenden des Landes Baden-Württemberg beim Ministerium für Inneres, Digitalisierung und Migration (ARGE-HPR)
- Architektenkammer Baden-Württemberg (AK BW)
- Baden-Württembergische Krankenhausgesellschaft e. V. (BWKG)
- Baden-Württembergischer Handwerkstag e. V. (BWHT)
- Baden-Württembergischer Industrie- und Handelskammertag (IHK)
- Badischer Notarverein e. V. (BADNV)
- Beamtenbund Tarifunion (BBW)
- Bund Deutscher Finanzrichterinnen und Finanzrichter, Landesverband Baden-Württemberg (BDFR)
- Bund Deutscher Kriminalbeamter, Landesverband Baden-Württemberg (BDK)
- Deutsche Rentenversicherung Baden-Württemberg (DRV BW)
- Deutscher Gewerkschaftsbund, Bezirk Baden-Württemberg (DGB)
- Duale Hochschule Baden-Württemberg (DHBW)
- Evangelische Landeskirche in Baden, Evangelische Landeskirche in Württemberg, Erzdiözese Freiburg, Diözese Rottenburg-Stuttgart (Kirchen)
- Hauptpersonalrat beim Ministerium für Inneres, Digitalisierung und Migration Baden-Württemberg (HPR IM)
- Hauptpersonalrat für Grund-, Haupt-, Werkreal-, Real- und Gemeinschaftsschulen sowie an Sonderpädagogischen Bildungs- und Beratungszentren beim Ministerium für Kultus, Jugend und Sport Baden-Württemberg (HPR GHWRGS)
- Hauptschwerbehindertenvertretung der Polizei beim Ministerium für Inneres, Digitalisierung und Migration Baden-Württemberg (HSBV Polizei)
- Hochschulen für Angewandte Wissenschaften Baden-Württemberg (HAW BW)

- Ingenieurkammer Baden-Württemberg (ING BW)
- Karlsruher Institut für Technologie (KIT)
- Landesanstalt für Kommunikation Baden-Württemberg (LfK)
- Landesarchiv Baden-Württemberg (LA)
- Landesbeauftragter für den Datenschutz und die Informationsfreiheit (LfD)
- Landeselternbeirat Baden-Württemberg (LEB BW)
- Landesinnungsverband des Schornsteinfegerhandwerks Baden-Württemberg (LIV BW)
- Landesrektorenkonferenz Forschungsuniversitäten Baden-Württemberg (LRK)
- Landesschulbeirat Baden-Württemberg (LSB BW)
- Landessportverband Baden-Württemberg e. V. (LSV BW)
- Landkreistag Baden-Württemberg (LKT)
- Liga der freien Wohlfahrtspflege in Baden-Württemberg e. V. (Liga BW)
- Notarkammer Baden-Württemberg (NK BW)
- Pädagogische Hochschulen in Baden-Württemberg (PH BW)
- Rechnungshof Baden-Württemberg (RH)
- Rechtsanwaltskammer Freiburg (RAK FR)
- Rechtsanwaltskammer Stuttgart (RAK S)
- Rechtsanwaltskammer Tübingen (RAK TÜ)
- Regierungspräsidium Freiburg – behördlicher Datenschutzbeauftragter (RP FR)
- Städtetag Baden-Württemberg (ST)
- Steuerberaterkammer Stuttgart (StBK S)
- Südwestrundfunk (SWR)
- Universitätsklinikum Tübingen (UK TÜ)
- Universitätsklinikum Ulm (UK UL)
- Verband für Energie- und Wasserwirtschaft Baden-Württemberg e. V. (VfEW)
- Verband kommunaler Unternehmen e. V., Landesgruppe Baden-Württemberg (VKU)
- Versorgungswerk der Architektenkammer (VWdA)
- Versorgungswerk der Rechtsanwälte in Baden-Württemberg (VW RA)
- Versorgungswerk der Steuerberater Baden-Württemberg (StBVW)
- Zentrum für Kunst und Medien Karlsruhe (ZKM)

Die Stellungnahmen sind als Anlagen beigefügt.

## 2. Grundsätzliche Haltung der Verbände und Institutionen

### a) Allgemeines

Zusammengefasst ergibt sich aus den eingegangenen Stellungnahmen, dass die Notwendigkeit des Gesetzes von keiner Seite in Frage gestellt wird. Die Stellungnahmen lassen kein einheitliches Bild erkennen. Es wird auf der einen Seite positiv bewertet, dass der Landesgesetzgeber von der Möglichkeit

der Verwendung der Öffnungsklauseln Gebrauch macht. Auf der anderen Seite wird ein zu weitreichender Gebrauch der Öffnungsklauseln kritisiert. In vielen Stellungnahmen werden Ergänzungen und Nachbesserungen vorgeschlagen, wobei sich die meisten Stellungnahmen auf Artikel 1 des Gesetzentwurfs und damit die geplante Änderung des Landesdatenschutzgesetzes konzentrieren.

Angeführt wird in den Stellungnahmen häufig, dass die Neuregelung des allgemeinen Datenschutzrechts durch die vorgesehene Regelungstechnik zu erheblicher Intransparenz führe, was sowohl für die Bürgerinnen und Bürger als auch für die Mitarbeitenden der Landesverwaltung, die das Datenschutzrecht umsetzen und anwenden müssen, eine erhebliche Erschwernis bedeute. Aus diesem Grund wird mehrfach gefordert, im jeweiligen Normtext einen Bezug zu dem zu konkretisierenden Artikel der Verordnung (EU) 2016/679 herzustellen. Andererseits werden im vorliegenden Gesetzentwurf auch Verstöße gegen das Wiederholungsverbot beanstandet. Daneben wird mehrfach angeregt, die entsprechende Regelung des neuen Bundesdatenschutzgesetzes in den Gesetzentwurf zu übernehmen. Des Öfteren wird auch die Hoffnung geäußert, dass die notwendigen Anpassungen das Datenschutzrecht in den einzelnen Bundesländern harmonisieren. Darüber hinaus sollen das Gesetz zur Umsetzung der Richtlinie (EU) 2016/680 und der vorliegende Gesetzentwurf zu einer möglichst einheitlichen Regelung führen. Schließlich wird teilweise gefordert, dass das Land zusätzliche Mittel zur Umsetzung des Datenschutzgesetzes zur Verfügung stellt.

Die eigenständige Stellung des Landesbeauftragten für den Datenschutz in einer eigenen Behörde wird im Wesentlichen begrüßt, aber seine Befugnisse insbesondere in Bezug auf Berufsgeheimnisträger als zu weitgehend kritisiert.

Die Änderungsvorschläge der Verbände und Institutionen beziehen sich hauptsächlich auf die Regelungen in Artikel 1 des Gesetzentwurfs. Es gibt zahlreiche Änderungsvorschläge zu der Regelung der Datenverarbeitung zu anderen Zwecken (§ 5) sowie zu den Vorschriften bezüglich der Rechte der betroffenen Person (§§ 8 ff.). Außerdem werden der Beschäftigtendatenschutz sowie die Mitbestimmungsrechte der Interessenvertretungen als unzureichend kritisiert. Daneben werden zahlreiche Ergänzungen und Änderungen zu den Regelungen der Datenverarbeitung zu Forschungszwecken (§ 13) sowie bei Arbeits- und Dienstverhältnissen (§ 14) vorgeschlagen. Viele Anmerkungen gibt es auch zu § 17 (Videoüberwachung) und § 27 (Ordnungswidrigkeiten).

Bei den weiteren Artikeln des Gesetzentwurfs sind die Regelungen des Artikels 17 und somit die geplanten Änderungen zum Landesbeamtengesetz ein Schwerpunkt der abgegebenen Stellungnahmen.

Der Landesschulbeirat und der Landessportverband haben keine Änderungsvorschläge und können dem Gesetzentwurf uneingeschränkt folgen. Der Landeselternbeirat stimmt der Vorlage des Landesdatenschutzgesetzes vollumfänglich zu.

Der Gesetzentwurf wurde im Beteiligungsportal Baden-Württemberg veröffentlicht und konnte dort während der Anhörung kommentiert werden. Bis zu der Beendigung der Kommentierungsphase wurden insgesamt neun Kommentare von vier Nutzern abgegeben. Die Kommentare befassen sich mit den Themen Bußgelder für öffentliche Stellen, der Unabhängigkeit des Rundfunkbeauftragten sowie dem Datenschutzbeauftragten an den Hochschulen. Daneben wurde die Regelung zur wissenschaftlichen Forschung thematisiert sowie eine Regelung für die grenzüberschreitende Forschung gefordert.

## b) Einzelne Änderungsvorschläge

Der Landkreistag und der Städtetag sehen wegen der dynamischen Entwicklung des Datenschutzes in Zusammenhang mit der Digitalisierung Bedarf an einer „Experimentierklausel“ sowie einer Evaluierung des Landesdatenschutzgesetzes nach zwei Jahren. Im Übrigen werden Präzisierungen und Ergänzungen im Interesse der Verwaltung vorgeschlagen, insbesondere hinsichtlich des Anwendungsbereichs und der Regelung in Artikel 1 § 5 sowie der Übermittlungsvorschrift. Bezüglich der Regelung der Videoüberwachung öffentlich zugänglicher Räume wird der Wegfall des Tatbestandsmerkmals „tatsächliche Anhaltspunkte für eine Gefährdung“ begrüßt sowie eine Klarstellung des Anwendungsbereichs im Hinblick auf das Hausrecht angeregt. In Artikel 1 § 27 wird um Klarstellung gebeten, inwiefern gegen Kommunen Bußgelder erhoben werden können. Schließlich wird eine Klarstellung bezüglich der Verwendung von Personalaktendaten für die Außendarstellung angeregt.

Der LfD sieht erheblichen Nachbesserungsbedarf in zahlreichen Punkten, um den Anliegen der Verordnung (EU) 2016/679 gerecht zu werden. Er regt an, das Datengeheimnis zu regeln und verlangt erhebliche Änderungen von Artikel 1, §§ 14 und 17. Die Regelung in Artikel 1 § 18 sei daneben nicht mit der Verordnung (EU) 2016/679 vereinbar. Außerdem würde eine Rechtsgrundlage für die Anwendung von Zwangsmitteln zur Durchsetzung seiner Anordnungen gegenüber Behörden fehlen. Ergänzungs- und Änderungsbedarf sieht der LfD bei den Vorschriften über die Aufsichtsbehörden. Bei Artikel 15 kritisiert der LfD unter anderem die Speicherdauer von einer Woche im Rahmen der Videoüberwachung. Bezüglich Artikel 17 regt der LfD ebenfalls einige Änderungen an, unter anderen der Regelung zur Auftragsdatenverarbeitung sowie die Streichung von § 87 Absatz 4 Nummer 1. Schließlich schlägt er eine Änderung des Landesbesoldungsgesetzes vor.

Der Rechnungshof regt an die staatlichen Rechnungsprüfungsämter in die Regelung des Artikels 1 § 2 Absatz 4 Satz 3 aufzunehmen.

Der BBW und der DGB fordern insbesondere Nachbesserungen beim Beschäftigtendatenschutz und den Regelungen des Artikels 17 § 83 Absatz 1 und § 87, insbesondere in Bezug auf die Einschränkung des Auskunftsrechts.

Der DGB begrüßt Artikel 1 § 14 Absatz 3 im Interesse eines einheitlichen Rechts für alle Beschäftigtengruppen, fordert aber eine Regelung der Beteiligungsrechte der Interessenvertretungen der Beschäftigten und eine Nachbesserung des Absatz 6. Daneben werden fehlende Regelungen zur Bestellung von behördlichen Datenschutzbeauftragten bemängelt. Die dienstrechtlichen Regelungen, insbesondere zur Datenverarbeitung im Auftrag sowie zur automatisierten Datenverarbeitung werden abgelehnt. Dasselbe gilt für die bereits vom BBW kritisierte Einschränkung des Auskunftsrechts.

Die Personalvertretungen (ARGE-HPR, HPR IM und HPR GHWRGS) kritisieren einen unzureichenden Beschäftigtendatenschutz und schlagen ergänzende Regelungen zu Artikel 1 § 14 vor, insbesondere eine Verbesserung der Rechte der Personalvertretungen. Außerdem regen sie Änderungen des Artikels 17, vor allem des § 87, an, wofür sich auch die HSBV Polizei ausspricht.

Der Anwaltsverband Baden-Württemberg betrachtet Artikel 1 des Entwurfs in weiten Teilen als gelungen, verweist aber auf Defizite bei dem Schutz der in § 203 StGB genannten Berufsheimlichkeitsgeheimnisse und schlägt eine Einschränkung der Befugnisse der Aufsichtsbehörden im Rahmen der Berufsverschwiegenheit vor. Daneben seien die zahlreichen Beschränkungen der Rechte Betroffener nur unzureichend begründet und missachteten das

Grundrecht auf informationelle Selbstbestimmung. Außerdem solle der Anwendungsbereich des § 17 konkreter gefasst werden.

Die Rechtsanwaltskammern Freiburg, Stuttgart und Tübingen schlagen vor, dass die Aufsichtsbefugnisse des Landesdatenschutzbeauftragten gegenüber den Rechtsanwältinnen und Rechtsanwälten durch die zuständigen Rechtsanwaltskammern wahrgenommen werden. Sie begrüßen die Regelung des Artikels 1 § 27, sprechen sich aber für eine umfassende Wirkung des Verbots, gegen öffentliche Stellen Bußgelder zu verhängen aus.

Das Versorgungswerk der Rechtsanwälte sowie das Versorgungswerk der Steuerberater begrüßen den Wegfall des bisherigen § 10 LDSG sowie die Ausgestaltung des Artikels 1 § 4 als subsidiären Erlaubnistatbestand. Zu Artikel 1 § 27 wird vorgeschlagen, die Bußgelder gegen öffentliche Stellen uneingeschränkt auszuschließen. Das Versorgungswerk der Architektenkammer regt an, die Regelung zur Beschränkung der Informationspflicht in Artikel 1 § 8 zu überarbeiten.

Die Notarkammer und der Badische Notarverein verlangen bessere Regelungen zum Schutz der Daten, die ihrer notariellen Verschwiegenheitspflicht unterliegen.

Der Bund Deutscher Finanzrichterinnen und Finanzrichter befürchtet eine Beeinträchtigung der gerichtlichen Arbeit, wenn die Betroffenenrechte und Informationspflichten für die Justiz nicht beschränkt werden. Außerdem fehle es an der Regelung der Aufsicht über Datenverarbeitungsvorgänge bei den Gerichten.

Die Architektenkammer, die Ingenieurkammer und die Steuerberaterkammer fordern Nachbesserungen in Bezug auf Beschränkungen weiterer Betroffenenrechte, insbesondere des Rechts auf Einschränkung der Verarbeitung und des Widerspruchsrechts sowie der Benachrichtigungspflicht.

Der Handwerkstag und der Industrie- und Handelskammertag regen eine Beschränkung des Widerspruchsrechts sowie der Sanktionen in Artikel 1 § 28 auf Geldbußen an. Der IHK begrüßt daneben die Regelungen des Artikels 1 §§ 8 und 9 Absatz 2, wobei zusätzlich eine Regelung zur Beschränkung des Widerspruchsrechts gefordert wird. Daneben wird darauf hingewiesen, dass die Änderung von Artikel 14 § 32 Absatz 6 dem Datenschutzbeauftragten eine größere Pflicht auferlegt als die in der Verordnung (EU) 2016/679 vorgeschriebene Datenschutz-Folgeabschätzung. Der Landesinnungsverband des Schornsteinfegerhandwerks fordert Nachbesserungen in Artikel 1 §§ 6 und 13.

Der VfEW verweist darauf, dass Eigenbetriebe in Artikel 1 § 2 Absatz 6 nicht schlechter gestellt werden dürfen als Unternehmen die eine eigenständige Rechtsform haben. Der VKU fordert Klarstellungen in Artikel 1 §§ 3, 14 und 17 sowie eine dem neuen Bundesdatenschutzgesetz entsprechende Formulierung in Artikel 1 § 28.

Die Hochschulen für Angewandte Wissenschaften begrüßen die Intention des Gesetzentwurfs, im Rahmen der Regelungsspielräume angemessene Erweiterungen zugunsten der Forschung im Datenschutzrecht zu implementieren. Sie halten jedoch weitere Vereinfachungen für wünschenswert, um das Datenschutzrecht zu entbürokratisieren. Aus der Sicht der Uniklinika Ulm und Tübingen ist vor allem eine einheitliche Gesetzgebung zugunsten der Forschung über Landesgrenzen hinweg erforderlich. Der Gesetzentwurf schränke im Vergleich zu anderen Bundesländern die Forschung zu sehr ein, indem er ein „erhebliches“ Überwiegen der Forschungsinteressen verlange. Dieser Ansicht ist auch die BWKG.

Die Landesrektorenkonferenz Forschungsuniversitäten und die Pädagogischen Hochschulen teilen ebenfalls diese Auffassung und halten im Inte-

resse des Wissenschaftsstandorts Baden-Württemberg außerdem eine Beschränkung der Informationspflichten für erforderlich. Die Anonymisierungspflicht solle alle personenbezogenen Daten erfassen. Sie verweisen außerdem auf die Open Access-Strategie des Europäischen Forschungsraums, die dazu führen müsse, dass in größerem Umfang die Veröffentlichung personenbezogener Forschungsdaten erlaubt werde.

Das KIT fordert eine Rechtsgrundlage, die die Verarbeitung von Beschäftigten zu Zweck der Prüfrechte von Drittmittelgebern zulässt und hält die Anwendung der beamtenrechtlichen Regelungen auf alle Beschäftigten im öffentlichen Dienst für sachfremd.

Die DHBW bemängelt einige Ungenauigkeiten und fordert im Hinblick auf die Regelung zur Videoüberwachung sowie zur Überwachung von Beschäftigten engere Voraussetzungen.

Die AOK BW regt an, die Regelung in Artikel 1 § 27 entsprechend der Vorschrift des Bundesdatenschutzgesetzes zu fassen oder klarzustellen, dass gegen die gesetzlichen Krankenkassen keine Bußgelder verhängt werden können.

Die Deutsche Rentenversicherung schlägt unter anderem vor, die Vorschrift des § 16 Landeskreisregistergesetzes an die Verordnung (EU) 2016/679 anzupassen.

Die BWKG schlägt vor, um den Gebrauch des Landesdatenschutzgesetzes zu erleichtern, im jeweiligen Normtext einen Bezug zu dem konkretisierenden Artikel der Verordnung (EU) 2016/679 herzustellen. In Artikel 1 § 3 beanstandet die BWKG Verstöße gegen das Wiederholungsverbot. Daneben werden unter anderem Ergänzungen in Artikel 1 §§ 8 und 9, die die Betroffenenrechte zusätzlich einschränken, vorgeschlagen. In § 12 sollen die Erlaubnistatbestände des Artikels 9 Absatz 2 Buchstaben h und i der Verordnung (EU) 2016/679 aufgenommen werden. § 17 solle um die Wahrung des Hausrechts ergänzt werden.

Das Landesarchiv verweist darauf, dass der Gesetzentwurf keine Rechtsgrundlage für die Verarbeitung besonderer Kategorien von Daten sowie Ausnahmen von den Betroffenenrechten für im öffentlichen Interesse liegende Archivzwecke vorsieht. Da es weiterhin Archivierungsmöglichkeiten für Unterlagen geben soll, die Löschungsverpflichtungen unterliegen, wird um eine Ergänzung des Gesetzentwurfs gebeten. Die Bundesregelung könne hier Vorbild sein. Allerdings seien bei der Derogation für Archivzwecke auch Artikel 18 und 19 der Verordnung (EU) 2016/679 einzubeziehen. Des Weiteren solle die Anbietungspflicht durch eine entsprechende Regelung gesichert werden.

Die Kirchen bitten in ihrer Stellungnahme um die Aufnahme einer Regelung zur Übermittlung personenbezogener Daten an Stellen der öffentlich-rechtlichen Religionsgemeinschaften sowie einer Vorschrift zur Vollstreckung von Bußgeldbescheiden der kirchlichen Datenschutzaufsicht.

Die Liga der freien Wohlfahrtspflege erachtet die Videoüberwachung innerhalb der Abschiebungshafteinrichtung in Artikel 15 § 10 Absatz 4 in ihrer Ausgestaltung als „totale 24-h-Überwachung“ als unverhältnismäßig. Eine solche Maßnahme bedürfe außerdem einer richterlichen Anordnung.

Der Bund Deutscher Kriminalbeamter kritisiert im Rahmen des Artikels 11 § 16 den vollständigen Ausschluss der Verarbeitung genetischer Daten.

Die Landesanstalt für Kommunikation fordert eine Klarstellung in Artikel 1 § 24 dergestalt, dass die Zuständigkeit des Landesbeauftragten für den Datenschutz zur Aufsicht über den Datenschutz bei der LfK nicht gegeben ist, soweit der Vorsitzende des Vorstands seinerseits eine Aufsichtsfunktion nach § 50 Absatz 3 Landesmediengesetz-neu wahrnimmt.

Der SWR wünscht eine Klarstellung im Hinblick auf den Vorrang des Rundfunkbeitrags-Staatsvertrags. Außerdem hält er eine Einschränkung des Auskunftsrechts bei Datenspeicherung aufgrund gesetzlicher Aufbewahrungsvorschriften für angemessen. Eine Pflicht zur Veröffentlichung der Vergütung der oder des Rundfunkbeauftragten für den Datenschutz sei abzulehnen. Die Regelung zur Vereinbarkeit mit anderen Tätigkeiten innerhalb und außerhalb des SWR wird als zu einschränkend kritisiert. Der Gesetzgeber solle ferner die Feststellung treffen, dass die Amtszeit des derzeitigen Rundfunkbeauftragten für den Datenschutz unberührt bleibe.

Das ZKM begrüßt ausdrücklich, dass das Medienprivileg durch Artikel 1 § 18 ausgeweitet werden soll. Einige Unklarheiten in Bezug auf seine Reichweite müssten aber noch beseitigt werden.

Im Übrigen wird zu den Einwendungen im Einzelnen, soweit ihnen nicht gefolgt wurde (siehe unter 3.), unter 4. Stellung genommen.

### 3. Änderungen aufgrund des Ergebnisses der Anhörung sowie der Normenprüfung

Aufgrund der vorgebrachten Einwände und Anregungen wurden folgende inhaltliche Änderungen im Gesetzentwurf vorgenommen:

#### Zu Artikel 1 § 2

- Im Anwendungsbereich des Landesdatenschutzgesetzes wird klargestellt, dass die Polizeibehörden, der Polizeivollzugsdienst sowie die Gerichte und Staatsanwaltschaften ausgenommen sind, sofern sie zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten und Ordnungswidrigkeiten oder der Strafvollstreckung personenbezogene Daten verarbeiten, während die sonstigen Behörden erst ab der Einleitung eines Ordnungswidrigkeitenverfahrens aus dem Anwendungsbereich herausfallen (Absatz 1 Satz 3 Nummern 3, 4), im Übrigen aber unter das Landesdatenschutzgesetz fallen.
- Die staatlichen Rechnungsprüfungsämter sind in gleicher Weise wie der Rechnungshof zu behandeln, da es sich bei ihnen um eigenständige höhere Sonderbehörden im Geschäftsbereich des Rechnungshofs handelt, die gemeinsam die staatliche Finanzkontrolle in Baden-Württemberg bilden (Absatz 4).
- In Absatz 1 Satz 3 Nummer 3 werden die Gerichte aus dem Anwendungsbereich herausgenommen, sofern sie zur Umsetzung der Richtlinie (EU) 2016/680 tätig werden. In Absatz 5 erfolgt sodann eine klarstellende Regelung in Bezug auf die Verwaltungstätigkeit der Gerichte zu anderen als den in Absatz 1 Satz 3 Nummer 3 genannten Zwecken. Die Richtlinienumsetzung erfolgt durch ein eigenes Gesetz.

#### Zu Artikel 1 § 3

- Zur Sicherstellung des Datenschutzes sind Beispielmaßnahmen aufgeführt. Die Beteiligung der oder des Datenschutzbeauftragten ist nach Artikel 38 Absatz 1 der Verordnung (EU) 2016/679 aber verpflichtend und gehört daher nicht in diesen Katalog (Absatz 1 Satz 3).
- Die Vorschrift zum Datengeheimnis verdeutlicht die Verpflichtung der Beschäftigten bei den öffentlichen Stellen (Absatz 2).

## Zu Artikel 1 § 5

- Zur Wahrung erheblicher Belange des Gemeinwohls wird ebenfalls die Zweckänderung zugelassen (Absatz 1 Nummer 1), damit die in Artikel 23 Absatz 1 Buchstabe e genannten wichtigen Ziele des allgemeinen öffentlichen Interesses auch präventiv ausreichend geschützt werden können (z. B. im Haushalts- und Steuerbereich zur Sicherung des Steuer- und Zollaufkommens). Für die Abwehr einer Gefahr für die öffentliche Sicherheit wird die Zweckänderung erst erlaubt, wenn der Gefahrentritt unmittelbar droht. Dies entspricht der bisherigen Rechtslage.
- Die Erlaubnis zur Zweckänderung beschränkt sich auf die Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung.
- Weitere Klarstellungen sind in Absatz 3 und 4 enthalten.

## Zu Artikel 1 § 6

- Die Vorschrift zur Zulässigkeit der Übermittlung wird zur Erhöhung der Anwenderfreundlichkeit eingefügt (Absatz 1).

## Zu Artikel 1 § 8

- Für die Forschung wird die Informationspflicht ergänzend zu den sonstigen Beschränkungen der Betroffenenrechte in Artikel 1 § 13 Absatz 4 eingeschränkt (Absatz 1 Nummer 5).

## Zu Artikel 1 § 8 und § 11

- Um Missverständnisse zu vermeiden, werden die gesetzlichen Geheimhaltungsvorschriften (z. B. die notarielle Schweigepflicht) aufgenommen. Erforderlich ist eine Abwägung mit den Interessen der betroffenen Person (§ 8 Absatz 1 Nummer 3, § 11 Nummer 2).

## Zu Artikel 1 § 9

- Bei der Verarbeitung einer großen Menge von Informationen über die betroffene Person wird das Auskunftsrecht zwar eingeschränkt, jedoch die öffentliche Stelle verpflichtet, zumindest die Verarbeitungsvorgänge sowie die Art der verarbeiteten Daten zu benennen (Absatz 2).

## Zu Artikel 1 § 10

- Die betroffene Person ist über die Einschränkung der Verarbeitung anstelle der Löschung zu unterrichten, damit sie ihre Betroffenenrechte ggf. geltend machen kann. Die betroffene Person kann stattdessen die Löschung verlangen.

## Zu Artikel 1 § 12

- Die Einfügung des Forschungszwecks ergänzt die Forschungsregelung sinnvoll, indem personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, unter den dort genannten Voraussetzungen, auch zu Forschungs- oder statistischen Zwecken verarbeitet werden dürfen. Dasselbe gilt für die Verarbeitung zu Archivzwecken.

## Zu Artikel 1 § 13

- Die Datenverarbeitung zu Forschungszwecken bedarf auch hinsichtlich der Verarbeitung personenbezogener Daten einer Ermächtigungsgrundlage

außer der Einwilligung (Absatz 1 Satz 1). Bisher war eine solche nur für die Verarbeitung besonderer Kategorien personenbezogener Daten enthalten.

- Im Interesse der Forschung, für die ein öffentliches Interesse streitet, wird die Verarbeitung personenbezogener Daten einschließlich der Verarbeitung besonderer Kategorien personenbezogener Daten im Einklang mit Artikel 89 Absatz 1 der Verordnung (EU) 2016/679 bereits dann für zulässig gehalten, wenn das Forschungsinteresse das Interesse der betroffenen Person an einem Ausschluss der Verarbeitung überwiegt. Ein „erhebliches“ Überwiegen würde die Forschung zu sehr einschränken (Absatz 1 Satz 1).
- Die Anonymisierungspflicht soll alle personenbezogenen Daten erfassen (Absatz 2). In Satz 2 wurde der bisher fehlende Statistikzweck eingefügt.
- Zur Klarstellung wird bezüglich der Veröffentlichung auch die historische Forschung einbezogen (Absatz 3).
- Die Einschränkung der Betroffenenrechte wird im Interesse der Forschung an die Regelung in § 27 Absatz 2 des Bundesdatenschutzgesetzes angeglichen (Absatz 4).

Zu Artikel 1 § 14

- Die Vorschrift wird eingefügt, um den besonderen Interessen der Archivverwaltung, die auch besondere Kategorien personenbezogener Daten verarbeiten müssen, an einer spezifischen Einschränkung der Betroffenenrechte Rechnung zu tragen.

Zu Artikel 1 § 15

- Das Wort „nur“ wird gestrichen, da sich für bestimmte Verarbeitungssituationen eine Ermächtigung zur Datenverarbeitung direkt aus der Verordnung (EU) 2016/679 ergeben kann (Absatz 1 und 2).
- Die Beschäftigten- oder Bewerberdaten dürfen auch an die Interessenvertretungen wie den Personalrat oder die Schwerbehindertenvertretung übermittelt werden (Absatz 1).
- Die Verarbeitung der besonderen Kategorien personenbezogener Daten wird zur besseren Lesbarkeit in einem eigenen Absatz geregelt (Absatz 2).
- Rechtsgrundlage für die Verarbeitung besonderer Kategorien personenbezogener Daten können auch Kollektivvereinbarungen sein (Absatz 2).
- Die Verarbeitung besonderer Kategorien personenbezogener Daten muss auch zugunsten der Rechte der betroffenen Person zulässig sein. Dies entspricht der Regelung in Artikel 9 Absatz 2 Buchstabe b der Verordnung (EU) 2016/679 (Absatz 2).
- Nach der Rechtsprechung rechtfertigt auch der Verdacht einer schwerwiegenden Pflichtverletzung entsprechende Maßnahmen, die mit der Verarbeitung personenbezogener Daten einhergehen. Die Anhaltspunkte sind zu dokumentieren, um die Nachprüfbarkeit zu garantieren (Absatz 5).
- Die Verarbeitung biometrischer Daten zu Authentifizierungs- und Autorisierungszwecken wird geregelt (Absatz 6).
- Die Überwachung von Beschäftigten mit technischen Einrichtungen zum Zwecke der Verhaltens- und Leistungskontrolle ist differenziert zu betrachten: Während die optisch-elektronische Überwachung generell verboten ist, müssen sonstige Einrichtungen erforderlich sein und den Anforderungen des Artikels 5 der Verordnung (EU) 2016/679 genügen (Absatz 7).

- In Absatz 8 erfolgt eine Klarstellung in Bezug auf die Beteiligungsrechte der Interessenvertretungen der Beschäftigten.
- Auch sicherheitstechnisch relevante Bereiche können betroffen sein.

Zu Artikel 1 § 18

- In die Regelung zur Videoüberwachung wird zur Klarstellung der Zweck „zur Ausübung des Hausrechts“ aufgenommen und die Erforderlichkeit als Zulässigkeitsvoraussetzung ausdrücklich normiert. Die Vorschrift betrifft nur die Videoüberwachung öffentlich zugänglicher Räume. Die Erforderlichkeit ist im Einzelfall, mithin auf das zu überwachende Objekt bezogen, zu prüfen und zu begründen.

Zu Artikel 1 § 19

- Die Datenschutzaufsicht wird nicht ausgeschlossen. Sie wird durch die Landesbeauftragte für den Datenschutz oder den Landesbeauftragten für den Datenschutz ausgeübt. Die Haftung beschränkt sich auf unzureichende Maßnahmen nach den genannten Artikeln der Verordnung (EU) 2016/679. Das Auskunftsrecht soll ebenfalls in modifizierter Form ausgeübt werden können.

Zu Artikel 1 § 24

- Die Verschwiegenheitspflicht ist auf die Beschäftigten der oder des Landesbeauftragten für den Datenschutz zu erstrecken.

Zu Artikel 1 § 25

- Die Vorschrift ist § 30 LDSG a. F. nachgebildet (Absatz 4).
- Bei der Kontrolle der nichtöffentlichen Stellen hat das Bundesdatenschutzgesetz Vorrang. Die Notarinnen und Notare des Landes werden im Hinblick auf ihre Verschwiegenheitspflicht den Rechtsanwälten gleichgestellt. Im Übrigen wird die Geheimhaltungspflicht der kontrollierten Stelle auf die Aufsichtsbehörde erstreckt (Absatz 5).

Zu Artikel 1 § 30

- Auch für die Gerichte und die zur Verfolgung und Ahndung von Ordnungswidrigkeiten zuständigen Behörden sind Übergangsregelungen erforderlich.

Zu Artikel 13 Nummer 3

- § 20 Satz 2 der Meldeverordnung wird um einen Hinweis auf die Verordnung (EU) 2016/679 ergänzt, da die Anforderungen der Verordnung (EU) 2016/679 in Artikel 1 § 3 nicht vollständig enthalten, aber auf jeden Fall einzuhalten sind.

Zu Artikel 15 Nummer 3

- § 3 Absatz 4 Satz 2 des Abschiebungshaftvollzugsgesetzes wird um die Verarbeitungszwecke ergänzt.

Zu Artikel 15 Nummer 4 Buchstabe a

- Die Speicherfrist für die Aufzeichnungen aus der Videoüberwachung wird im neuen § 10 Absatz 4 des Abschiebungshaftvollzugsgesetzes auf drei Werkzeuge nach der Erhebung verkürzt.

## Zu Artikel 17 Nummer 2

- In § 83 Absatz 1 des Landesbeamtengesetzes wird die Verarbeitung aufgrund einer Dienstvereinbarung eingefügt.
- Wegen des umfassenden Verarbeitungsbegriffs der Verordnung (EU) 2016/679 wurden die Wörter „gespeichert, verändert oder verwendet“ durch das Wort „verarbeitet“ ersetzt (§ 83 Absatz 2 und Absatz 3).

## Zu Artikel 17 Nummer 5

- Der LfD hat in Bezug auf die Auftragsdatenverarbeitung angeregt, dass zum Schutz der Beschäftigten auf Grundlage von Artikel 88 der Verordnung (EU) 2016/679 spezifische Vorschriften getroffen werden sollen. Die ARGE-HPR und der DGB lehnen aufgrund der besonderen Sensibilität der Personalaktendaten jegliche Verarbeitung von Personalaktendaten im Auftrag, insbesondere auch eine Verarbeitung durch Externe ab.

Dem Anliegen des LfD soll durch Aufnahme eines neuen § 85 a Landesbeamtengesetz zur Verarbeitung von Personalaktendaten im Auftrag entsprochen werden. Dem Anliegen der ARGE-HPR und des DGB ist insoweit entsprochen worden, als der neue § 85 a eine spezifischere Vorschrift im Sinne von Artikel 88 der Verordnung (EU) 2016/679 enthält und die Verarbeitung durch nichtöffentliche Stellen an konkrete Voraussetzungen geknüpft wurde. Im Übrigen stellt die Verordnung (EU) 2016/679 in den unmittelbar geltenden Artikeln 28 und 29 Vorgaben hinsichtlich der Modalitäten und Anforderungen der Datenverarbeitung im Auftrag auf.

## Zu Artikel 17 Nummer 7

- Ergänzend wird in § 87 Absatz 3 die Pflicht aufgenommen, auf Verlangen die gefertigten Abschriften, Kopien oder Ausdrucke zu überlassen.
- Die Regelung, wonach Feststellungen über den Gesundheitszustand nicht der Auskunft unterliegen, wenn zu befürchten ist, dass die betroffene Beamtin oder der betroffene Beamte bei Kenntnis des Befunds weiteren Schaden an der Gesundheit nimmt, wird gestrichen.

## 4. Die Behandlung der sonstigen erheblichen Anregungen und Einwände

Von den Verbänden und Institutionen wurden außerdem folgende Anregungen oder Einwände vorgebracht, die nicht oder nicht vollständig zu den begehrten Änderungen des Gesetzentwurfs geführt haben:

## a) Intransparenz des Gesetzes

- Sowohl die ARGE-HPR als auch die BWKG weisen darauf hin, dass Artikel 1 des Gesetzes intransparent sei und für den Anwender schwer zu erschließen. Hilfreich sei, die Normen durch Verweise auf die entsprechenden Vorschriften der Verordnung (EU) 2016/679 zu ergänzen.

*Haltung der Landesregierung*

Wegen der unmittelbaren Geltung der Verordnung (EU) 2016/679 ist es dem Gesetzgeber verwehrt, eine vollständige Regelung der datenschutzrechtlichen Anforderungen zu treffen. Den Nationalstaaten ist nur eine ergänzende Regelung möglich, soweit die Verordnung (EU) 2016/679 hierzu Regelungsspielräume eröffnet. Im Übrigen gilt das Wiederholungsverbot, das es verbietet, die Regelungen der Verordnung (EU) 2016/679 zu wiederholen. Soweit sinnvoll wurden die Normen als Ergän-

zung zu den entsprechenden Artikeln der Verordnung (EU) 2016/679 gekennzeichnet.

b) Normenklarheit

- Der BBW fordert, weitgehend auf unbestimmte Rechtsbegriffe zu verzichten, um mehr Normenklarheit zu erreichen.

*Haltung der Landesregierung*

Begriffsdefinitionen sind im Wesentlichen in der Verordnung (EU) 2016/679 enthalten (vgl. Artikel 4) und verbindlich. Die Verwendung unbestimmter Rechtsbegriffe kennzeichnet im Übrigen das Datenschutzrecht seit langem und ist unvermeidlich. Es obliegt der Datenschutzaufsicht sowie den Gerichten, die unbestimmten Rechtsbegriffe verbindlich auszufüllen.

c) Wiederholungsverbot

- Verschiedentlich wird ein Verstoß gegen das Wiederholungsverbot gerügt.

*Haltung der Landesregierung*

Wiederholungen sind im Gesetzentwurf nur enthalten, soweit dies für erforderlich erachtet wird, um die Kohärenz zu wahren und die nationalen Rechtsvorschriften für die Personen, für die sie gelten, verständlicher zu machen (vgl. Erwägungsgrund 8 der Verordnung [EU] 2016/679).

d) Zersplitterung des Datenschutzrechts

- Vor allem aus dem Forschungsbereich und von den Wirtschaftsverbänden wird bemängelt, dass wegen der unterschiedlichen Auslegung der Verordnung (EU) 2016/679 in den einzelnen Bundesländern Standortnachteile erwachsen können. Die notwendigen Anpassungen sollten genutzt werden, um eine Harmonisierung des Datenschutzrechts herbeizuführen.

*Haltung der Landesregierung*

Die Regelungsspielräume können von den Bundesländern unterschiedlich genutzt werden. Im Übrigen wird die Institution des Europäischen Datenschutzausschusses in Zukunft zu einer einheitlicheren Auslegung des Datenschutzrechts führen.

e) Evaluierung nach zwei Jahren, Experimentierklausel, zusätzliche finanzielle Mittel

- LKT/ST fordern wegen der dynamischen Entwicklung des Datenschutzes in Zusammenhang mit der Digitalisierung eine „Experimentierklausel“ sowie eine Evaluierung des Landesdatenschutzgesetzes nach zwei Jahren. ARGE-HPR und PH BW halten es für erforderlich, dass das Land zusätzliche finanzielle Mittel zur Umsetzung der neuen datenschutzrechtlichen Anforderungen zur Verfügung stellt.

*Haltung der Landesregierung*

Die Datenschutzaufsicht übt ihre Tätigkeit unabhängig aus und gibt daher die Auslegung des Gesetzes im Zweifelsfall vor. In dem Rahmen, den

die Datenschutzaufsicht lässt, sind unterschiedliche Auslegungen möglich. Das Gesetz wird wie jedes Gesetz bei Bedarf überprüft und ggf. werden Nachbesserungen vorgenommen.

Zusätzliche finanzielle Mittel können nicht bereitgestellt werden. Im Einzelfall können bestehende Fördertöpfe einschlägig sein.

f) Zu den einzelnen Bestimmungen:

aa) Anwendungsbereich (Artikel 1 § 2)

Zu Absatz 4

- LKT/ST fordern eine Klarstellung, dass die nicht-elektronische Datenverarbeitung generell von Absatz 4 Satz 2 erfasst wird, damit wie bisher nur für die automatisierten Verfahren ein Verzeichnis geführt werden muss.

*Haltung der Landesregierung*

Für eine solche Regelung bietet die Verordnung (EU) 2016/679 keine Öffnungsklausel, da sie den Dateibegriff abschließend regelt.

Zu Absatz 6

- UK TŪ und UK UL sowie die AOK BW regen an, den in Absatz 6 verwendeten Unternehmensbegriff näher zu definieren. Der VfEW fordert zusätzlich, dass Unternehmen im Wettbewerb ohne eigenständige Rechtsform, z. B. Eigenbetriebe, nicht schlechter gestellt werden als solche Unternehmen mit eigener Rechtspersönlichkeit.

*Haltung der Landesregierung*

Entscheidend für die Regelung ist die Gleichstellung der öffentlich-rechtlich organisierten Wettbewerbsunternehmen mit den privatrechtlich organisierten, wobei das Erfordernis der eigenen Rechtspersönlichkeit eine klare Abgrenzung erlaubt. Die Regelung bestand bereits nach altem Recht.

bb) Sicherstellung des Datenschutzes (Artikel 1 § 3)

- Der DGB fordert, die Einhaltung technischer Mindeststandards festzuschreiben. Vielfach wird die Norm als Verstoß gegen das Wiederholungsverbot angesehen (LfD, BWKG, UK TŪ, UK UL) bzw. um Klarstellung gebeten, dass es sich um eine nicht abschließende Aufzählung handelt.

*Haltung der Landesregierung*

Mit dem Verweis auf den Stand der Technik sind technische Mindeststandards erfasst. Aus dem Wort „insbesondere“ in Absatz 1 Satz 3 ergibt sich der beispielhafte Charakter. Teilweise handelt es sich um Wiederholungen aus Artikel 32 der Verordnung (EU) 2016/679. Diese werden jedoch im Interesse einer kohärenten Regelung als zulässig angesehen.

## cc) Zulässigkeit der Verarbeitung personenbezogener Daten (Artikel 1 § 4)

- Die Vorschrift wird vom Versorgungswerk der Rechtsanwälte als subsidiäre Rechtsgrundlage begrüßt. Ebenso sieht sie die ING BW als Rechtsgrundlage ihrer Schlichtungstätigkeit und juristischen Rechtsberatung. Der LfD bemängelt jedoch, dass die Vorschrift dem Gesetzesvorbehalt nicht ausreichend Rechnung trägt, vielmehr nur „Aufgaben, die der öffentlichen Stelle durch oder aufgrund eines Gesetzes“ übertragen wurden, heranzuziehen sind.

*Haltung der Landesregierung*

Dem Gesetzesvorbehalt ist Genüge getan, da sich die „Aufgabe“ im Sinne des Gesetzes immer aus einer Rechtsgrundlage ergeben muss, die die „zuständige“ Behörde bestimmt.

## dd) Datenverarbeitung zu anderen Zwecken (Artikel 1 § 5)

## Zu Absatz 1

- Der IHK bemängelt das Fehlen eines Tatbestands, der die Verarbeitung von Daten aus öffentlichen Quellen einbezieht sowie eine Zweckänderung aufgrund mutmaßlicher Einwilligung gestattet.

*Haltung der Landesregierung*

Die Verarbeitung von Daten, die aus allgemein zugänglichen Quellen entnommen werden können, stellt keine Zweckänderung dar. Die Verarbeitung aufgrund einer mutmaßlichen Einwilligung wird unter Geltung der Verordnung (EU) 2016/679 als zu starker Eingriff in die informationelle Selbstbestimmung der betroffenen Person angesehen.

## Zu Absatz 3

- Der DAV BW findet die Regelung nicht überzeugend, weil nicht ersichtlich sei, welche Interessen die öffentliche Stelle über den verfolgten Zweck hinaus haben könne.

*Haltung der Landesregierung*

Ergänzend zu der erlaubten Zweckänderung wird die Informationspflicht gemäß Artikel 13 der Verordnung (EU) 2016/679 für den Fall beschränkt, dass bei der Information über die Zweckänderung der beabsichtigte Zweck unter Umständen nicht erreicht werden könnte. Eine entsprechende Regelung sieht die Verordnung (EU) 2016/679 in Artikel 14 Absatz 5 Buchstabe b der Verordnung (EU) 2016/679 vor, wenn die Daten nicht bei der betroffenen Person erhoben wurden.

## ee) Übermittlung personenbezogener Daten (Artikel 1 § 6)

- Der LfD sowie das RP FR bezweifeln die grundsätzliche Zulässigkeit der Regelung, da nach Artikel 5 der Verordnung (EU) 2016/679 grundsätzlich die verarbeitende öffentliche Stelle die Verantwortung trägt. Außerdem bemängelt der LfD das Fehlen einer spezifischen Regelung zu automatisierten Abrufverfahren.

*Haltung der Landesregierung*

Die Regelung bestimmt nach Auffassung der Landesregierung in zulässiger Weise den Verantwortlichen. Regelungen zur Zulässigkeit

automatisierter Abrufverfahren sind nach der Verordnung (EU) 2016/679 nicht zulässig.

ff) Datenverarbeitung in der gemeinsamen Dienststelle (Artikel 1 § 7)

- Vom DAV BW wird eine ausreichende Regelung über den innerbehördlichen Datenaustausch unter Berücksichtigung des „Once Only Prinzips“ vermisst. Die ARGE-HPR und der HPR GHWRGS bemängeln die fehlende Definition der „örtlich zuständigen öffentlichen Stelle“.

*Haltung der Landesregierung*

Diese Vorschrift betrifft lediglich die gemeinsame Dienststelle nach § 16 Absatz 1 des Landesverwaltungsgesetzes und wurde inhaltlich unverändert aus § 33 a LDSG a. F. übernommen. Sonstige Datenübermittlungen innerhalb der Dienststelle richten sich nach den allgemeinen Vorschriften. Zur Implementierung des „Once Only Prinzips“ gibt es insbesondere im Hinblick auf die Nutzung von Registerdaten erste Überlegungen, auch auf Bundesebene, die in den nächsten Jahren eine Anpassung der datenschutzrechtlichen Vorschriften oder sonstigen Fachgesetze erwarten lassen.

gg) Beschränkung der Informationspflicht (Artikel 1 § 8)

- Während der DAV BW die Beschränkungen als zu weitreichend ablehnt, wird die Regelung vom IHK begrüßt. LKT/ST regen an, die landesrechtlichen Regelungen an die verwaltungsvereinfachenden Regelungen des Bundesdatenschutzgesetzes anzupassen. Der BWKG gehen dagegen die Einschränkungen der Informationspflicht nicht weit genug; sie fordert weitere Ausnahmen bei unverhältnismäßigem Aufwand für die öffentliche Stelle, aber geringem Interesse der betroffenen Person sowie der Regelung der Datenverarbeitung in Rechtsvorschriften.

*Haltung der Landesregierung*

Die Landesregierung hat sich bei der Regelung von der Absicht leiten lassen, die Informationspflicht im Interesse der betroffenen Person so wenig wie möglich einzuschränken. Dem wird eine Beschränkung durch unverhältnismäßigen Aufwand nicht gerecht.

Zu Absatz 1 Nummer 2

- Der DAV BW hält es für erforderlich, Absatz 1 Nummer 2 auf Ordnungswidrigkeiten von erheblicher Bedeutung zu beschränken.

*Haltung der Landesregierung*

Diese Beschränkung wird nicht für erforderlich gehalten. Dem Gewicht der Ordnungswidrigkeit ist bei der Abwägung mit dem Interesse der betroffenen Person an der Informationserteilung Rechnung zu tragen.

Zu Absatz 1 Satz 1 Nummer 3

- Für den DAV BW ist kein öffentliches Interesse an dieser Regelung ersichtlich, da die öffentliche Stelle sich mit der Zurückhaltung der Information in Widerspruch zum Rechtsstaatsgebot setzen würde.

*Haltung der Landesregierung*

Das Ergebnis der vorzunehmenden Abwägung kann nicht vorweggenommen werden. Der Staat kann auch als Privater handeln, z. B. privatrechtliche Verträge schließen und in diesem Kontext andere Interessen als sein Vertragspartner verfolgen. Im Übrigen bleiben prozesuale Rechte sowie Akteneinsichtsrechte unberührt.

## hh) Beschränkung des Auskunftsrechts (Artikel 1 § 9)

## Zu Absatz 1 Satz 1

- Die BWKG sowie der SWR fordern, das Auskunftsrecht auch dann zu beschränken, wenn die Daten nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher (SWR), satzungsmäßiger oder vertraglicher Aufbewahrungsfristen (BWKG) nicht gelöscht werden dürfen.

*Haltung der Landesregierung*

Eine derartige umfängliche Einschränkung wird als zu weitgehend angesehen, da aus dem Auskunftsrecht weitere Betroffenenrechte erwachsen können, wie etwa Berichtigung und Löschung, die ohne Auskunft nicht geltend gemacht werden könnten.

## Zu Absatz 1 Satz 2

- Der DAV BW sowie der LfD sehen die Beschränkung als zu weitgehend an.

*Haltung der Landesregierung*

Wegen der Zweckbindung der Daten besteht keine Gefahr für das informationelle Selbstbestimmungsrecht der betroffenen Person.

## Zu Absatz 2

- Die LRK, die PH BW und die HAW BW fordern eine Definition bzw. Präzisierung des Begriffs „eine große Menge von Informationen“.

*Haltung der Landesregierung*

Wegen der Vielzahl möglicher Fallgestaltungen erscheint eine Präzisierung des Begriffs nicht sinnvoll.

## Zu Absatz 5

- Der DAV BW sieht durch die Einschränkung der Prüfungsbefugnis des Landesbeauftragten für den Datenschutz den Rechtsschutz für die Bürger in unzulässiger Weise gekürzt.

*Haltung der Landesregierung*

Eine entsprechende Regelung ist auch in § 34 Absatz 3 Bundesdatenschutzgesetz enthalten und zum Schutz der öffentlichen Sicherheit erforderlich. Sie ist restriktiv zu handhaben, das heißt als eine Art Notstandsklausel anzusehen, deren Anwendung nur in extremen Ausnahmefällen in Betracht kommt.

## ii) Beschränkung des Rechts auf Löschung (Artikel 1 § 10)

## Zu Absatz 2

- Der LfD fordert, die Löschung nur dann zu unterlassen, wenn der Wille der betroffenen Person zuvor ermittelt wurde.

*Haltung der Landesregierung*

Durch die Einschränkung der Verarbeitung statt der Löschung entstehen für die betroffene Person keine Nachteile, während umgekehrt durch eine Löschung, die nach der Verordnung (EU) 2016/679 zwingend wäre, sobald die Daten nicht mehr benötigt werden, der betroffenen Person jedoch erhebliche Nachteile entstehen könnten. Die Erforschung des Willens der betroffenen Person im Einzelfall würde die öffentlichen Stellen unangemessen belasten.

## Zu Absatz 3

- Die ARGE-HPR kritisiert die Beschränkung als zu weitgehend.

*Haltung der Landesregierung*

Die Beschränkung des Rechts in dem vorgenommenen Umfang ist geringfügig und sieht im Sinne von Artikel 23 Absatz 2 der Verordnung (EU) 2016/679 ausreichende Rechte zugunsten der betroffenen Personen vor.

## jj) Beschränkung der Benachrichtigungspflicht (Artikel 1 § 11)

- Die AK BW, die ING BW sowie die StBK S fordern, die Regelung um eine Nummer 4 zu ergänzen, die die Pflicht zur Benachrichtigung bei unverhältnismäßigem Aufwand entfallen lässt.

*Haltung der Landesregierung*

Eine derartige Einschränkung des Betroffenenrechts lässt Artikel 23 Absatz 1 der Verordnung (EU) 2016/679 nicht zu.

- Der LfD fordert die Streichung der Nummer 3, da diese inhaltlich bereits von Nummer 1 umfasst ist.

*Haltung der Landesregierung*

Die Regelung soll zur Klarstellung beibehalten werden.

## kk) Verarbeitung personenbezogener Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen (Artikel 1 § 12)

- Die BWKG regt an, die Erlaubnistatbestände des Artikels 9 Absatz 2 Buchstaben h und i der Verordnung (EU) 2016/679 in die Vorschrift aufzunehmen.

*Haltung der Landesregierung*

Die Regelung der Verarbeitung besonderer Kategorien personenbezogener Daten im Gesundheits- und Sozialbereich ist speziellen Gesetzen vorbehalten.

Zu Absatz 2 Nummer 2

- Der LfD kritisiert die Zulassung der Zweckänderung zur Abwehr einer Gefahr für die öffentliche Sicherheit.

*Haltung der Landesregierung*

Die Regelung entspricht der bisherigen Regelung in § 34 Absatz 2 LDSG a. F. und ist gemäß Artikel 23 Absatz 1 Buchstaben a, c, d, e und i der Verordnung (EU) 2016/679 zulässig. Artikel 9 der Verordnung (EU) 2016/679 bleibt unberührt.

II) Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken (Artikel 1 § 13)

- Aus Sicht der UK TÜ und UK UL würden ohne die landesrechtlichen Regelungen mit den Regelungen der Verordnung (EU) 2016/679 eine geeignete Basis für die wissenschaftlichen Herausforderungen bestehen.

*Haltung der Landesregierung*

Dieser Hinweis ist nicht zutreffend. Gemäß Artikel 9 Absatz 2 Buchstabe h der Verordnung (EU) 2016/679 bedarf es mitgliedstaatlicher Regelungen im Bereich der Forschung.

- Die HAW BW halten einen einheitlichen Forschungsbegriff für vorzugswürdig. Außerdem schlagen sie vor, Verarbeitung und Veröffentlichung in getrennten Paragraphen zu regeln.

*Haltung der Landesregierung*

Der Begriff „wissenschaftliche oder historische Forschungszwecke“ wird in der Verordnung (EU) 2016/679 verwendet und ist damit verbindlich. Wegen des Sachzusammenhangs mit der Forschung soll die Veröffentlichung nicht gesondert geregelt werden, zumal diese auch die Verarbeitung personenbezogener Daten betrifft. Der unterschiedliche Regelungsgehalt wird durch die Trennung in verschiedene Absätze hinreichend deutlich.

Zu Absatz 1

- Die BWKG sieht die Interessenabwägung durch die Regelung auf das individuelle Interesse des Verantwortlichen verengt; es müsse um das Interesse der Allgemeinheit gehen. Außerdem fehle ein Hinweis auf die Einwilligung als mögliche Rechtsgrundlage. Bisher sei es nur bei einer Verarbeitung ohne Kenntnis der betroffenen Person erforderlich gewesen, dass der Forschungszweck ohne die Verarbeitung nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden könnte. Ferner vermisst sie die bisherige Regelung des § 19 LDSG a. F., die es zuließ, die Anonymisierung auch durch den Empfänger der Daten durchführen zu lassen.

*Haltung der Landesregierung*

Maßgeblich ist auch nach der getroffenen Regelung stets das wissenschaftliche Interesse. Die Möglichkeit der Einwilligung folgt unmittelbar aus Artikel 6 Absatz 1 Buchstabe a bzw. Artikel 9 Absatz 2

Buchstabe a der Verordnung (EU) 2016/679. Im Übrigen folgt die Regelung den Vorgaben der Verordnung (EU) 2016/679, wenn sie die Erforderlichkeit zur Zweckerreichung verlangt.

Gerade bei einer Übermittlung besteht eine erhöhte Gefahr für die Rechte und Freiheiten der betroffenen Person. Zum Schutz der betroffenen Person ist daher die Anonymisierung durchzuführen, sobald dies nach dem Forschungszweck möglich ist.

- Die LRK sowie die PH BW fordern, dass „Interessen“ der betroffenen Person, die nicht überwiegen dürfen, durch die „schutzwürdigen Belange“ der betroffenen Person zu ersetzen seien.

#### *Haltung der Landesregierung*

Da es um Interessenabwägung geht, soll es bei dem Begriff bleiben. Auch das Bundesdatenschutzgesetz verwendet diesen Begriff.

- UK UL und UK TŪ fordern, dass öffentliche Stellen besondere Kategorien personenbezogener Daten zu Forschungs- oder Statistikzwecken verarbeiten dürfen, wenn die Einholung der Einwilligung nicht möglich ist oder mit unverhältnismäßigem Aufwand verbunden wäre, das Interesse der öffentlichen Stelle das Interesse der betroffenen Person an einem Ausschluss überwiegt, die Verarbeitung erhebliche Fortschritte im Allgemeininteresse ermöglicht und die Verarbeitung geeigneten Garantien für die Rechte und Freiheiten der betroffenen Person gemäß der Verordnung (EU) 2016/679 unterliegt.

#### *Haltung der Landesregierung*

Die Verordnung (EU) 2016/679 lässt eine solche Regelung nicht zu, da Verarbeitungen personenbezogener Daten nur zulässig sind, wenn sie zur Erreichung des Forschungszwecks erforderlich sind.

#### Zu Absatz 2

- Die HAW BW fordern, eine alternative Lösung zur Anonymisierung für die Fälle vorzusehen, in denen die Anonymisierung nur mit unverhältnismäßig großem Aufwand möglich wäre. Der LIV BW sieht Fälle, in denen die Anonymisierung zur Wahrung der Rechte und Freiheiten der betroffenen Person nicht ausreicht.

#### *Haltung der Landesregierung*

Die Pflicht zur Anonymisierung besteht nur, wenn dies nach dem Forschungszweck möglich ist. Im Übrigen gilt Artikel 1 § 3 für alle Verarbeitungen personenbezogener Daten. Danach kann auch eine aggregierte Zusammenstellung der personenbezogenen Daten eine Maßnahme zur Wahrung der Interessen der betroffenen Person sein.

#### Zu Absatz 3

- Die LRK und die PH BW fordern die Schaffung einer Rechtsgrundlage für die Veröffentlichungen der Forschung betreibenden Stellen. Dies sei im Zuge des wissenschaftspolitisch gewollten „Open Access“-Gedankens erforderlich. Die HAW BW fordern eine Ausweitung der Vorschrift dahingehend, dass eine Veröffentlichung immer dann zulässig ist, wenn dies für die Darstellung von Forschungsergebnissen unerlässlich ist.

*Haltung der Landesregierung*

Die Regelung entspricht der bisherigen Rechtslage.

- Der LfD kritisiert, dass durch die Regelung zur Veröffentlichung in die Betroffenenrechte eingegriffen werde, anstatt diese zu garantieren, zumal die derzeitige Voraussetzung des § 35 Absatz 3 LDSG a. F., wonach schutzwürdige Interessen nicht entgegenstehen dürfen, entfalle.

*Haltung der Landesregierung*

Absatz 3 schränkt die Veröffentlichung als Form der Verarbeitung ein. Diese Einschränkung dient den Betroffenenrechten. Im Übrigen verzichtet auch das Bundesdatenschutzgesetz auf eine Einschränkung bei entgegenstehenden schutzwürdigen Interessen.

*Zu Absatz 4*

- Der DAV BW sieht keine Begründung dafür, warum die Beschränkung für den Forschungszweck erforderlich sein könnte.

*Haltung der Landesregierung*

Diese Einschränkung folgt unmittelbar aus Artikel 89 Absatz 2 der Verordnung (EU) 2016/679.

*mm) Datenverarbeitung bei Dienst- und Arbeitsverhältnissen (Artikel 1 § 15)*

- Der LfD fordert eine klarstellende Regelung, dass die Vorschrift auch anzuwenden ist, wenn personenbezogene Daten von Beschäftigten verarbeitet werden, ohne dass sie in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Ferner hält er es für angebracht, die Grundsätze für die Beurteilung der Freiwilligkeit einer Einwilligung gesetzlich zu regeln und die Schriftform anzudordnen, um dem Schutz der Beschäftigten Rechnung zu tragen.

*Haltung der Landesregierung*

Die Anwendbarkeit des Landesdatenschutzgesetzes für alle Formen der Verarbeitungen personenbezogener Daten ergibt sich aus Artikel 1 § 2 Absatz 4 Satz 1, der außerhalb des sachlichen Anwendungsbereichs der Verordnung (EU) 2016/679 die entsprechende Geltung anordnet.

Die Freiwilligkeit der Einwilligung ist Voraussetzung ihrer Wirksamkeit. Sie ist vom Arbeitgeber nachzuweisen. Gesetzliche Regelungen sind insofern nicht notwendig. Wegen der fortschreitenden Digitalisierung, die auch im Rechtsverkehr zunehmende Bedeutung erlangt, wird das Schriftformerfordernis nicht mehr für zeitgemäß gehalten.

*Zu Absatz 1*

- Das KIT bittet darum, als Zweck der Verarbeitung von Beschäftigten die Prüfrechte von Drittmittelgebern aufzunehmen, da hierfür Arbeitsverträge übermittelt werden müssten.

*Haltung der Landesregierung*

Dieser Bitte wird nicht nachgekommen. Eine solche Vorschrift stünde – jedenfalls soweit es Beamte angeht – in Widerspruch zu § 85

Absatz 1 Nummer 10 LBG, wonach die Übermittlung von Personalaktendaten nur unter engeren Voraussetzungen möglich ist. Die dort vorgesehene Abwägung in jedem Einzelfall dient gerade dem Schutz der informationellen Selbstbestimmung. Im Übrigen bleibt eine solche Regelung Spezialgesetzen vorbehalten.

Zu Absatz 3

- Der ARGE-HPR sowie dem HPR GHWRGS ist es ein Anliegen, eine Regelung zu ergänzen, die wie bisher die Löschung der Bewerbungsunterlagen spätestens nach einem Jahr, außer in begründeten Ausnahmefällen, anordnet.

*Haltung der Landesregierung*

Die Verordnung (EU) 2016/679 verlangt im Grundsatz eine unverzügliche Löschung, sobald die Daten nicht mehr benötigt werden. Dem würde eine regelmäßige einjährige Aufbewahrung widersprechen.

Zu Absatz 4

- Das KIT hält eine entsprechende Anwendung der beamtenrechtlichen Vorschriften auf die Angestellten und Arbeiter für nicht angemessen.

*Haltung der Landesregierung*

Die Regelung entspricht der bisherigen Rechtslage. Eine Änderung ist nicht beabsichtigt. Für das Personalaktendatenrecht sollen im Land generell die gleichen Regelungen für alle Beschäftigten gelten.

nn) Öffentliche Auszeichnungen und Ehrungen (Artikel 1 § 16)

- Der LfD sieht keine Rechtfertigung, für den genannten Zweck in erheblicher Weise in die Grundrechte der betroffenen Person einzugreifen und die Betroffenenrechte auszuschließen.

*Haltung der Landesregierung*

Die Verleihung staatlicher und kommunaler Auszeichnungen und Ehrungen ist eine Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt. Die Verordnung (EU) 2016/679 ist daher nicht unmittelbar anwendbar.

Eine vorzeitige Information über die Erhebung von Daten für ein Auszeichnungs- und Ehrungsverfahren sowie die Wahrnehmung des Auskunftsrechts sind dem Verfahren nicht angemessen. Durch die angeordnete Zweckbindung sind Beeinträchtigungen der Rechte und Freiheiten der betroffenen Personen nicht zu befürchten. Wie für jede Tätigkeit der Verwaltung gilt auch hier der Verhältnismäßigkeitsgrundsatz, der eine willkürliche Durchleuchtung ausschließt.

oo) Verarbeitung personenbezogener Daten im öffentlichen Interesse (Artikel 1 § 17)

Zu Absatz 1

- Der LfD hält die Bestimmung für zu unbestimmt und nicht ausreichend. Die HAW BW sowie die LRK fordern, auf das Erfordernis

der Einwilligung zu verzichten, da dieses in der Praxis erforderliche Tätigkeiten behindert.

*Haltung der Landesregierung*

Die Zuverlässigkeitsüberprüfung bezieht sich nicht auf die Beschäftigten, sondern auf Dritte, die in sicherheitsrelevante Bereiche von öffentlichen Stellen gelangen sollen. Daten dürfen nur im erforderlichen Umfang erhoben werden. Auf die Einwilligung kann wegen der Eingriffstiefe nicht verzichtet werden. Im Übrigen steht es den öffentlichen Stellen frei, ggf. auf die Zuverlässigkeitsüberprüfung zu verzichten, sofern diese nicht gesetzlich vorgeschrieben ist.

Zu Absatz 2

- Der LfD regt an, eine Regelung zur Zweckänderung zusätzlich aufzunehmen, die § 24 Absatz 2 Bundesdatenschutzgesetz entspricht.

*Haltung der Landesregierung*

Der Vorschlag wird nicht aufgegriffen; Satz 1 umfasst alle Arten der Verarbeitung, auch die Zweckänderung und Übermittlung unter den genannten Voraussetzungen.

pp) Videoüberwachung öffentlich zugänglicher Räume (Artikel 1 § 18)

Zu Absatz 1

- Sowohl die DHBW als auch der LfD kritisieren, dass in Zukunft bereits eine abstrakte Gefahr ausreichen soll, um die Videoüberwachung zu rechtfertigen. Der VKU möchte eine Klarstellung, dass öffentliche Parkhäuser erfasst sind.

*Haltung der Landesregierung*

Der Gesetzentwurf enthält im Gegensatz zur Regelung in § 20 a LDSG a. F. nicht mehr die Voraussetzung, dass „Tatsachen die Annahme rechtfertigen, dass die (...) genannten Rechtsgüter, Einrichtungen oder Objekte gefährdet sind“. Daraus zu schließen, dass es keiner Anhaltspunkte für eine Gefahr mehr bedürfe, ist unzutreffend. Das Tatbestandsmerkmal der Erforderlichkeit verlangt auf jeden Fall die Beurteilung der Gefahr im Einzelfall mit dem Unterschied, dass im Gegensatz zur bisherigen Regelung sich die Anhaltspunkte für eine Gefährdung auch aus einer abstrakten Gefahrenlage ergeben können.

Öffentliche Parkhäuser werden nicht von der Vorschrift erfasst, da es sich bei dem Betreiben eines Parkhauses nicht um die Wahrnehmung einer öffentlichen Aufgabe handelt, sondern, selbst wenn sie von öffentlichen Stellen wahrgenommen wird, im Wettbewerb mit anderen Anbietern erfolgt. Es gelten die datenschutzrechtlichen Vorschriften des Bundesdatenschutzgesetzes für nichtöffentliche Stellen.

Zu Absatz 2

- Der LfD sieht die Informationspflichten in unzulässiger Weise beschränkt.

*Haltung der Landesregierung*

Zum Zeitpunkt der Videoüberwachung bestehen die Pflichten aus Artikel 13 der Verordnung (EU) 2016/679 noch nicht, da die Daten nicht bei bestimmten Personen erhoben werden. Es gilt vielmehr das allgemeine Transparenzgebot, dem mit der Mitteilung der verantwortlichen öffentlichen Stelle Genüge getan ist.

Zu Absatz 6

- LKT/ST halten die Regelung neben der in der Verordnung (EU) 2016/679 ohnehin vorgeschriebenen Einbeziehung des behördlichen Datenschutzbeauftragten für überflüssig. Der DAV BW befürchtet, dass eine Datenschutz-Folgeabschätzung nur rückwirkend vorgenommen wird.

*Haltung der Landesregierung*

Die Regelung konkretisiert die Pflicht der verantwortlichen Stelle, auf jeden Fall den behördlichen Datenschutzbeauftragten zu beteiligen.

qq) Verarbeitung personenbezogener Daten zu künstlerischen und literarischen Zwecken (Artikel 1 § 19)

- Der LfD hält einen über den in Artikel 85 Absatz 2 der Verordnung (EU) 2016/679 hinausgehenden Ausschluss von Bestimmungen der Verordnung (EU) 2016/679 für europarechtswidrig. Insbesondere wird die Einschränkung von Artikel 82 der Verordnung (EU) 2016/679 für unzulässig angesehen. Es drohe ein Vertragsverletzungsverfahren. Dem ZKM erscheint der Verweis auf Artikel 24 der Verordnung (EU) 2016/679 unklar. Die zu treffenden Sicherheitsmaßnahmen seien zu konkretisieren.

*Haltung der Landesregierung*

Das sog. Medienprivileg ist für den öffentlich-rechtlichen Rundfunk unter den Bundesländern abgestimmt. Es soll im Wesentlichen gleichlautend auch für den privaten Rundfunk, die Telemedien und die Presse gelten. Die getroffene Regelung erstreckt dieses Medienprivileg zum vollständigen Schutz der Meinungsfreiheit auch auf die Verarbeitung zu künstlerischen und literarischen Zwecken. Sinn und Zweck des Privilegs ist es, bestimmte grundrechtlich geschützte Tätigkeiten, die darauf angewiesen sind personenbezogene Daten ohne Einwilligung der betroffenen Person zu erheben und zu verarbeiten, von der Anwendung zentraler Vorschriften der Verordnung (EU) 2016/679 zu entbinden, damit sie in der Ausübung ihrer grundrechtlich geschützten Tätigkeit nicht behindert werden.

Ein Verstoß gegen die Verordnung (EU) 2016/679 wird nicht gesehen, da in Bezug auf Artikel 82 der Verordnung (EU) 2016/679 nur eine deklaratorische Regelung getroffen wird, insofern als eine Schadensersatzpflicht nur für die bestehenden Pflichten entstehen kann, also bei unzureichenden Maßnahmen nach Artikel 5 Absatz 1 Buchstabe f, 24 und 32 der Verordnung (EU) 2016/679.

Der Verweis auf Artikel 24 der Verordnung (EU) 2016/679 macht deutlich, dass der für die Datenverarbeitung Verantwortliche seinen Pflichten unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen nachkommen muss. Der für den Verantwortlichen geltende Pflichtenkatalog folgt aus den Vorgaben der Verordnung (EU) 2016/679 einschließlich der aufgrund Artikel 85 der Verordnung (EU) 2016/679 erlassenen nationalen Rechtsvorschriften. Der Verweis auf Artikel 32 der Verordnung (EU) 2016/679 konkretisiert die an die Datensicherheit zu stellenden Anforderungen. Satz 2 stellt im Sinne allgemeiner schadensrechtlicher Prinzipien klar, dass die in Artikel 82 der Verordnung (EU) 2016/679 enthaltenen Regelungen zum Schadensersatz beziehungsweise zu Geldbußen nur bei einer Verletzung der für anwendbar erklärten Pflichten in Betracht kommt, also für unzureichende Maßnahmen nach Artikel 5 Absatz 1 Buchst. f, 24 und 32 der Verordnung (EU) 2016/679. Die zu treffenden Maßnahmen liegen in der Verantwortung der öffentlichen Stelle.

rr) Errichtung (Artikel 1 § 20)

- Der LfD fordert eine Regelung, die die Einbeziehung in den Personalaustausch der Landesverwaltung garantiert sowie die Prüfung, ob eine förmliche Übertragung der Unterschriftsbefugnis erforderlich ist.

*Haltung der Landesregierung*

Die vom LfD vorgeschlagene Änderung ist appellativer Natur und weist keinen gesetzlichen Regelungscharakter auf. Für das Personal anderer oberster Landesbehörden, wie beispielsweise des Rechnungshofes oder der Landtagsverwaltung, ist eine vergleichbare Regelung nicht bekannt.

Wer vonseiten des Arbeitgebers bzw. der Dienststelle die Vertragsurkunde beim Abschluss eines Arbeitsvertrages gemäß § 2 Absatz 1 Tarifvertrag für den Öffentlichen Dienst der Länder (TV-L) unterschreibt, richtet sich grundsätzlich nach den allgemeinen Regelungen des Bürgerlichen Gesetzbuchs (BGB) bzw. den speziell dafür vorgesehenen Regelungen im Gesetz zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679.

Der Vertreter der neu zu schaffenden obersten Landesbehörde ist kraft Absatz 1 die oder der Landesbeauftragte für den Datenschutz. In Absatz 3 ist ausdrücklich geregelt, dass Aufgaben der Personalverwaltung und Personalwirtschaft übertragen werden können. Inwiefern von dem Leiter dieser Behörde weitere Personen zum Abschluss von Arbeitsverträgen im Sinne der §§ 164 ff. BGB bevollmächtigt werden, kann von der oder dem Landesbeauftragten für den Datenschutz in eigener Zuständigkeit bestimmt werden.

ss) Aufgaben und Befugnisse (Artikel 1 § 25)

Zu Absatz 3

- Nach Auffassung der ARGE-HPR sollen auch Interessenvertretungen die Landesbeauftragte für den Datenschutz oder den Landesbeauftragten für den Datenschutz anrufen können.

*Haltung der Landesregierung*

Ein Beschwerderecht steht nur der betroffenen Person zu. Jedoch können sich auch Interessenvertretungen von der Datenschutzaufsichtsbehörde beraten lassen, da sie Teil der Landesverwaltung sind.

Zu Absatz 5

- Die RAK FR, RAK S und RAK TŪ stehen der Aufsichtsbezugnis der oder des Landesbeauftragten für den Datenschutz über die Datenverarbeitung bei Rechtsanwälten ablehnend gegenüber. Sie fordern eine sektorale Datenschutzaufsicht auf Bundesebene für Rechtsanwälte. Auf Landesebene möchten sie in Amtshilfe für die Landesbeauftragte für den Datenschutz oder den Landesbeauftragten für den Datenschutz die Aufsicht wahrnehmen.

*Haltung der Landesregierung*

Die Unabhängigkeit der Datenschutzaufsicht als Kernanliegen der Verordnung (EU) 2016/679 wäre bei dieser Vorgehensweise nicht ausreichend gewährleistet.

- tt) Rundfunkbeauftragte oder Rundfunkbeauftragter für den Datenschutz (Artikel 1 § 27)

Zu Absatz 3 Satz 3

- Der SWR befürchtet einen Eingriff in das Persönlichkeitsrecht des Rundfunkbeauftragten für den Datenschutz, wenn dessen konkretes Gehalt in einer Satzung geregelt und damit veröffentlicht werden müsste.

*Haltung der Landesregierung*

Da nur die Grundsätze der Vergütung anzugeben sind, soll gerade nicht das konkrete Gehalt veröffentlicht werden.

Zu Absatz 4 Sätze 1 und 2

- Der SWR sieht in der Regelung zur Vereinbarkeit der Tätigkeit des Rundfunkbeauftragten für den Datenschutz mit weiteren Aufgaben einen Widerspruch. Damit werde einer im Rahmen der Zusammenarbeit der ARD notwendigen Flexibilität entgegengewirkt.

*Haltung der Landesregierung*

Der Widerspruch wird nicht gesehen. Während Satz 1 sich auf andere Aufgaben innerhalb des SWR und seiner Beteiligungs- und Hilfsunternehmen bezieht, betrifft Satz 2 sonstige Aufgaben außerhalb des SWR und seiner Beteiligungs- und Hilfsunternehmen. Durch diese Formulierung ist nicht ausgeschlossen, dass Tätigkeiten etwa bei einer anderen Landesrundfunkanstalt wahrgenommen werden, sofern diese die Unabhängigkeit nicht gefährden. Die Formulierung entspricht zudem dem Wortlaut des § 16 Absatz 1 Satz 5 und 6 des ZDF-Staatsvertrags neu.

- Der SWR geht davon aus, dass die Amtszeit des amtierenden Rundfunkbeauftragten für den Datenschutz durch die gesetzliche Rege-

lung nicht berührt wird und wünscht diesbezüglich eine Klarstellung im Gesetz oder in der Begründung.

*Haltung der Landesregierung*

Eine gesetzliche Regelung zum Fortbestand der Amtszeit auch unter Geltung der Verordnung (EU) 2016/679 erfolgt nicht. Aufgrund des Grundsatzes der Staatsferne ist es Angelegenheit des SWR über den Fortbestand der Amtszeit zu befinden.

uu) Ordnungswidrigkeiten (Artikel 1 § 28)

- Der LfD sieht eine Sanktionslücke, wenn gegen Behördenmitarbeiter keine Geldbußen verhängt werden können.

*Haltung der Landesregierung*

Nach Auffassung der Landesregierung lässt die Verordnung (EU) 2016/679 keinen Spielraum, auch für Verstöße von Mitarbeitern Bußgelder zu ermöglichen, da Artikel 83 der Verordnung (EU) 2016/679 Bußgelder allein gegen Verantwortliche oder Auftragsverarbeiter vorsieht. Dies ist eine abschließende Regelung.

- LKT/ST fordern eine Klarstellung, inwieweit gegen Kommunen Bußgelder erhoben werden können. Die AOK BW, die RAK FR, RAK S, RAK Tü sowie das StBVW und das VW RA halten die Einschränkung der Bußgeldfreiheit im Hinblick auf öffentliche Stellen, die am Wettbewerb teilnehmen, für bedenklich, da der Bundesgesetzgeber generell die Bußgeldverhängung gegen öffentliche Stellen ausschließt. StBVW sowie VW RA üben auch Kritik, weil staatlichen Stellen (im Wettbewerb) mangelnde Rechtstreue unterstellt werde, wofür es keinen Anlass gebe.

*Haltung der Landesregierung*

An der Regelung wird festgehalten. Der Verweis auf das Bundesdatenschutzgesetz trägt nicht, da nach § 2 Absatz 5 des Bundesdatenschutzgesetzes öffentliche Stellen des Bundes als nichtöffentliche Stellen gelten, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen. Dementsprechend nimmt § 43 Absatz 3 Bundesdatenschutzgesetz nur Behörden und sonstige öffentliche Stellen im Sinne des § 2 Absatz 1 von der Bußgeldverhängung aus. Es besteht also ein Gleichlauf mit dem Bundesrecht. Bei der Teilnahme am Wettbewerb besteht auch für staatliche Stellen kein Grund, besser gestellt zu werden als ihre Mitbewerber.

vv) Strafvorschrift (Artikel 1 § 29)

- Der BWHT sowie der IHK halten es für ausreichend, die Sanktionen auf Bußgelder zu beschränken.

*Haltung der Landesregierung*

Der Vorschlag wird nicht aufgegriffen. Die Verordnung (EU) 2016/679 sieht Bußgelder nur gegen Verantwortliche und Auftragsverarbeiter vor, fordert aber in Artikel 84 zugleich, weitere Sanktionen festzulegen. Die Strafvorschrift trägt dem Rechnung. Sie ist auch nicht unverhältnismäßig, da zu dem objektiven Verstoß der subjek-

tive Tatbestand der Bereicherungs- oder Schädigungsabsicht hinzu kommen muss.

- Die LRK, die PH BW, UK TÜ und UK UL schlagen vor, statt der einzelnen Verarbeitungsschritte den Begriff „verarbeitet“ zu verwenden.

*Haltung der Landesregierung*

Es sollen nicht alle Verarbeitungstätigkeiten erfasst werden. Die unbefugte Erhebung reicht für den Straftatbestand noch nicht aus.

ww) Polizeibehörden und Polizeivollzugsdienst, Justizbehörden, Landesamt für Verfassungsschutz und Vollzug des Landessicherheitsüberprüfungsgesetzes (Artikel 1 § 30)

- Der LfD kritisiert die sprachliche Fassung, da für die Polizeibehörden primär das Polizeigesetz gelte und das Landesdatenschutzgesetz gemäß § 48 Polizeigesetz nur subsidiär Anwendung finde. Entsprechendes gelte für das Landesverfassungsschutzgesetz.

*Haltung der Landesregierung*

Es handelt sich um eine Übergangsregelung. Die materielle Geltung des Datenschutzrechts wird im Verhältnis zur bisherigen Regelung nicht erweitert.

g) Vorgeschlagene Ergänzungen zu Artikel 1

Seitens der Verbände und Institutionen wurden Vorschläge zur Ergänzung von Artikel 1 des Gesetzentwurfs vorgelegt, die, sofern ihnen nicht Rechnung getragen wurde, aus folgenden Gründen nicht berücksichtigt werden.

aa) Zwangsvollstreckung durch den Landesbeauftragten für den Datenschutz

- Der LfD fordert eine Rechtsgrundlage für die Anwendung von Mitteln des Verwaltungszwangs gegenüber Behörden, um die Anforderungen der Verordnung (EU) 2016/679 wirksam durchsetzen zu können.

*Haltung der Landesregierung*

Nach geltender Rechtslage kann gegen Behörden und juristische Personen des öffentlichen Rechts nur vollstreckt werden, soweit dies durch Rechtsvorschriften ausdrücklich gestattet ist (§ 22 des Landesverwaltungsvollstreckungsgesetzes), da aufgrund ihrer Bindung an Gesetz und Recht (Artikel 20 Absatz 3 des Grundgesetzes und Artikel 25 Absatz 2 der Verfassung des Landes Baden-Württemberg) grundsätzlich Rechtstreue erwartet werden kann. Erfüllt eine Behörde oder juristische Person des öffentlichen Rechts eine rechtliche Verpflichtung ausnahmsweise nicht, bietet sich bereits jetzt mit der Einschaltung der Rechts- oder Fachaufsicht ein milderer Mittel, mit dem die Erfüllung der Verpflichtung erreicht werden kann. Andernfalls kann die Erfüllung der Verpflichtung auf gerichtlichem Weg durchgesetzt werden.

Daneben besteht keine europarechtliche Verpflichtung, die geforderte Regelung vorzusehen. Zwar verpflichtet Artikel 58 Absatz 5 der Verordnung (EU) 2016/679 die Mitgliedstaaten, der unabhängigen

Behörde für die Überwachung der Anwendung dieser Verordnung die Befugnis einzuräumen, Verstöße gegen diese Verordnung den Justizbehörden zur Kenntnis zu bringen und gegebenenfalls die Einleitung eines gerichtlichen Verfahrens zu betreiben oder sich sonst daran zu beteiligen. Die Verordnung (EU) 2016/679 verpflichtet die Mitgliedstaaten aber gerade nicht, eine Befugnis einzuräumen, Anweisungen, Anordnungen, Verbote und sonstige Maßnahmen nach Artikel 58 Absatz 2 der Verordnung (EU) 2016/679 mit Mitteln des Verwaltungszwangs durchzusetzen.

bb) Übermittlung personenbezogener Daten an Religionsgemeinschaften

- Die Kirchen fordern im Hinblick auf die bisherige Regelung in § 17 LDSG a. F., dass auch im Gesetzentwurf die Übermittlung personenbezogener Daten an Stellen der öffentlich-rechtlichen Religionsgemeinschaften geregelt wird.

*Haltung der Landesregierung*

Artikel 91 Absatz 1 der Verordnung (EU) 2016/679 lässt zu, dass Kirchen und religiöse Vereinigungen oder Gemeinschaften eigenständige datenschutzrechtliche Regelungen auf eine Verarbeitung anwenden, sofern diese inhaltlich mit dieser Verordnung in Einklang gebracht werden. Die Regelung dient dazu, im Einklang mit Artikel 17 des Vertrags über die Europäische Union und des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) den Status dieser Institutionen in den Mitgliedstaaten zu achten und nicht zu beeinträchtigen. Der Begriff des „Status“ bezeichnet das gesamte Rechtsverhältnis zwischen Mitgliedstaat und den dort vorhandenen Religionsgemeinschaften bzw. Kirchen.

Die Verträge des Landes Baden-Württemberg mit den Kirchen, wie der Evangelische Kirchenvertrag Baden-Württemberg (EvKiVBW) und die Römisch-katholische Kirchenvereinbarung Baden-Württemberg (RkKiVBW) enthalten Regelungen zur Datenübermittlung, vgl. Artikel 16 Absatz 2 und Artikel 27 Absatz 4 EvKiVBW. Die Regelungen zur Übermittlung der Daten gelten auf Basis des Grundsatzes der Parität auch im Verhältnis zu den katholischen Diözesen, obwohl die Römisch-katholische Kirchenvereinbarung Baden-Württemberg keine entsprechende Regelung enthält. Durch die Zustimmung im Gesetz zu dem Evangelischen Kirchenvertrag Baden-Württemberg und zu der Römisch-katholischen Kirchenvereinbarung Baden-Württemberg haben die Verträge Gesetzeskraft. Für eine Regelung der Übermittlung personenbezogener Daten an öffentlich-rechtliche Religionsgemeinschaften besteht daher kein Bedarf.

cc) Vollstreckung von Bußgeldbescheiden der kirchlichen Datenschutzaufsicht

- Die Kirchen schlagen vor, in Artikel 1 des Gesetzentwurfs eine Vorschrift aufzunehmen, die der kirchlichen Datenschutzaufsicht auf Antrag die Möglichkeit gibt, die von ihr verhängten Geldbußen unmittelbar im Verwaltungszwangsverfahren durch staatliche Behörden im Wege der Amts- und Vollstreckungshilfe betreiben zu lassen. Anderenfalls wären die Kirchen auf den Zivilrechtsweg und die nachfolgende Zwangsvollstreckung verwiesen.

*Haltung der Landesregierung*

Aus der religionsverfassungsrechtlichen Rechtsstellung der Religionsgemeinschaften ergibt sich für die Vollstreckung von Rechtsakten der Kirchen durch staatliche Stellen keine unmittelbare Grundlage. Kirchliche und staatliche Behörden sind grundsätzlich nicht gegenseitig zur Amtshilfe verpflichtet. Nach Artikel 140 des Grundgesetzes in Verbindung mit Artikel 137 Absatz 5 der deutschen Verfassung vom 11. August 1919 ist aber eine Kooperation von Staat und Kirche zulässig. Regelungen der Amtshilfe beziehungsweise der Vollstreckungshilfe für die Kirchen bestehen etwa für die Erhebung der Kirchensteuer (Kirchensteuergesetz).

Diese Konzeption lässt sich allerdings nicht unmittelbar auf die Vollstreckung von kirchlichen Bußgeldbescheiden übertragen. Zum einen besteht z. B. im Bereich des Kirchensteuerrechts mit Blick auf die Berechnung der Höhe der Kirchensteuer eine maßgebliche Kontrolle durch die staatlichen Stellen. Ein Bußgeldbescheid unterläge keiner entsprechenden Kontrolle, würde aber auf Grundlage der vorgeschlagenen Regelung unmittelbar durch die staatlichen Stellen vollstreckt. Dies erscheint insbesondere mit Blick auf den Rechtscharakter eines Bußgeldbescheids kritisch. Die Eingriffsqualität des Bußgelds ist weitreichender als die der Rechtsakte, auf die sich die bisherige Kooperation bezieht.

Daneben wäre dem Landesverwaltungsvollstreckungsgesetz und dem Landesverwaltungsverfahrensgesetz eine solche Regelung fremd. Eine entsprechende Regelung müsste auf Ebene des Staatskirchenrechts im Rahmen einer Änderung der Kirchenverträge bzw. -vereinbarungen getroffen werden.

## dd) Einschränkungen der Betroffenenrechte

- Die AK BW, die ING BW sowie die StBK S schlagen vor, auch das in Artikel 18 der Verordnung (EU) 2016/679 normierte Recht auf Einschränkung der Verarbeitung zu beschränken. Zusätzlich soll auch das Widerspruchsrecht gemäß Artikel 21 der Verordnung (EU) 2016/679 beschränkt werden, was auch der BWHT und der IHK fordern.

*Haltung der Landesregierung*

Ein Erfordernis für die vorgeschlagenen Beschränkungen wird nicht gesehen. Bereits das LDSG a. F. sieht in § 4 Absatz 6 ein Widerspruchsrecht vor. Im Übrigen enthalten Artikel 18 und 21 der Verordnung (EU) 2016/679 selbst ausreichende Beschränkungsgründe.

- Die HAW BW schlagen eine Klarstellung vor, dass das Recht auf Datenportabilität in Artikel 20 der Verordnung (EU) 2016/679 im hoheitlichen Bereich der Hochschulen nicht gilt.

*Haltung der Landesregierung*

Einer solchen Klarstellung bedarf es nicht, da sie bereits in Artikel 20 der Verordnung (EU) 2016/679 enthalten ist.

- Der BDFR hält es für notwendig, für die Justiz Einschränkungen der Betroffenenrechte sowie der Informationspflichten vorzunehmen. Hierzu müsse der Geltungsbereich des Landesdatenschutzgesetzes auch auf den justiziellen Bereich erstreckt werden.

*Haltung der Landesregierung*

Das Landesdatenschutzgesetz gilt gemäß § 2 Absatz 5 nicht für die justizielle Tätigkeit der Gerichte. Dies wird auch für sachgerecht gehalten. Vorrangig vor den geforderten landesrechtlichen Regelungen kommen insofern die Ausnahmetatbestände der Verordnung (EU) 2016/679 und des Bundesrechts zur Anwendung, insbesondere des Bundesdatenschutzgesetzes und der gerichtlichen Verfahrensordnungen.

## ee) Datenschutzaufsicht in der Justiz

- Der BDFR regt an, entsprechend Erwägungsgrund 20 der Verordnung (EU) 2016/679 besondere Stellen in der Justiz mit der Aufsicht zu betrauen.

*Haltung der Landesregierung*

In ihrer justiziellen Tätigkeit sind die Gerichte des Landes frei von einer Aufsicht durch die Landesbeauftragte für den Datenschutz oder den Landesbeauftragten für den Datenschutz (vgl. Artikel 55 Absatz 3 der Verordnung [EU] 2016/679). Folgerichtig sieht das Landesdatenschutzgesetz keine Aufsicht vor. Eine spezielle Einrichtung müsste die verfassungsrechtliche Garantie richterlicher Unabhängigkeit wahren.

## ff) Regelungen zum behördlichen Datenschutzbeauftragten

- Der DGB hält die Statuierung einer gesetzlichen Verpflichtung zur Bestellung einer oder eines behördlichen Datenschutzbeauftragten für erforderlich, die eine Stellvertretung einschließen soll. Mindestens eine der beiden Personen sollte dabei in einem Beschäftigungsverhältnis zur öffentlichen Stelle oder Behörde stehen. Auch die HAW BW schlagen eine Konkretisierung der Rechtsstellung des behördlichen Datenschutzbeauftragten einschließlich eines Benachteiligungsverbots vor.

*Haltung der Landesregierung*

Die Regelungen der Verordnung (EU) 2016/679 zum behördlichen Datenschutzbeauftragten sind sehr ausführlich. Eigene abweichende Regelungen sind nicht zulässig, insbesondere kann Artikel 37 Absatz 6 der Verordnung (EU) 2016/679 nicht abbedungen werden. Artikel 38 Absatz 3 der Verordnung (EU) 2016/679 enthält auch ein Benachteiligungsverbot.

## gg) Regelungen zur Auftragsdatenverarbeitung und zu automatisierten Ab-rufverfahren

- Die HAW BW möchten geprüft sehen, ob auch in Zukunft, wie in § 7 Absatz 2 Satz 5 LDSG a. F. vorgesehen, die Fachaufsichtsbehörde für die nachgeordneten Behörden die Vereinbarung über die Auftragsdatenvereinbarung abschließen kann. Ferner sollten Erleichterungen wie bisher in § 7 Absatz 3 LDSG a. F. geprüft werden.

*Haltung der Landesregierung*

Die Regelungen zur Auftragsdatenverarbeitung in der Verordnung (EU) 2016/679 sind abschließend.

- Der LfD vermisst Regelungen zur Zulässigkeit der Einrichtung von automatisierten Abrufverfahren.

*Haltung der Landesregierung*

Die Zulässigkeit von automatisierten Verfahren richtet sich nach den allgemeinen Regelungen zur Zulässigkeit der Verarbeitung personenbezogener Daten. Sonderregelungen sind nicht zielführend. Ggf. ist eine Datenschutz-Folgeabschätzung nach Artikel 35 Absatz 1 der Verordnung (EU) 2016/679 erforderlich.

hh) Beschäftigtendatenschutz

- Der BBW vermisst im Zusammenhang mit den Regelungen zum Beschäftigtendatenschutz eine Regelung zur Verwendung von Daten aus sozialen Medien im Rahmen von Einstellungsverfahren.

*Haltung der Landesregierung*

Mangels einer ausdrücklichen Regelung gilt auch diesbezüglich § 15 Absatz 1 und Absatz 2. Ein vollständiges Verbot wird nicht als sachgerecht angesehen.

ii) Verwendung von Personalaktendaten für die Außerstellung der öffentlichen Stelle

- LKT/ST wünschen sich eine gesetzliche Regelung für die Verarbeitung von Personalaktendaten insbesondere für den Internet-Auftritt.

*Haltung der Landesregierung*

Einer speziellen Regelung bedarf es nicht. Es finden die allgemeinen datenschutzrechtlichen Vorschriften Anwendung, wobei der Vorrang spezialgesetzlicher Vorschriften, insbesondere auch des Informationsfreiheitsrechts, zu beachten ist. Das Landesinformationsfreiheitsgesetz (LIFG) enthält in § 5 besondere Regeln zum Schutz personenbezogener Daten.

jj) Besoldung des Stellvertreters des Landesbeauftragten für den Datenschutz

- Der LfD hält die Einstufung seiner ständigen Vertreterin oder seines ständigen Vertreters in Besoldungsgruppe B 3 für angemessen. Der Aufgaben- und Bedeutungszuwachs der Dienststelle des LfD rechtfertigt diese Bewertung, vor allem auch aus dem Vergleich mit der bisherigen besoldungsrechtlichen Einstufung des ständigen Vertreters eines Abteilungsleiters bei einer obersten Landesbehörde in die Besoldungsgruppe B 3.

*Haltung der Landesregierung*

Eine Anhebung der Besoldung der Stellvertretung des Landesbeauftragten für den Datenschutz wird abgelehnt, da diese zu Verwerfungen im Gefüge der Landesbesoldungsordnung B führen würde. Dies könnte weitere Änderungen nach sich ziehen, die im Hinblick auf einen ausgeglichenen Haushalt vermieden werden sollen.

## h) Artikel 2 bis 16

## aa) Zu Artikel 7 – Änderung der Verordnung der Landesregierung über Zuständigkeiten nach dem Gesetz über Ordnungswidrigkeiten

- Der LfD hält es für notwendig § 4 Absatz 2 Nummer 5 OWiZuVO aufzuheben. Auch Artikel 8 Absatz 3 des Gesetzes zur Änderung des Landesdatenschutzgesetzes und anderer Rechtsvorschriften von 7. Februar 2011 (GBl. S. 43, 46) sei aufzuheben.

*Haltung der Landesregierung*

Für die Änderung der OWiZuVO ist das Innenministerium in Bezug auf die Ordnungswidrigkeiten nach dem Landesmediengesetz nicht zuständig. Da § 40 LDSG a. F. aufgehoben wird, ist die Regelung des Artikels 8 Absatz 3 des Gesetzes zur Änderung des Landesdatenschutzgesetzes und anderer Rechtsvorschriften von 7. Februar 2011 (GBl. S. 43, 46) diesbezüglich hinfällig. Die Rechtsbereinigung ist in einer weiteren Anpassung vorgesehen.

## bb) Zu Artikel 11 – Änderung des Flüchtlingsaufnahmegesetzes

- Der BDK gibt zu bedenken, dass der neu eingefügte Ausschluss der Verarbeitung genetischer Daten, der die Nutzung der Ergebnisse einer molekulargenetischen Analyse vollständig verhindere, dazu führen könne, dass eine eindeutige Identifizierung nicht möglich sei. Dies sei dann zu befürchten, wenn biometrische Daten (z. B. Fingerabdruck) nicht zur Verfügung stehen.

*Haltung der Landesregierung*

Die Einfügung dieser Passage wurde vorgenommen, da durch den künftigen Verweis in § 16 Absatz 1 Flüchtlingsaufnahmegesetz (FlüAG) auf Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 auch die Verarbeitung von genetischen Daten durch die Aufnahmebehörden erfasst würde. Gemäß Artikel 4 Nummer 13 der Verordnung (EU) 2016/679 sind genetische Daten personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden.

In der Begründung ist ausgeführt, dass die Verarbeitung genetischer Daten für die Aufgabenwahrnehmung der Aufnahmebehörden nicht erforderlich ist. Dies gilt auch unter Berücksichtigung der Ausführungen des Bundes Deutscher Kriminalbeamter. Diese beziehen sich auf die effektive Wahrnehmung polizeilicher Aufgaben durch die Verarbeitung genetischer Daten. Das Flüchtlingsaufnahmegesetz regelt in § 16 jedoch lediglich die Datenverarbeitung durch die Aufnahmebehörden. Rechtsgrundlagen, welche die Polizei ggf. zur Verarbeitung genetischer Daten ermächtigen, werden davon nicht berührt.

## cc) Zu Artikel 14 – Änderung des Landesglücksspielgesetzes

- Der IHK gibt zu bedenken, dass die „Überprüfung“ der Videoüberwachung dem Datenschutzbeauftragten eine größere Pflicht auferlegt, als die Datenschutz-Folgeabschätzung gemäß Artikel 35 Absatz 2 der Verordnung (EU) 2016/679 vorsieht.

*Haltung der Landesregierung*

Der Datenschutzbeauftragte hat das Konzept für die Videoüberwachung vor dessen Umsetzung zu überprüfen. Anschließend ist es durch die Spielbank als verantwortliche Stelle freizugeben. Somit verbleibt die letztliche Verantwortung bei der Spielbank. Hierin liegt kein Verstoß gegen Artikel 35 Absatz 2 der Verordnung (EU) 2016/679.

Daneben hat der Verantwortliche nach Artikel 38 der Verordnung (EU) 2016/679 sicherzustellen, dass der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird. Die Aufgabenerfüllung sowie die Position des Datenschutzbeauftragten wird durch die Regelung in § 32 Absatz 6 Landesglücksspielgesetz (LGlüG) erleichtert, da er sich auf diese Vorschrift berufen kann, um speziell beim für alle Besucher der Spielbanken (grundrechts-)relevanten Bereich der Videoüberwachung Zugang zu sämtlichen Daten zu erhalten. Im Übrigen entspricht die Regelung weitgehend dem bisherigen § 32 Absatz 7, sodass materiell-rechtlich keine Änderung erfolgt.

dd) Zu Artikel 15 – Änderung des Abschiebungshaftvollzugsgesetzes Baden-Württemberg

Zu Nummern 4 und 5

- Die Liga BW hat vorgetragen, dass es sich bei der Inhaftierung um einen schweren Grundrechtseingriff handele und eine 24-Stunden-Überwachung gerade von Krankenzimmern oder sonstigen Räumen unverhältnismäßig sei. In der Stellungnahme wird ausgeführt, dass weder die Erforderlichkeit dieser Maßnahme begründet noch dargelegt worden sei, ob mildere Mittel zur Verfügung stünden. Die Erforderlichkeit wird insbesondere auch in Bezug auf suizidgefährdete Personen und Personen mit psychischen Erkrankungen in Frage gestellt, da diese gar nicht in Haft genommen werden dürften.

*Haltung der Landesregierung*

Dem ist entgegenzuhalten, dass sowohl in § 10 Absatz 4 als auch in § 10a Absatz 1 der Zweck der Datenerhebung bzw. -speicherung explizit genannt ist, und zwar in Gestalt der „Aufrechterhaltung der Sicherheit oder Ordnung der Einrichtung oder zur Verhinderung oder Verfolgung von Straftaten oder Ordnungswidrigkeiten, durch welche die Sicherheit oder Ordnung der Einrichtung gefährdet ist.“ Der Schutz dieser Rechtsgüter ist ein legitimes Ziel, welches Einschränkungen des Persönlichkeitsrechts der inhaftierten Personen zu rechtfertigen vermag. Dies gilt umso mehr, als in einer Abschiebehafteinrichtung Gefahren für die öffentliche Sicherheit nicht auszuschließen, ja sogar wahrscheinlich sind. Die Aufrechterhaltung der öffentlichen Sicherheit sowie die Verhinderung und Aufklärung kommt dabei auch gerade den inhaftierten Personen selbst zugute. Ein milderes Mittel, welches im gleichen Maße geeignet wäre, die Ziele zu erreichen, ist nicht ersichtlich. Die Überwachung durch die Bereitstellung von mehr Personal in den entsprechenden Räumlichkeiten würde in ähnlicher Weise in die schutzwürdigen Belange der Inhaftierten eingreifen. Zwar würde in diesem Falle die – im Regelfall vorübergehende – Speicherung personenbezogener Daten entfallen. Allerdings wäre – abgesehen von unververtretbaren Personalkosten – dadurch die Verwertbarkeit für die Aufklärung von Straftaten nicht in vergleichbarem Maße sichergestellt.

Soweit die Erforderlichkeit im Hinblick auf psychisch kranke bzw. suizidgefährdete Personen angezweifelt wird, ist hierzu auszuführen, dass die genannten Erkrankungen nicht zwangsläufig die Haftunfähigkeit nach sich ziehen müssen.

Die Notwendigkeit, einen Richtervorbehalt für die Videoüberwachung vorzusehen, ist nicht ersichtlich.

Zu Nummer 4 Buchstabe a

- Die Speicherdauer von einer Woche ist nach Auffassung des LfD unverhältnismäßig. Dies gelte insbesondere vor dem Hintergrund, dass z. B. bei der Überwachung medizinischer Bettenstationen regelmäßig sensible Daten erhoben würden. Er schlägt vor, die Speicherdauer auf 48 Stunden zu reduzieren.

#### *Haltung der Landesregierung*

Gegen die Verkürzung der Speicherfrist spricht, dass die Speicherung überhaupt nur erfolgen darf, wenn dies zum Zweck der Aufrechterhaltung der Sicherheit oder Ordnung oder zur Verhinderung oder Verfolgung von Straftaten oder Ordnungswidrigkeiten, durch welche die Sicherheit oder Ordnung der Einrichtung gefährdet wird, erforderlich ist und zur Erreichung dieser Zielsetzung ein gewisser Zeitraum zur Sichtung der Materialien zugestanden werden muss.

Hierbei ist insbesondere zu berücksichtigen, dass der Kreis der Zugriffsberechtigten gerade im Interesse des Datenschutzes auf besonders ausgewählte und datenschutzrechtlich sensibilisierte Bedienstete beschränkt ist. Wollte man sicherstellen, dass zu jeder Zeit binnen 48 Stunden unter Berücksichtigung des permanenten Personalwechsels durch den Schicht- und Wechseldienst, Urlaubs- und sonstige Abwesenheitszeiten Zugriff auf die Aufzeichnungen gewährleistet ist, müsste man den Kreis der Zugriffsberechtigten erheblich erweitern. Hinzu kommt, dass sich Untergebrachte ggf. erst ein paar Tage nach einem (nicht allgemein bekannt gewordenen) Vorfall bei der Einrichtungsleitung oder Dritten melden und beschweren und zugunsten der Untergebrachten dann auf objektivierbare Beweismittel zurückgegriffen werden muss (z. B. in Fällen von Nötigung, Erpressung oder Provokation).

Daneben ist bei Straftaten den Ermittlungsbehörden ein gewisses Zeitfenster einzuräumen, in welchem diese die Beschlagnahme der Videoaufzeichnungen erwirken können.

Dem Anliegen wird aber insoweit entgegengekommen, als die Speicherfrist auf drei Werktagen verkürzt wird.

Zu Nummer 5

- Der LfD gibt zu bedenken, dass bestimmte Bereiche wie z. B. Sozialräume, Toiletten oder Duschen keiner Vollüberwachung unterliegen dürften. Außerdem sei darauf zu achten, dass keinesfalls Privatanwesen Dritter erfasst werden dürften und auch die Beobachtung des öffentlichen Raums auf einen eng begrenzten Bereich außerhalb des Einrichtungsgeländes zu beschränken sei.

#### *Haltung der Landesregierung*

Diesen Anregungen wird insoweit Rechnung getragen, als bei der konkreten Umsetzung sichergestellt wird, dass sensible Bereiche wie

z. B. Toiletten oder Duschen von einer Überwachung ausgenommen werden. Im Hinblick auf Sozialräume ist jedoch festzuhalten, dass es gerade in solchen gemeinschaftlich genutzten Räumen (z. B. Internet-Raum, Lounge, Bibliothek, Fitnessraum, Fernseh-/Speisezimmer, Wohngruppenküche etc.) eher zu Spannungen oder gar körperlichen Übergriffen kommt. Die Abschiebungshafteinrichtung ist darauf ausgelegt, den Untergebrachten tagsüber eine möglichst große Bewegungsfreiheit einzuräumen. Aufgrund der Gebäudestruktur und aus Gründen eines sparsamen Personaleinsatzes können dabei weite Bereiche nicht durch die persönliche Anwesenheit von Personal überwacht werden.

Aufgabe der Abschiebungshafteinrichtung ist unter anderem jedoch auch der Schutz der Untergebrachten, auch vor Übergriffen durch andere Untergebrachte. Schon allein aufgrund des Zusammentreffens verschiedener Nationalitäten und Religionen bleiben Spannungen unter den Untergebrachten nicht aus. Die Videoüberwachung dient daher in erster Linie dem Schutz jedes einzelnen Untergebrachten sowie dem Ziel, allen Untergebrachten in dem Areal einen möglichst großen ganztägigen und zeitlich nicht limitierten Freiraum zur freien Bewegung zu verschaffen. Eine Videoüberwachung ist daher gerade auch bei gemeinschaftlich genutzten Räumlichkeiten und Flächen geboten. Ohne Videoüberwachung müsste die Bewegungsfreiheit auf überschaubare Gruppen und Bereiche beschränkt, zeitlich limitiert und den verfügbaren Personalkapazitäten angepasst werden, d. h. die jetzige Bewegungsfreiheit müsste um weit mehr als 50 % reduziert werden.

Die Notwendigkeit der Überwachung in bestimmten Räumlichkeiten der vorübergehenden Unterbringung ergibt sich aus dem Schutzzweck. Bei akuter Selbstbeschädigungsabsicht ist die Videoüberwachung ein milderes Eingriffsmittel gegenüber der ständigen unmittelbaren Anwesenheit von zwei Bediensteten. Dabei ist sichergestellt, dass jederzeit unmittelbar eingegriffen werden kann, wenn ein in einer Ausnahmesituation befindlicher Untergebrachter Hand an sich legt; zum anderen wirkt die fehlende ggf. über Stunden dauernde unmittelbare Anwesenheit von Personal beruhigend auf den Betroffenen.

Ohne Videoüberwachung wäre, wenn man von einer ständigen, durchgehenden unmittelbaren Anwesenheit von Personal absieht, der Untergebrachte alle paar Minuten aufzusuchen und zu stören, was insbesondere in den Ruhezeiten als menschenunwürdige Behandlung anzusehen wäre.

Die Videoüberwachung bestimmter Räumlichkeiten der vorübergehenden Unterbringung dient somit einer menschenwürdigen Behandlung und ist als milderes Mittel gegenüber einer sonstigen unmittelbaren personengestützten Überwachung anzusehen.

Nicht vorgesehen ist eine Videoüberwachung der Zimmer der Untergebrachten, der Sanitärräume sowie von Anwaltsbesuchen und Gesprächen mit Geistlichen.

i) Artikel 17 – Änderung des Landesbeamtengesetzes

aa) Allgemeines

- Der BBW hält es für sinnvoll, in den Regelungen des Landesbeamtengesetzes zum Personalaktendatenrecht ausdrücklich darauf hinzuweisen, wenn die Regelungen der Verordnung (EU) 2016/679 abschließend sind.

*Haltung der Landesregierung*

Die Landesregierung kann diesen Vorschlag im Gesetzentwurf nicht berücksichtigen. Inwieweit die Regelungen der Verordnung (EU) 2016/679 abschließend sind oder an die nationalen Gesetzgeber adressierte Regelungsaufträge und -optionen bestehen, von denen der Landesgesetzgeber Gebrauch gemacht hat, ist jeweils bezogen auf die konkrete Regelung durch Auslegung der Verordnung (EU) 2016/679 sowie der bereichsspezifischen Regelungen zur Datenverarbeitung zu ermitteln.

## bb) Zu Nummer 2

- Der BDFR kritisiert, dass die Norm, welche bisher die „Erhebung“ von Personalaktendaten regelte, auf den Vorgang der „Verarbeitung“ ausgeweitet und damit in ihrem Regelungsinhalt erweitert würde, ohne dass ein sachlicher Grund hierfür ersichtlich sei.

*Haltung der Landesregierung*

Eine Änderung kann nicht erfolgen. Die Anpassung erfolgt auf Grundlage des umfassenden Verarbeitungsbegriffs der Verordnung (EU) 2016/679. Nach Artikel 4 Nummer 2 der Verordnung (EU) 2016/679 ist die „Erhebung“ nur ein Teilschritt des weit gefassten Oberbegriffs der „Verarbeitung“. Eine inhaltliche Ausweitung ist damit nicht beabsichtigt. Als Folge wurden Vorschriften, auf deren Grundlage schon bisher weitere Schritte der Verarbeitung zulässig waren (§ 84 Absatz 1 a.F.), gestrichen. Dies ist in der Begründung klargestellt.

- Der DGB fordert zu § 83 Absatz 1 Satz 1 die alte Formulierung, wonach eine Verarbeitung von Personalaktendaten „nur“ unter den in der Regelung genannten Voraussetzungen möglich war, wieder aufzunehmen, um sicherzustellen, dass der Dienstherr eine Verarbeitung auch nur aus den dort genannten Zwecken vornehme. Die bisherige Fassung von § 83 schließe unmittelbar an die Formulierung in § 50 des Beamtenstatusgesetzes an. Der BBW regt an, das Wort „nur“ in § 83 Absatz 1 Satz 1 beizubehalten und Satz 1 um den klarstellenden Zusatz „, es sei denn, für bestimmte Verarbeitungssituationen ergibt sich eine Ermächtigung zur Datenverarbeitung direkt aus der Verordnung (EU) 2016/679.“ zu ergänzen.

*Haltung der Landesregierung*

Diese Forderungen des DGB und des BBW sollen im Gesetzentwurf nicht berücksichtigt werden. Das Wort „nur“ ist nicht wieder aufzunehmen, da sich für bestimmte Verarbeitungssituationen eine Ermächtigung zur Datenverarbeitung direkt aus der Verordnung (EU) 2016/679 ergeben kann. Dementsprechend hat der Bund in seinem aktuellen Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 auch eine entsprechende Anpassung von § 50 des Beamtenstatusgesetzes angekündigt. Eine ausdrückliche Klarstellung des Verhältnisses der Verordnung (EU) 2016/679 zu den bereichsspezifischen Regelungen zur Datenverarbeitung im Gesetzestext über den erläuternden Hinweis in der Begründung hinaus erscheint nicht angezeigt.

Die vom BBW vorgeschlagene Formulierung gerät in Konflikt mit dem Anwendungsvorrang der Verordnung (EU) 2016/679, da sie letztendlich auf eine Regelung hinausliefe, welche die Verordnung (EU) 2016/679 ausdrücklich für anwendbar erklärt.

cc) Zu Nummer 3

- Die ARGE-HPR kritisiert, dass mit § 84 eine generelle Einführung von automatisierten Entscheidungen ermöglicht würde. Sie fordert eine datenschutzrechtliche Vorabkontrolle und die Einbeziehung der zuständigen Personalvertretung vor Einführung eines jeden einzelnen automatisierten Entscheidungsverfahrens sowie eine erneute datenschutz- und personalvertretungsrechtliche Kontrolle nach der Einführung. Außerdem fehle eine Evaluation des Erfolgs der automatisierten Vorgehensweise. Der DGB verlangt, dass unter der Beteiligung des jeweils zuständigen Personalrats vorab bestimmt werden müsse, bei welchen beamtenrechtlichen Entscheidungen die automatisierte Verarbeitung personenbezogener Daten angewendet werden dürfe und bei welcher nicht.

*Haltung der Landesregierung*

Diese Forderung soll im Gesetzentwurf nicht berücksichtigt werden. Mit § 84 wird zunächst nur eine Ermächtigungsgrundlage für die Einführung einer automatisierten Bearbeitung geschaffen. Vor der Einführung eines konkreten Verfahrens werden die im Rahmen der datenschutz- und personalvertretungsrechtlichen Bestimmungen notwendigen Prüfungen und Beteiligungen durchgeführt werden. Eine Evaluation ist von sich aus vorgesehen und bedarf keiner zusätzlichen Regelung in § 84. Strittige Fälle bzw. Fälle, die für eine automatisierte Bearbeitung nicht geeignet sind, werden ausgesteuert und einer manuellen Bearbeitung zugeleitet.

dd) Zu Nummer 4

- Der LfD weist darauf hin, dass auch die Übermittlung eine Form der Verarbeitung darstelle, § 85 müsse insgesamt an den einheitlichen Verarbeitungsbegriff angepasst werden. Weiterhin sei in der Übermittlungsvorschrift zwischen „Empfängern“ im Sinne des Artikels 4 Nummer 9 und „Dritten“ im Sinne des Artikels 4 Nummer 10 der Verordnung (EU) 2016/679 zu unterscheiden.

*Haltung der Landesregierung*

Dieser Forderung soll nicht entsprochen werden. § 85 regelt einen Teilschritt der Verarbeitung und ist im Vergleich zu § 83 LBG als speziellere Vorschrift anzusehen. Die Nennung von Einzelschritten wird für zulässig erachtet, soweit durch die Verwendung der durch Artikel 4 Nummer 2 der Verordnung (EU) 2016/679 definierten Begrifflichkeiten klar wird, dass es sich um einen Teilschritt der Verarbeitung handelt.

Weiterhin kann der Begriff der „Übermittlung“ sowie des „Dritten“ in § 85 aufrechterhalten werden. Nach dem Verständnis der Verordnung (EU) 2016/679 ist Übermittlung die Weitergabe von Daten an eine Stelle außerhalb des Verantwortlichen. Dieses Verständnis liegt auch § 85 zugrunde. „Dritter“ im Sinne von § 85 ist „Dritter“ im Sinne des Artikels 4 Nummer 10 der Verordnung (EU) 2016/679. Eine von der Verordnung (EU) 2016/679 abweichende (unzulässige) Eigendefinition liegt § 85 nicht zugrunde.

## ee) Zu Nummer 6

- Der LfD ist der Auffassung, dass die Rechte und Pflichten betreffend die Löschung nur unter den Voraussetzungen des Artikels 23 der Verordnung (EU) 2016/679 beschränkt werden können. Artikel 17 der Verordnung (EU) 2016/679 enthalte keine Öffnungsklausel. Die Anforderungen, die Artikel 23 der Verordnung (EU) 2016/679 an eine wirksame Beschränkung der Betroffenenrechte stelle, seien nicht erfüllt.

*Haltung der Landesregierung*

Dieser Einwand kann im Gesetzentwurf nicht berücksichtigt werden. Bei den Lösungsfristen nach § 86 handelt es sich um spezifische Vorschriften auf Grundlage von Artikel 88 der Verordnung (EU) 2016/679. Da insoweit keine Beschränkungen des Rechts auf Löschung vorliegen, sind die Regelungen auch nicht an Artikel 23 der Verordnung (EU) 2016/679 zu messen.

## ff) Zu Nummer 7

- Der BBW fordert, dass in § 87 Absatz 3 Satz 2 aus Gründen der Klarheit ein Zusatz ergänzt wird, wonach Abschriften, Kopien oder Ausdrucke auf Verlangen den Beamtinnen und Beamten auch zu überlassen sind. Nach einer Forderung des HPR GHWRGS soll zudem ausgeschlossen werden, dass von Beschäftigten für Auszüge aus ihren Personalaktendaten Gebühren verlangt werden können.

*Haltung der Landesregierung*

Die Landesregierung hält die vorgeschlagene Ergänzung für nicht erforderlich. Dass die Beamtin oder der Beamte Abschriften, Kopien oder Ausdrucke auch ausgehändigt erhält, ergibt sich aus Sinn und Zweck der Regelung und kommt zudem in der Begründung klar zum Ausdruck („Erhalt einer Kopie“). Insofern wurde die Regelung auch inhaltlich nicht geändert.

Der Forderung des HPR GHWRGS nach der Gebührenfreiheit von Auszügen aus den Personalaktendaten, kann nicht entsprochen werden. Beamtinnen und Beamten ist nach Artikel 15 Absatz 3 Satz 1 der Verordnung (EU) 2016/679 unentgeltlich eine Kopie der gespeicherten Personalaktendaten zur Verfügung zu stellen. Die Verordnung (EU) 2016/679 sieht in Artikel 15 Absatz 3 Satz 2 jedoch vor, dass für alle weiteren Kopien ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten verlangt werden kann. Dies erscheint auch erforderlich, um denkbaren Missbrauchsfällen begegnen bzw. einen funktionierenden Dienstbetrieb sicherstellen zu können. Kostenerstattungen sollen daher nicht generell ausgeschlossen werden (vgl. Artikel 12 Absatz 5 der Verordnung (EU) 2016/679). Ein genereller Ausschluss von Gebühren für Auszüge aus den Personalaktendaten wäre zudem eine Überschreitung des Schutzniveaus des Artikels 15 der Verordnung (EU) 2016/679. Eine derartige Regelung wäre mit europarechtlichen Risiken verbunden.

## j) Zu Artikel 19 – Änderung des Landespersonalvertretungsgesetzes

## Zu Nummer 3

- Der BBW hält Änderungen am Landespersonalvertretungsgesetz grundsätzlich, ausgenommen sprachliche Anpassungen, für nicht erforderlich und stellt fest, dass das Beteiligungsrecht durch einen Wechsel von einem Widerspruchsrecht hin zu einem Zustimmungsvorbehalt eingeschränkt werden soll.

*Haltung der Landesregierung*

Durch diese Feststellung soll der Gesetzentwurf keine Änderung erfahren. Beschäftigte, die eine Beteiligung des Personalrats vor der Gewährung von Unterstützungen, Vorschüssen, Darlehen und entsprechenden sozialen Zuwendungen an sie verhindern wollen, zum Beispiel, weil der Personalrat dadurch sehr persönliche Verhältnisse von Beschäftigten und deren Familienangehörigen erfahren könnte, sollen künftig nicht mehr nur auf ein Widerspruchsrecht angewiesen sein, das sie aktiv ausüben müssen. Vielmehr soll die Beteiligung des Personalrats nur erfolgen, wenn die Beschäftigten dies ausdrücklich beantragen, wobei sie auf ihr Antragsrecht hinzuweisen sind. Hierdurch wird das Recht der Beschäftigten auf informationelle Selbstbestimmung in derart sensiblen Angelegenheiten gegenüber dem Personalrat gestärkt, wie dies in anderen Fällen, etwa der Kündigung einer dienstlich gestellten Wohnung bereits der Fall ist. Dem ist immanent, dass die Personalratsbefugnisse datenschutzrechtskonform entsprechend hinter den berechtigten Interessen der Betroffenen zurückstehen müssen. Die Gesamtheit der Beteiligungsrechte der Personalräte wird hierdurch jedoch nicht wesentlich beeinträchtigt.

## k) Sonstige Gesetze

- Die DRV BW regt an, § 16 des Landeskrebsregistergesetzes an den Verarbeitungsbegriff der Verordnung (EU) 2016/679 anzupassen.

*Haltung der Landesregierung*

Die Anpassung des bereichsspezifischen Datenschutzrechts an die Verordnung (EU) 2016/679 bleibt, sofern andere Ressorts als das Innenressort betroffen sind, eigenen Gesetzgebungsverfahren vorbehalten.

*B. Einzelbegründung*

## Zu Artikel 1 – Landesdatenschutzgesetz (LDSG)

## Zu Abschnitt 1 – Allgemeine Bestimmungen

## Zu § 1 – Zweck des Gesetzes

Da die Verordnung (EU) 2016/679 unmittelbar gilt, kann das Landesdatenschutzgesetz ab Geltung der Verordnung (EU) 2016/679 nur noch im Rahmen der Öffnungsklauseln der Verordnung (EU) 2016/679 ergänzende Regelungen treffen. Diese können, sofern durch die Verordnung (EU) 2016/679 zugelassen, auch Ausnahmen von den Pflichten der Verordnung (EU) 2016/679 regeln. Wiederholende Regelungen der Verordnung (EU) 2016/679 sind außer in Ausnahmefällen nicht vorgesehen, da der Europäische Gerichtshof im Hinblick auf unmittelbar

geltende Verordnungen ein Wiederholungsverbot statuiert hat. Die Verordnung (EU) 2016/679 enthält auch Regelungsaufträge und -optionen, die in diesem Gesetz ebenfalls geregelt sind.

Darüber hinaus enthält das Landesdatenschutzgesetz auch Regelungen für Datenverarbeitungen, die nicht von der Verordnung (EU) 2016/679 und nicht von bereichsspezifischen Regelungen erfasst sind.

#### Zu § 2 – Anwendungsbereich

##### Zu Absatz 1

Der Begriff der öffentlichen Stelle wird in Satz 1 legal definiert. Sie ist Verantwortlicher nach Artikel 4 Nummer 7 der Verordnung (EU) 2016/679, soweit nichts anderes bestimmt ist.

Normadressaten des Landesdatenschutzgesetzes sind weiterhin alle öffentlichen Stellen, das sind die unmittelbare Verwaltung (Landesverwaltung), die Kommunalverwaltung (Gemeinden, Städte und Landkreise) und die mittelbare Verwaltung (sonstige Selbstverwaltungsträger). Das Landesdatenschutzgesetz gilt für die gesamte Tätigkeit der Normadressaten bei der Ausführung von Bundes- oder Landesrecht. Ausgenommen ist lediglich die datenverarbeitende Tätigkeit der Polizeibehörden, des Polizeivollzugsdiensts, der Gerichte und Staatsanwaltschaften zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten und Ordnungswidrigkeiten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit. Diese Tätigkeit unterfällt dem Anwendungsbereich der Richtlinie (EU) 2016/680, die mit gesonderten Gesetzen in nationales Recht umgesetzt wird. Wegen der Eingliederung der allgemeinen Polizeibehörden in die allgemeine Verwaltung lässt sich eine einheitliche Regelung für die Verwaltung, unabhängig davon, welche Rechtsgrundlage sie anwendet, nicht aufstellen. Der Bereich der Gefahrenabwehr durch die allgemeinen Polizeibehörden (§ 62 Polizeigesetz [PolG] in der Fassung vom 13. Januar 1992) wird dem Anwendungsbereich der Richtlinie (EU) 2016/680 zugerechnet und wird daher nicht von diesem Gesetz erfasst. Selbst wenn bei polizeilichem Handeln zur Gefahrenabwehr nicht bereits von vornherein die Verhütung von Straftaten als Zweck oder Ergebnis feststeht, besteht nahezu immer zumindest die Möglichkeit, dass die Gefahrenlage zu einer Straftat führen kann. Dies gilt aber nur, soweit das allgemeine Polizeirecht angewendet wird.

Eine eigenständige Regelung wird in Bezug auf die Datenverarbeitung personenbezogener Daten für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Ordnungswidrigkeiten, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, getroffen. Zwar erfasst der Straftatenbegriff in Artikel 2 Absatz 2 Buchstabe d der Verordnung (EU) 2016/679 nach der Auslegung des Europäischen Gerichtshofs auch die Ordnungswidrigkeiten. Dennoch ist ein enges Verständnis in Bezug auf ordnungsrechtliche Tätigkeiten angezeigt, da im Grundsatz sämtliche Verarbeitungsvorgänge in der Verwaltung, mit Ausnahme der polizeilichen Tätigkeit, der Verordnung (EU) 2016/679 unterfallen sollen. So sind Datenverarbeitungen zur Abwehr von Gefahren durch die allgemeinen Sicherheitsbehörden, soweit sie nicht das Polizeirecht anwenden, ebenso wie durch für spezielle Fachbereiche zuständige Behörden grundsätzlich nach den Bestimmungen der Verordnung (EU) 2016/679 zu beurteilen. Erst wenn ein verwaltungsrechtliches Verfahren formal in ein konkretes Ordnungswidrigkeitenverfahren übergeht, finden die zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Regelungen Anwendung.

Die Datenverarbeitung durch das Landesamt für Verfassungsschutz im Rahmen der Erfüllung seiner Aufgaben nach § 3 des Landesverfassungsschutzgesetzes wird ausschließlich bereichsspezifisch im Landesverfassungsschutzgesetz gere-

gelt, wobei hier teilweise auch Verweisungen auf das Landesdatenschutzgesetz enthalten sein können. Desgleichen wird die Datenverarbeitung für die Sicherheitsüberprüfung im Landessicherheitsüberprüfungsgesetz geregelt. Auch hier ist eine Verweisung auf das Landesverfassungsschutzgesetz und, soweit dieses keine Regelungen trifft, auf das Landesdatenschutzgesetz möglich. Der Landesgesetzgeber ist hierzu befugt, da beide Bereiche nicht in den Anwendungsbereich des Unionsrechts fallen und daher gemäß Artikel 2 Absatz 2 Buchstabe a nicht der Verordnung (EU) 2016/679 unterliegen. § 30 dieses Gesetzes ordnet als Übergangsregelung, bis die Gesetze zur Umsetzung der Richtlinie (EU) 2016/680 in Kraft treten, die Fortdauer des bisherigen Landesdatenschutzgesetzes im bisherigen Umfang an.

#### Zu Absatz 2

Wie bisher gelten unter bestimmten Voraussetzungen auch privatrechtlich organisierte staatliche und kommunale Beteiligungsgesellschaften als öffentliche Stellen gemäß Absatz 1.

#### Zu Absatz 3

Spezifische Rechtsvorschriften des Bundes und des Landes gehen den allgemeinen Regelungen des Landesdatenschutzgesetzes grundsätzlich vor. Dies gilt auch für durch verbindliche Staatsverträge getroffene Regelungen (z. B. Rundfunkbeitragsstaatsvertrag). Im Übrigen kommt dem Landesdatenschutzgesetz lückenfüllende Auffangfunktion zu, soweit keine oder keine vollständige bereichsspezifische Regelung vorliegt.

Bedeutung kommt der Subsidiarität des Landesdatenschutzgesetzes vor allem im Hinblick auf die in Abschnitt 3 getroffenen Einschränkungen der Betroffenenrechte zu. Auf diese Regelungen kann als Auffangregelung zurückgegriffen werden, sofern im jeweiligen Fachrecht keine tatbestandskongruente Regelung besteht.

Der Vorrang des Landesdatenschutzgesetzes bei der Sachverhaltsermittlung bezieht sich auf die §§ 24, 26 des Landesverwaltungsverfahrensgesetzes (LVwVfG), die der Behörde weitreichende Befugnisse einräumen. In Bezug auf personenbezogene Daten hat das Landesdatenschutzgesetz Vorrang. Dies betrifft vor allem die Datenerhebung gemäß § 4. Die Verordnung (EU) 2016/679 geht dem Landesverwaltungsverfahrensgesetz vor.

#### Zu Absatz 4

Der sachliche Anwendungsbereich der Verordnung (EU) 2016/679 ist gemäß Artikel 2 Absatz 2 der Verordnung (EU) 2016/679 beschränkt. Die angeordnete entsprechende Anwendung stellt sicher, dass auch für die nicht unter die Verordnung (EU) 2016/679 oder die Richtlinie (EU) 2016/680 fallenden Datenverarbeitungen öffentlicher Stellen ein datenschutzrechtliches Vollregime angeboten wird, sofern keine besonderen Rechtsvorschriften vorhanden sind.

Auch für die nicht-automatisierte Datenverarbeitung wird hiermit die Geltung der Verordnung (EU) 2016/679 angeordnet. Zugleich wird auf die Pflicht zur Führung eines Verzeichnisses (Artikel 30 der Verordnung (EU) 2016/679), zur Datenschutz-Folgeabschätzung (Artikel 35 der Verordnung (EU) 2016/679) sowie zur vorherigen Konsultation (Artikel 36 der Verordnung (EU) 2016/679) verzichtet, da hier ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen nicht zu besorgen ist.

Der verfassungsrechtlich garantierten Unabhängigkeit des Rechnungshofs und der staatlichen Rechnungsprüfungsämter in Bezug auf ihre Prüfungstätigkeiten wird wie bisher in § 2 Absatz 3 LDSG a. F. Rechnung getragen.

## Zu Absatz 5

Der Landtag, seine Gremien, seine Mitglieder und Fraktionen unterliegen dem Landesdatenschutzgesetz nur im Bereich der Verwaltungsangelegenheiten (z. B. Personalverwaltung, Besucherregelungen, Abgeordnetenentschädigung). Dies gilt auch für die Gerichte, sofern sie bezüglich ihrer Verwaltungstätigkeit nach der Verordnung (EU) 2016/679 zu handeln haben. Damit ist die Verwaltungstätigkeit der Gerichte in Strafsachen ausgenommen, sofern sie Strafverfolgungs- oder Strafvollstreckungszwecke verfolgt. Im Bereich der justiziellen Tätigkeit haben die prozessualen Vorschriften Vorrang.

## Zu Absatz 6

Die Vorschrift wurde ihrem Sinngehalt nach unverändert aus dem bisherigen Landesdatenschutzgesetz übernommen. Aus Gründen der Wettbewerbsgleichheit werden am Wettbewerb teilnehmende öffentliche Stellen denselben Regeln wie ihre privatrechtliche Konkurrenz unterworfen. Die Vorschrift gilt auch für öffentlich-rechtliche Kreditinstitute sowie für ihre Zusammenschlüsse und Verbände, soweit diese am Wettbewerb teilnehmen.

Teilnahme am Wettbewerb steht im Gegensatz zum hoheitlichen Handeln. Entscheidend ist, dass die öffentlichen Stellen Leistungen erbringen, die entsprechend auch von privaten Unternehmen erbracht werden (können).

## Zu Absatz 7

Die Ausübung des Begnadigungsrechts unterliegt nicht dem Anwendungsbereich des Unionsrechts und damit auch nicht der Geltung der Verordnung (EU) 2016/679. Sie soll keinen besonderen datenschutzrechtlichen Anforderungen unterworfen werden.

## Zu § 3 – Sicherstellung des Datenschutzes

## Zu Absatz 1

Die Verordnung (EU) 2016/679 stellt die Bedeutung des technischen und organisatorischen Datenschutzes heraus und verlangt hierzu entsprechende Maßnahmen, die ein dem Risiko angemessenes Schutzniveau gewährleisten. Die aufgeführten Maßnahmen stellen eine Konkretisierung der in Artikel 32 Absatz 1 Buchstaben a bis d der Verordnung (EU) 2016/679 als geeignet genannten Maßnahmen auf der Grundlage von Artikel 6 Absatz 2 der Verordnung (EU) 2016/679 dar. Ihre Aufzählung ist nicht abschließend. Sie tragen entscheidend dazu bei, bei der Verarbeitung personenbezogener Daten die Gefahren für die Rechte und Freiheiten der betroffenen Personen möglichst gering zu halten und damit die Grundrechte der betroffenen Personen zu wahren.

Damit setzt die Regelung zugleich das Erfordernis um, bei der Verarbeitung besonderer Kategorien personenbezogener Daten nach Artikel 9 der Verordnung (EU) 2016/679 „angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person“ vorzusehen.

Verpflichtende Maßnahmen, wie z. B. die Beteiligung der oder des Datenschutzbeauftragten der öffentlichen Stelle sind nicht aufgeführt.

## Zu Absatz 2

Die Regelung übernimmt das Datengeheimnis entsprechend der Regelung in § 6 LDSG a. F. Damit ist im Sinne von Artikel 32 Absatz 4 der Verordnung (EU)

2016/679 sichergestellt, dass die dem Verantwortlichen unterstellten natürlichen Personen personenbezogene Daten nur auf Anweisung des Verantwortlichen verarbeitet werden, es sei denn, sie sind gesetzlich dazu verpflichtet. Ein Verstoß hiergegen ist strafbewehrt (vgl. § 29).

#### Zu Abschnitt 2 – Rechtsgrundlagen der Verarbeitung personenbezogener Daten

##### Zu § 4 – Zulässigkeit der Verarbeitung personenbezogener Daten

Auf der Grundlage von Artikel 6 Absatz 1 Buchstabe e in Verbindung mit Artikel 6 Absatz 3 Satz 1 der Verordnung (EU) 2016/679 wird eine Rechtsgrundlage für die Datenverarbeitung geschaffen. Dies ist rechtlich notwendig, da Artikel 6 Absatz 1 Buchstabe e der Verordnung (EU) 2016/679 selbst keine Rechtsgrundlage für die Verarbeitung von Daten schafft, was sich aus der Formulierung in Artikel 6 Absatz 3 Satz 1 der Verordnung (EU) 2016/679 ergibt. Der Unions- oder der nationale Gesetzgeber hat eine Rechtsgrundlage zu setzen. Diesem Regelungsauftrag wird mit dieser Vorschrift nachgekommen.

Öffentliche Stellen können vorbehaltlich anderer bereichsspezifischer Regelungen auf die Regelung unabhängig davon zurückgreifen, zu welchen Zwecken die Datenverarbeitung erfolgt.

Die Verarbeitung personenbezogener Daten durch öffentliche Stellen ist nach der Vorschrift zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der öffentlichen Stelle nach § 2 liegenden Aufgabe erforderlich ist oder wenn sie in Ausübung öffentlicher Gewalt erfolgt, die der öffentlichen Stelle übertragen wurde. Beides kann sich sowohl aus nationalen Rechtsvorschriften als auch aus EU-Recht ergeben.

Die Verarbeitung personenbezogener Daten ist allerdings nicht nur auf dieser Rechtsgrundlage zulässig, sondern auch auf der Grundlage der weiteren in Artikel 6 Absatz 1 der Verordnung (EU) 2016/679 aufgeführten Erlaubnistatbestände einschließlich der auf der Grundlage der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 erlassenen bereichsspezifischen Regelungen. So ist beispielsweise die Zulässigkeit der Verarbeitung von Schülerdaten bisher im Schulgesetz oder von Sozialdaten im Zehnten in Verbindung mit dem Ersten Buch Sozialgesetzbuch sowie in den übrigen Sozialgesetzbüchern geregelt. Die Einwilligung als Rechtsgrundlage der Verarbeitung personenbezogener Daten ergibt sich aus Artikel 6 Absatz 1 Satz 1 Buchstabe a der Verordnung (EU) 2016/679 unmittelbar.

Die Regelung nimmt den bisher in § 13 Absatz 1 und § 15 Absatz 1 des Landesdatenschutzgesetzes enthaltenen Regelungsgehalt auf, unterscheidet aber nicht mehr zwischen den Phasen der Erhebung, Speicherung, Veränderung und Nutzung, sondern verwendet, dem Grundgedanken der Verordnung (EU) 2016/679 folgend, allgemein den umfassenden Begriff der Verarbeitung. Dieser umfasst nach der Definition in Artikel 4 Nummer 2 der Verordnung (EU) 2016/679 alle Phasen der Verarbeitung personenbezogener Daten. Wie nach geltendem Recht enthält § 4 Absatz 1 eine subsidiäre, allgemeine Rechtsgrundlage für Datenverarbeitungen mit geringer Eingriffsintensität in die Rechte der betroffenen Person.

##### Zu § 5 – (Ergänzung zu Artikel 6 Absatz 3 und 4 der Verordnung [EU] 2016/679) – Datenverarbeitung zu anderen Zwecken

###### Zu Absatz 1

Die Zweckbindung ist in Artikel 5 Absatz 1 Buchstabe b der Verordnung (EU) 2016/679 als Grundsatz der Datenverarbeitung aufgeführt und bedarf daher keiner weiteren Erwähnung im Landesdatenschutzgesetz. Sie besagt im Grundsatz, dass die erhobenen Daten von der erhebenden Stelle oder dem Dritten, an den die Da-

ten übermittelt werden, nur für den Erhebungszweck verarbeitet werden dürfen. Daneben wird die Zweckänderung bei Vereinbarkeit mit dem Erhebungszweck in Artikel 6 Absatz 4 der Verordnung (EU) 2016/679 unter den dort genannten Voraussetzungen zugelassen.

Die gesetzliche Regelung im Landesdatenschutzgesetz dient dazu, die Tatbestände zu regeln, in denen gemäß Artikel 6 Absatz 4 der Verordnung (EU) 2016/679 eine Verarbeitung personenbezogener Daten für andere Zwecke in der Regel eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 der Verordnung (EU) 2016/679 genannten Ziele darstellt oder als kompatibel mit den ursprünglichen Erhebungszwecken im Sinne von Artikel 6 Absatz 4 der Verordnung (EU) 2016/679 erachtet wird. Denn gemäß Erwägungsgrund 50 Satz 3 der Verordnung (EU) 2016/679 können im mitgliedstaatlichen Recht Aufgaben und Zwecke konkretisiert werden, für die eine Weiterverarbeitung als vereinbar und rechtmäßig angesehen wird.

Nicht erwähnt werden die Zweckänderungen, deren Zulässigkeit sich direkt aus der Verordnung (EU) 2016/679 ergibt. Dies sind die Zulässigkeit einer Zweckänderung aufgrund einer Einwilligung gemäß Artikel 6 Absatz 4 Fall 1 oder aufgrund einer sonstigen mit dem Erhebungszweck zu vereinbarenden Weiterverarbeitung gemäß Artikel 6 Absatz 4 Fall 3 der Verordnung (EU) 2016/679.

Die bisher nach § 15 Absatz 2 LDSG a. F. zulässigen Zweckänderungen konnten nur insoweit als Befugnisse für zweckändernde Datenverarbeitungen aufrechterhalten werden, als diese durch die Verordnung (EU) 2016/679 gedeckt sind und dem Wiederholungsverbot nicht entgegenstehen.

Im Einzelnen werden die Tatbestände des Absatzes 1 auf folgende Normen der Verordnung (EU) 2016/679 gestützt:

Nummer 1: Artikel 6 Absatz 4 Fall 2 in Verbindung mit Artikel 23 Absatz 1 Buchstaben c und e,

Nummer 2: Artikel 6 Absatz 4 Fall 2 in Verbindung mit Artikel 23 Absatz 1 Buchstabe i,

Nummer 3: Artikel 6 Absatz 4 Fall 2 in Verbindung mit Artikel 23 Absatz 1 Buchstaben d und e,

Nummer 4: die Weiterverarbeitung wird als kompatibel mit dem ursprünglichen Verarbeitungszweck angesehen.

Diese Regelung berührt nicht die Zulässigkeit einer Zweckänderung aufgrund einer spezialgesetzlichen Regelung, die gemäß Artikel 6 Absatz 1 Buchstaben c und e der Verordnung (EU) 2016/679 in Verbindung mit Artikel 6 Absatz 3 der Verordnung (EU) 2016/679 erlassen wurde oder aufgrund einer sonstigen Rechtsgrundlage gemäß Artikel 6 Absatz 1 der Verordnung (EU) 2016/679. Sie gilt nicht für die Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Artikel 9 Absatz 1 der Verordnung (EU) 2016/679.

Mit dem Erforderlichkeitsprinzip wird die Zulässigkeit an ein weiteres Kriterium gebunden.

Zu Absatz 2

Die Verarbeitung personenbezogener Daten zu den in Absatz 2 genannten Zwecken wird nicht als Zweckänderung angesehen, da in Bezug auf die betroffene Person kein inhaltlich neuer Zweck verfolgt wird. Es ist unabdingbar, dass öffentliche Stellen personenbezogene Daten auch zu diesen Zwecken verarbeiten dürfen, um ein rechtmäßiges und effizientes Verwaltungshandeln sicherzustellen. Deshalb sollen diese Zwecke auf der Grundlage von Artikel 6 Absatz 1 Buchstabe e in Verbindung mit Absatz 2 und 3 der Verordnung (EU) 2016/679 von vornherein als zulässige Verarbeitungszwecke definiert werden. Die Weiterverarbeitung für

Aus- und Fortbildungszwecke wird aber zum Schutz der betroffenen Personen nur eingeschränkt zugelassen.

Als Aufsicht ist die Dienst- und Fachaufsicht durch die jeweils übergeordnete Stelle zu verstehen. Hinzu kommt die Aufsicht über Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie die Rechnungsprüfung.

Die Weiterverarbeitung zu statistischen und wissenschaftlichen Zwecken ist bereits in Artikel 5 Absatz 1 Buchstabe b der Verordnung (EU) 2016/679 geregelt.

Zu Absatz 3

Diese Regelung ist als Annex zu Absatz 1 zur Absicherung der Erfüllung der dort in den Nummern 1 bis 4 genannten Zwecke zu verstehen. Die Informationspflicht gemäß Artikel 13 der Verordnung (EU) 2016/679 wird gemäß Artikel 23 Absatz 1 der Verordnung (EU) 2016/679 eingeschränkt. Für die Informationspflicht nach Artikel 14 der Verordnung (EU) 2016/679 ergibt sich der Wegfall der Informationspflicht bereits aus dessen Absatz 5 Buchstabe b. Zu beachten ist, dass im Hinblick auf die Formulierung „soweit und solange“ die Informationspflicht nachzuholen ist, sobald der Hinderungsgrund entfallen ist.

Zu Absatz 4

Die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebs gespeicherten Daten unterliegen einer engen Zweckbindung. Die Weiterverarbeitung ist nur für dienst- und arbeitsrechtliche Maßnahmen in Bezug auf die betroffene Person zulässig. Artikel 23 Absatz 1 Buchstabe h der Verordnung (EU) 2016/679 lässt eine solche Regelung, die bisher in § 15 Absatz 4 LDSG a. F. enthalten war, zu. Eine Weiterverarbeitung für die anderen in Absatz 1 aufgeführten Zwecke ist damit ausgeschlossen, ebenso für die Mitarbeiterüberwachung. Die Zweckbindung soll aber nicht die Verwendung dieser Daten zur Verhütung oder Verfolgung von Straftaten gegen Leib, Leben oder Freiheit einer Person verhindern und wird daher für diesen Fall aufgehoben. Diese Regelung wird auf Artikel 23 Absatz 1 Buchstabe d in Verbindung mit Artikel 5 der Verordnung (EU) 2016/679 gestützt. Daneben können weitere spezialgesetzliche Ermächtigungen zur Weiterverarbeitung, insbesondere im Straf- oder Steuerrecht, bestehen.

Zu § 6 – Übermittlung personenbezogener Daten

Zu Absatz 1

Nach der Verordnung (EU) 2016/679 wird die Übermittlung personenbezogener Daten nicht gesondert geregelt, da es sich um einen Verarbeitungsschritt handelt. Ihre Zulässigkeit ist, sofern sie nicht zu den Zwecken erfolgt, zu denen die personenbezogenen Daten erhoben wurden, nach Artikel 5 und 6 Absätze 1, 3 und 4 der Verordnung (EU) 2016/679 zu beurteilen und muss wie eine Zweckänderung die Voraussetzungen des § 5 erfüllen, sofern ihre Übermittlung nicht durch eine spezielle Rechtsvorschrift geregelt ist.

Die Vorschrift schafft materiell eine besondere Rechtsgrundlage für die Übermittlung personenbezogener Daten durch öffentliche Stellen, soweit diese zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, erfolgt. Damit trägt sie dem Gesetzesvorbehalt Rechnung. Die Übermittlung zu den Zwecken, zu denen die personenbezogenen Daten erhoben wurden, beurteilt sich nach § 4 oder spezialgesetzlichen Vorschriften.

Die Regelung in Nummer 1 erfasst Datenübermittlungen, soweit diese zur Aufgabenerfüllung erforderlich sind. Eine Übermittlung ist gemäß dieser Vorschrift

zulässig, wenn die Voraussetzungen für eine Verarbeitung zu einem anderen Zweck nach § 5 vorliegen. Die Empfänger können öffentliche und nichtöffentliche Stellen sein.

Nummer 2 regelt die tatbestandlichen Voraussetzungen der Datenübermittlung an nichtöffentliche Stellen. Die Informationspflichten nach Artikel 13 und 14 der Verordnung (EU) 2016/679 sind zu beachten.

Zu Absatz 2

Die Regelung betrifft die Verantwortung der übermittelnden Stelle und erfolgt in Ausnutzung des in Artikel 4 Nummer 7 der Verordnung (EU) 2016/679 eröffneten Regelungsspielraums. Die Informationspflicht trifft die verantwortliche Stelle; dies wird für die ersuchende Behörde klargestellt.

Zu Absatz 3

Die Verantwortung wird in Bezug auf automatisierte Abrufverfahren gemäß Artikel 4 Nummer 7 und Artikel 26 der Verordnung (EU) 2016/679 festgelegt.

Zu § 7 – Datenverarbeitung in der gemeinsamen Dienststelle

Die bisherige Vorschrift des § 33 a LDSG a. F. wird beibehalten. Diese Vorschrift wurde mit dem Verwaltungsstruktur-Reformgesetz vom 1. Juli 2004 (GBl. S. 469) eingeführt. Die Gesetzesbegründung (Drucksache 13/3201, S. 293) geht davon aus, dass gemeinsame Dienststellen keine öffentlichen Stellen im Sinne des Landesdatenschutzgesetzes seien, da sie in personeller, haushaltsmäßiger und organisatorischer Hinsicht nicht ausreichend eigenständig seien. An der Sachlage hat sich seit damals nichts geändert. In der Praxis existieren zahlreiche gemeinsame Dienststellen der Landratsämter, insbesondere im Bereich der Flurneuordnung, die die bisher geltende Vorschrift angewendet haben.

Die Regelung grenzt die Verantwortlichkeiten in der gemeinsamen Dienststelle ab und stellt somit eine Regelung nach Artikel 4 Nummer 7 der Verordnung (EU) 2016/679 dar. Die örtlich zuständige öffentliche Stelle ergibt sich aus den Vorschriften zu der auszuführenden öffentlichen Aufgabe.

Zu Abschnitt 3 – Rechte der betroffenen Person

Zu §§ 8 bis 11

Die in Abschnitt 3 vorgenommenen Einschränkungen der Betroffenenrechte und Pflichten des Verantwortlichen und Auftragsverarbeiters ergänzen die in der Verordnung (EU) 2016/679 unmittelbar vorgesehenen Ausnahmen.

Die Beschränkungen der Betroffenenrechte finden auch Anwendung auf die in Artikel 89 der Verordnung (EU) 2016/679 geregelte Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken.

Zu § 8 – (Ergänzung zu Artikel 13 und 14 der Verordnung [EU] 2016/679) – Beschränkung der Informationspflicht

Zu Absatz 1

Die Verordnung (EU) 2016/679 sieht in ihren Artikeln 13 und 14 umfängliche Informationspflichten der verantwortlichen Stelle gegenüber der betroffenen Person

bei der Erhebung personenbezogener Daten sowie etwaiger zweckändernder Weiterverarbeitung vor. Auf diese Weise soll ein größtmögliches Maß an Transparenz im Sinne von Artikel 5 Absatz 1 Buchstabe a der Verordnung (EU) 2016/679 hergestellt werden.

Das Recht auf Information darf nur unter den engen Voraussetzungen des Artikels 23 Absatz 1 der Verordnung (EU) 2016/679 beschränkt werden. Die Beschränkungen der Nummern 1 bis 5 werden im Wesentlichen auf folgende Tatbestände des Artikels 23 Absatz 1 der Verordnung (EU) 2016/679 gestützt:

Nummer 1: Buchstaben c und e

Nummer 2: Buchstaben d und e

Nummer 3: Buchstabe j

Nummer 4: Buchstaben e und i

Nummer 5: Buchstabe e

Absatz 1 gilt sowohl bei der Erhebung von personenbezogenen Daten bei der betroffenen Person als auch bei der Erhebung bei Dritten. Anwendungsfälle der Nummer 1 sind unter anderen die in § 14 Absatz 3 Nummer 4 LDSG a. F. genannten Aufgaben der Gefahrenabwehr oder der Finanzverwaltung im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung oder die Verfolgung von Straftaten oder Ordnungswidrigkeiten. Bei der Verarbeitung von personenbezogenen Daten zu wissenschaftlichen oder historischen Forschungszwecken kann die Pflicht zur Information die spezifischen Forschungszwecke gefährden. Daher wurde eine entsprechende Beschränkung des Betroffenenrechts vorgesehen.

Weitere Ausnahmen von der Informationspflicht können sich aus Artikel 14 Absatz 5 der Verordnung (EU) 2016/679 ergeben, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden.

Zu Absatz 2

Dieser Absatz stützt sich auf Artikel 23 Absatz 1 Buchstaben a bis e der Verordnung (EU) 2016/679.

Zu Absatz 3

Die Gründe für das Absehen von der Information sind auf jeden Fall zu dokumentieren, um die Nachprüfbarkeit durch die Aufsichtsbehörde, Gerichte etc. zu ermöglichen.

Zu § 9 – (Ergänzung zu Artikel 15 der Verordnung [EU] 2016/679) – Beschränkung des Auskunftsrechts

Zu Absatz 1

Die Gründe für die Verweigerung der Auskunft entsprechen denen, die auch die Informationspflicht entfallen lassen. Damit ist gewährleistet, dass diesbezüglich ein Gleichlauf besteht.

Einzig für die Verarbeitung von personenbezogenen Daten zu wissenschaftlichen oder historischen Forschungszwecken besteht mit § 13 Absatz 4 eine besondere Regelung zur Beschränkung des Auskunftsrechts.

Das Auskunftsrecht für Sicherungsdaten ist weiterhin ausgeschlossen. Erforderlich ist aber eine Einschränkung der Verarbeitung zum Schutz der betroffenen Person. Die Sicherungsdaten werden nur vorgehalten, um den aktuellen Bestand

im Falle des Verlusts oder der Zerstörung jederzeit wieder rekonstruieren zu können. Die Einbeziehung der – mit dem aktuellen Bestand weithin identischen – Daten in die Auskunftspflicht ist entbehrlich. Schutzwürdige Interessen der betroffenen Personen werden nicht berührt.

Auch die Daten, die ausschließlich Zwecken der Datenschutzkontrolle dienen, sind von der Auskunftspflicht ausgenommen. Diese Unterlagen enthalten im Regelfall keine Daten über die betroffene Person, die sich nicht auch im Bestand der verantwortlichen Stelle befinden. Im Einzelfall ist eine Abwägung mit den Interessen der betroffenen Person vorzunehmen, die auch den Aufwand der Auskunftserteilung zu berücksichtigen hat.

#### Zu Absatz 2

Eine entsprechende Einschränkung sieht Erwägungsgrund 63 der Verordnung (EU) 2016/679 vor. Im Interesse der betroffenen Person wird die Beschränkung jedoch abgemildert, indem die öffentliche Stelle verpflichtet wird, zumindest die Verarbeitungsvorgänge sowie die Art der verarbeiteten Daten zu benennen.

#### Zu Absatz 3

Die Vorschrift dient dazu, wie in § 8 Absatz 2, die Interessen der Sicherheitsbehörden vor der Erteilung der Auskunft berücksichtigen zu können und die Auskunft gegebenenfalls zu verweigern.

#### Zu Absatz 4

Nur von der Begründung der Ablehnung der Auskunftserteilung gegenüber der betroffenen Person kann aus den genannten Gründen abgesehen werden. Die Gründe der Auskunftsverweigerung sind auf jeden Fall zu dokumentieren. Die Dokumentations- und die Begründungspflicht sind Maßnahmen zum Schutz der Rechte und Freiheiten der betroffenen Personen im Sinne des Artikels 23 Absatz 2 Buchstaben c, d, g und h der Verordnung (EU) 2016/679.

Die betroffene Person ist darauf hinzuweisen, dass sie die Landesbeauftragte für den Datenschutz oder den Landesbeauftragten für den Datenschutz anrufen kann.

#### Zu Absatz 5

Durch diese Maßnahme wird im Sinne von Artikel 23 Absatz 2 der Verordnung (EU) 2016/679 sichergestellt, dass die Rechte der betroffenen Person angemessen gewahrt bleiben. Der betroffenen Person wird grundsätzlich die Möglichkeit gegeben, durch die Landesbeauftragte für den Datenschutz oder den Landesbeauftragten für den Datenschutz prüfen zu lassen, ob sie durch die Verweigerung der Auskunft in ihrem Persönlichkeitsrecht beeinträchtigt worden ist. Die Beschränkung der Information an die Landesbeauftragte für den Datenschutz oder den Landesbeauftragten für den Datenschutz dient dem Schutz der öffentlichen Sicherheit (Artikel 23 Absatz 1 Buchstabe c der Verordnung (EU) 2016/679) und der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten (Artikel 23 Absatz 1 Buchstabe d der Verordnung (EU) 2016/679).

Die Versagungsgründe im Satz 1 sind sehr eng gefasst. Sie ist als eine Art Notstandsklausel anzusehen, deren Anwendung nur in extremen Ausnahmefällen in Betracht kommt. Im Regelfall wird zuzustimmen sein. Satz 2 soll verhindern, dass über die Einschaltung der Aufsichtsbehörde Ausforschungsanträge möglich sind.

Zu § 10 – (Ergänzung zu Artikel 17 der Verordnung [EU] 2016/679) – Beschränkung des Rechts auf Löschung

Zu Absatz 1

Es handelt sich um eine Klarstellung, die sich aus dem Vorrang bereichsspezifischer Regelungen ergibt.

Zu Absatz 2

Diese Ausnahme tritt neben die in Artikel 17 Absatz 3 Buchstaben a bis e der Verordnung (EU) 2016/679 genannten Ausnahmen. Sie stützt sich auf Artikel 23 Absatz 1 Buchstabe i der Verordnung (EU) 2016/679. Die öffentliche Stelle hat die betroffene Person über das Absehen von der Löschung und die Einschränkung der Verarbeitung zu unterrichten, damit diese ggf. ihre Betroffenenrechte ausüben kann. Der Zeitpunkt der Unterrichtung ist nicht festgelegt. Im Verwaltungsvollzug kann dies bereits im Vorhinein, z. B. bei der Information nach Artikel 13, 14 der Verordnung (EU) 2016/679 oder bei der Speicherung, erfolgen. Widerspricht die betroffene Person dem Absehen von der Löschung, sind die Daten zu löschen.

Zu Absatz 3

Erfasst werden von der Vorschrift vor allem Archivierungen in Papierform oder die Nutzung früher gebräuchlicher analoger Speichermedien, etwa Mikrofiches, bei denen es nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist, einzelne Informationen selektiv zu entfernen. Zusätzliche Voraussetzung für das Entfallen der Löschungspflicht ist, dass das Interesse der betroffenen Person an der Löschung als gering anzusehen ist.

Zu § 11 – (Ergänzung zu Artikel 34 der Verordnung [EU] 2016/679) – Beschränkung der Benachrichtigungspflicht

Das Recht der betroffenen Person auf bzw. die Pflicht des Verantwortlichen zur Benachrichtigung nach Artikel 34 der Verordnung (EU) 2016/679 darf nur unter den engen Voraussetzungen von Artikel 23 Absatz 1 der Verordnung (EU) 2016/679 beschränkt werden. Nach der bisherigen Rechtslage gibt es keine entsprechende Benachrichtigungspflicht.

Die Nummern 1 und 2 entsprechen den in § 8 unter Nummern 1 und 4 geregelten Beschränkungen bei der Informationspflicht und beim Auskunftsrecht (vgl. § 9) und werden in gleicher Weise auf Artikel 23 Absatz 1 der Verordnung (EU) 2016/679 gestützt.

Zusätzlich kann nach Nummer 3 die Benachrichtigung über die Verletzung des Schutzes personenbezogener Daten unterbleiben, soweit und solange die Benachrichtigung die Sicherheit von Datenverarbeitungssystemen gefährden würde. Dieses wird auf Artikel 23 Absatz 1 Buchstabe e der Verordnung (EU) 2016/679 gestützt. Die zunehmende Bedeutung der Digitalisierung für die Verwaltung erhöht auch das Risiko, dass eine Einschränkung der Funktionsfähigkeit von Datenverarbeitungssystemen zu einer Gefährdung der gesamten Verwaltungstätigkeit führen kann. Eine funktionsfähige Verwaltung ist ein sonstiges wichtiges Ziel des allgemeinen öffentlichen Interesses im Sinne von Artikel 23 Absatz 1 Buchstabe e der Verordnung (EU) 2016/679, vergleichbar mit den dort beispielhaft aufgeführten Zielen. Gefährdet die Benachrichtigung diese Ziele, muss sie unterbleiben, soweit und solange eine solche Gefährdung besteht. Der Verantwortliche hat zu prüfen, in welchem Umfang und in welchem Zeitraum eine entsprechende Gefährdung besteht. Soweit und sobald eine Gefährdung nicht mehr vorliegt, hat die entsprechende Benachrichtigung zu erfolgen.

Weitere Ausnahmen sind in Artikel 34 Absatz 3 der Verordnung (EU) 2016/679 geregelt.

Zu Abschnitt 4 – Besondere Verarbeitungssituationen

Zu § 12 – Verarbeitung personenbezogener Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen

Zu Absatz 1

Normadressat ist die Stelle, an die die der Geheimhaltungspflicht unterliegenden personenbezogenen Daten – ausnahmsweise – übermittelt oder auf eine sonstige Art bekannt gegeben wurden. Die Zweckbindung wird für personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, enger gefasst als nach § 5 dieses Gesetzes.

Artikel 9 der Verordnung (EU) 2016/679 bleibt unberührt. Die Voraussetzungen nach dieser Vorschrift müssen für die Datenverarbeitung zusätzlich erfüllt sein.

Zu Absatz 2

Eine Zweckdurchbrechung wird nur zugelassen, wenn es für das Gemeinwohl, die Gefahrenabwehr oder zur Strafverfolgung erforderlich ist und die zur Verschwiegenheit verpflichtete Stelle zugestimmt hat.

Zu §§ 13 bis 16

Die Verarbeitung besonderer Kategorien personenbezogener Daten ist nach Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 grundsätzlich untersagt. Die Definition dieser besonders sensiblen Daten ist in Artikel 9 Absatz 1 sowie in Artikel 4 Nummer 13 (genetische Daten), Nummer 14 (biometrische Daten) und Nummer 15 (Gesundheitsdaten) enthalten.

Ausnahmen von dem Verarbeitungsverbot sind gemäß Artikel 9 Absatz 2 der Verordnung (EU) 2016/679 aufgrund mitgliedstaatlicher Regelungen für bestimmte Zwecke erlaubt. In der Regel bedarf es daher fachlicher Gesetze, um die Verarbeitung besonderer Kategorien personenbezogener Daten zu regeln. Dieses Gesetz enthält daher nur insofern Regelungen für die Verarbeitung dieser Daten, als bereichsspezifische Gesetze fehlen. Dies betrifft die Datenverarbeitung für wissenschaftliche und statistische Zwecke, für im öffentlichen Interesse liegende Archivzwecke sowie die Datenverarbeitung bei Dienst- und Arbeitsverhältnissen, sofern diese nicht im Dienst- oder Arbeitsrecht geregelt ist. Außerdem wird eine Rechtsgrundlage für die Verarbeitung besonderer Kategorien personenbezogener Daten für die Entscheidung über die Verleihung von öffentlichen Auszeichnungen und Ehrungen geschaffen.

Angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person im Sinne von § 3 dieses Gesetzes vorzusehen, ist bezüglich der Verarbeitung besonderer Kategorien personenbezogener Daten von besonderer Bedeutung. Dies gilt auch für die in der Verordnung (EU) 2016/679 vorgeschriebene Datenschutz-Folgeabschätzung gemäß Artikel 35 und vorherige Konsultation der Aufsichtsbehörde gemäß Artikel 36.

Zu § 13 – Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken

Die wissenschaftliche Forschung unterliegt gemäß Artikel 5 Absatz 1 Buchstabe b, Artikel 9 Absatz 2 Buchstabe j und Artikel 89 Absatz 1 und 2 der Verordnung

(EU) 2016/679 Privilegierungen. Damit wird der verfassungsrechtlich garantierten Freiheit von Wissenschaft und Forschung Rechnung getragen. Diese ist in Einklang zu bringen mit dem Anspruch des Einzelnen auf informationelle Selbstbestimmung. Die Regelung verdrängt in ihrem Anwendungsbereich die allgemeinen Vorschriften.

#### Zu Absatz 1

Es wird eine besondere Rechtsgrundlage für die Datenverarbeitung für wissenschaftliche Forschungszwecke geschaffen. Diese ergänzt § 4 des Entwurfs hinsichtlich der Datenverarbeitung zu diesen Zwecken mit hoher Eingriffsintensität in die Rechte der betroffenen Person. Anderenfalls wäre die Forschung hierfür auf die Einwilligung gemäß Artikel 6 Buchstabe a der Verordnung (EU) 2016/679 als Rechtsgrundlage für die Datenverarbeitung angewiesen. Die Weiterverarbeitung zu Forschungszwecken richtet sich nach Artikel 5 Absatz 1 Buchstabe b der Verordnung (EU) 2016/679.

Zugleich wird von der Ermächtigung gemäß Artikel 9 Absatz 2 Buchstabe j der Verordnung (EU) 2016/679 Gebrauch gemacht, im nationalen Recht die Verarbeitung besonderer Kategorien personenbezogener Daten zu Forschungszwecken und statistischen Zwecken zu gestatten, wenn sie erforderlich ist. Erforderlichkeit ist nicht erst dann anzunehmen, wenn die Verarbeitung zur Erreichung des Zwecks unerlässlich ist, sondern schon dann, wenn es keine sinnvolle und zumutbare Alternative zur Erreichung des Zwecks gibt. Die in Artikel 9 Absatz 2 Buchstabe j der Verordnung (EU) 2016/679 geforderten angemessenen und spezifischen Maßnahmen werden auf der Grundlage von § 3 getroffen.

Absatz 1 gilt auch als Rechtsgrundlage für die Weiterverarbeitung personenbezogener Daten einschließlich besonderer Kategorien personenbezogener Daten zu den genannten Zwecken, da Artikel 5 Absatz 1 Buchstabe b der Verordnung (EU) 2016/679 die Weiterverarbeitung für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke als kompatibel mit der Erstverarbeitung regelt. Dies gilt insbesondere auch für die Übermittlung zu Forschungs- und Statistikzwecken. §§ 5 und 6 finden insoweit keine Anwendung.

#### Zu Absatz 2

Die Pflicht zur Anonymisierung gilt für alle personenbezogenen Daten. Für die Anonymisierung fehlt eine Definition in der Verordnung (EU) 2016/679; sie wird jedoch im Erwägungsgrund 26 erwähnt und beschrieben. Daneben können weitere Maßnahmen nach § 3 erforderlich sein zur Wahrung der Rechte der betroffenen Person (z. B. aggregierte Daten).

#### Zu Absatz 3

Diese Regelung spezifiziert die Verarbeitung personenbezogener Daten im Hinblick auf deren Veröffentlichung, indem zum Schutz der Rechte der betroffenen Personen nur im besonderen Ausnahmefall eine personenbezogene Darstellung der Forschungsergebnisse zugelassen wird. Dies soll, wie bisher, nur zulässig sein, wenn dies für die Darstellung von Ereignissen der Zeitgeschichte unerlässlich ist.

#### Zu Absatz 4

Die Einschränkung der Betroffenenrechte beruht auf der Öffnungsklausel des Artikels 89 Absatz 2 der Verordnung (EU) 2016/679. Sie gilt für alle Kategorien personenbezogener Daten.

Die Einschränkung der Betroffenenrechte für statistische Zwecke entspricht der Regelung in § 27 Absatz 2 des Bundesdatenschutzgesetzes und dient damit der Rechtsvereinheitlichung zwischen Bund und Land insbesondere im Bereich der amtlichen Statistik, sowie bei anderen öffentlichen Stellen nach § 2 Absatz 1. Im Bereich der amtlichen Statistik unterliegt die Datenverarbeitung zu statistischen Zwecken aufgrund der statistischen Geheimhaltung und dem Grundsatz der frühestmöglichen Anonymisierung weitreichenden Garantien zur Wahrung der Rechte der Betroffenen.

Die Regelung trägt auch den bestehenden besonderen Interessen im Bereich der Forschung Rechnung. Mit ihr wird die Arbeitsfähigkeit der Forschung gesichert und zugleich werden die Interessen der betroffenen Personen durch die engen Voraussetzungen in Satz 1 der Regelung angemessen berücksichtigt. Absatz 4 Satz 2 schränkt das Auskunftsrecht im Bereich der Forschung für die Fälle unverhältnismäßigen Aufwands unter Ausnutzung der Öffnungsklausel des Artikel 23 Absatz 1 Buchstabe e der Verordnung (EU) 2016/679 ein. Die Einschränkung des Auskunftsrechts für den Fall unverhältnismäßigen Aufwands kann beispielsweise gegeben sein, wenn ein Forschungsvorhaben mit besonders großen Datenmengen arbeitet. Zusätzlich werden die Rechte der betroffenen Personen durch die frühestmögliche Anonymisierung gewahrt.

Zu § 14 – Datenverarbeitung zu im öffentlichen Interesse liegenden Archivzwecken

Mit dieser Regelung wird auf der Grundlage von Artikel 9 Absatz 2 Buchstabe j der Verordnung (EU) 2016/679 ein weiterer Ausnahmetatbestand für die Verarbeitung besonderer Kategorien personenbezogener Daten für im öffentlichen Interesse liegende Archivzwecke geschaffen. In ihrem Anwendungsbereich verdrängt die Vorschrift die allgemeinen Regelungen.

Zu Absatz 1

Absatz 1 gilt als Rechtsgrundlage für die Verarbeitung besonderer Kategorien personenbezogener Daten zu im öffentlichen Interesse liegenden Archivzwecken. Diese Vorschrift regelt nur die Verarbeitung besonderer Kategorien personenbezogener Daten. Die Regelungen für die Verarbeitung sonstiger personenbezogener Daten ergeben sich aus der Verordnung (EU) 2016/679, diesem Gesetz oder bereichsspezifischem Recht.

Auch bei der Weiterverarbeitung zu im öffentlichen Interesse liegenden Archivzwecken ist Absatz 1 zu beachten.

Zu den Absätzen 2 bis 4

In den Absätzen 2 bis 4 werden unter Ausnutzung der Öffnungsklausel des Artikels 89 Absatz 3 der Verordnung (EU) 2016/679 die Rechte gemäß der Artikel 15, 16, 18, 19, 20 und 21 der Verordnung (EU) 2016/679 eingeschränkt. Die Ausnahme gemäß Absatz 2 bezieht sich auf sämtliche durch Artikel 15 der Verordnung (EU) 2016/679 gewährte Rechte, insbesondere auch auf das Recht zum Erhalt einer Kopie. Die Absätze 2 bis 4 gelten für die Verarbeitung sämtlicher personenbezogener Daten einschließlich der Verarbeitung besonderer Kategorien personenbezogener Daten.

Zu Absatz 5

Die Ausnahmen des Artikels 17 Absatz 3 der Verordnung (EU) 2016/679 gelten für die Löschungspflichten nach Artikel 17 Absatz 1 der Verordnung (EU)

2016/679. Absatz 5 dient der Klarstellung, dass auch personenbezogene Daten, die einer bereichsspezifischen Löschungspflicht unterliegen, dem zuständigen Archiv vor der Löschung anzubieten sind.

Zu § 15 – Datenverarbeitung bei Dienst- und Arbeitsverhältnissen

Zu den Absätzen 1 bis 7

Die Öffnungsklausel des Artikels 88 der Verordnung (EU) 2016/679 lässt spezifischere nationale Regelungen zur Datenverarbeitung im Beschäftigungskontext zu. Hiervon wird Gebrauch gemacht, um den Datenschutz für die Beschäftigten bei öffentlichen Stellen des Landes zu verbessern. § 15 gilt auch für die öffentlichen Stellen gemäß § 2 Absatz 2. Die Betroffenenrechte ergeben sich direkt aus der Verordnung (EU) 2016/679, eingeschränkt durch §§ 8 bis 11.

Für die Verarbeitung von Gesundheitsdaten im Beschäftigtenverhältnis enthält das Gesetz über den öffentlichen Gesundheitsdienst (Gesundheitsdienstgesetz – ÖGDG) vom 17. Dezember 2015 (GBl. S. 1210) bereichsspezifische Vorschriften.

Zur Verarbeitung personenbezogener Daten von Beschäftigten auf der Grundlage einer Einwilligung werden keine Regelungen getroffen. Die Verordnung (EU) 2016/679 enthält in Artikel 7 die für die Rechtmäßigkeit der Einwilligung maßgeblichen Regelungen. Von entscheidender Bedeutung ist die Freiwilligkeit der Einwilligung. Bei der Beurteilung der Freiwilligkeit sind insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen. Freiwilligkeit kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen. Bei der Verarbeitung besonderer Kategorien personenbezogener Daten ist zu beachten, dass sich die Einwilligung ausdrücklich auf die Verarbeitung dieser Daten beziehen muss.

Zu den Absätzen 1 und 2

Absätze 1 und 2 unterscheiden zwischen der Verarbeitung personenbezogener Daten und der Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679. Hinsichtlich letzterer ist nur die Verarbeitung zur Erfüllung von dienst- oder arbeitsrechtlichen Rechten und Pflichten gemäß Artikel 9 Absatz 2 Buchstabe b der Verordnung (EU) 2016/679 zulässig.

Mit Absatz 1 Satz 2 wird die Weitergabe personenbezogener Daten an Interessenvertretungen wie den Personalrat oder die Schwerbehindertenvertretung legitimiert.

Die Regelungen erfassen alle Fälle der Verarbeitung von Daten der Beschäftigten, welche nicht zu den Personalaktendaten gehören (da hier Absatz 3 gilt) und nicht von den Regelungen des Absatzes 3 zu den Bewerberdaten erfasst werden.

Zu Absatz 3

Für den Spezialfall der Bewerbung wird die bisherige Vorschrift des § 36 LDSG a. F. für die Erhebung und Übermittlung zwischen Dienstherrn und Arbeitgebern fortgeführt. Grundsätzlich ist die Einwilligung erforderlich, die gemäß Artikel 7 Absatz 4 der Verordnung (EU) 2016/679 freiwillig erteilt werden muss.

Die bisher normierte Pflicht zur unverzüglichen Löschung der vorgelegten Unterlagen, wenn das Dienst- oder Arbeitsverhältnis nicht zustande kommt, ergibt sich

aus Artikel 17 der Verordnung (EU) 2016/679 genauso wie die Pflicht, die Löschung zu unterlassen, wenn die Unterlagen zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt werden.

Zu Absatz 4

Für das Personalaktendatenrecht wird auf beamtenrechtliche Vorschriften verwiesen. Den Regelungen des Absatzes 3 können nur Rechtsvorschriften oder Tarifverträge vorgehen (nicht Betriebs- oder Dienstvereinbarungen).

Zu Absatz 5

Die Voraussetzungen für die Verarbeitung personenbezogener Daten von Beschäftigten zur Aufdeckung von Straftaten, die im Beschäftigungsverhältnis begangen worden sind, werden geregelt. Die Regelung beruht auf Artikel 10 der Verordnung (EU) 2016/679.

Zu Absatz 6

Gemäß Artikel 9 Absatz 4 der Verordnung (EU) 2016/679 werden zusätzliche Beschränkungen für die Verarbeitung biometrischer Daten zu Authentifizierungs- und Autorisierungszwecken im Beschäftigtenverhältnis eingeführt. Zudem wird die Verarbeitung aufgrund einer Dienst- oder Betriebsvereinbarung für zulässig erklärt. Diese Regelung beruht auf Artikel 9 Absatz 2 Buchstabe b der Verordnung (EU) 2016/679. Dabei ist Artikel 88 Absatz 2 der Verordnung (EU) 2016/679 zu beachten. In beiden Fällen muss ein dringendes dienstliches Bedürfnis nachgewiesen werden. Das heißt, es darf keine weniger belastende Maßnahme zur Verfügung stehen, die denselben Zweck mit geringerer Eingriffstiefe erfüllt.

Zu Absatz 7

Zum Schutz der Persönlichkeitsrechte der Beschäftigten ist eine systematische Überwachung mit Hilfe optisch-elektronischer Einrichtungen zum Zweck der Verhaltens- und Leistungskontrolle unzulässig. Dies wird mit Satz 1 klargestellt. Soweit es um die Aufdeckung von Straftaten geht, richtet sich die Zulässigkeit nach Absatz 5.

Die Zulässigkeit sonstiger technischer Einrichtungen, die der Verhaltens- und Leistungskontrolle dienen, ist nach Absatz 1 zu beurteilen. Entscheidend ist danach die Erforderlichkeit. Gemäß Artikel 88 Absatz 2 der Verordnung (EU) 2016/679 sind angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Personen zu treffen. Dem dient der Hinweis auf Artikel 5 der Verordnung (EU) 2016/679. Der Schutz vor unbefugter und unberechtigter Verarbeitung ist im Beschäftigtendatenschutz von besonderer Bedeutung ebenso wie technische und organisatorische Maßnahmen, die darauf ausgelegt sind, die Datenschutzgrundsätze wie etwa die Datenminimierung und die Zweckbindung wirksam umzusetzen.

Zu Absatz 8

Der Begriff des Beschäftigten wird definiert.

## Zu § 16 – Öffentliche Auszeichnungen und Ehrungen

## Zu Absatz 1

Zusätzlich zum bisherigen Landesdatenschutzgesetz wird eine Regelung über die Verarbeitung für Entscheidungen über die Verleihung von öffentlichen Auszeichnungen, zum Beispiel staatlichen Orden und Ehrungen getroffen, um diese Datenverarbeitung auf eine rechtliche Grundlage unabhängig von der Einwilligung zu stellen. Die Vergabe öffentlicher Auszeichnungen und Ehrungen unterfällt nicht dem Anwendungsbereich des Unionsrechts. Für sie gilt daher § 2 Absatz 4, der die entsprechende Regelung der Verordnung (EU) 2016/679 und der Vorschriften dieses Gesetzes anordnet. Hier werden besondere Regelungen geschaffen, da die Ordensverleihung besonders sensible Bereiche berührt und daher spezielle datenschutzrechtliche Regelungen wünschenswert sind.

Zur Vorbereitung der Entscheidung sind alle Daten erforderlich, die zur Beurteilung der Ehrungswürdigkeit der betroffenen Person benötigt werden. Dies betrifft einerseits die Aspekte des der Auszeichnung zugrunde liegenden Sachzusammenhangs. Andererseits kann aber auch die persönliche Integrität der auszuzeichnenden Person von Bedeutung sein, sodass je nach Einzelfall auch diesbezügliche Informationen erhoben werden dürfen. Dies kann sich auch auf die Daten von Referenzpersonen beziehen. Die Datenverarbeitungsbefugnis erstreckt sich auch auf besondere Kategorien personenbezogener Daten, wenn diese Daten für die Entscheidung erforderlich sind.

Die Umstände, die zu einer positiven oder negativen Entscheidung führen, sind oft sehr sensibel und berühren die Integrität der beteiligten Personen, sodass keine Offenlegungspflicht in diesen Fällen zu verlangen ist.

Im Übrigen wird durch § 2 Absatz 4 sichergestellt, dass die Anforderungen der Verordnung (EU) 2016/679 in Bezug auf die Grundsätze der Verarbeitung und den technischen und organisatorischen Datenschutz eingehalten werden und die Datenverarbeitung der Kontrolle durch die Landesbeauftragte für den Datenschutz oder den Landesbeauftragten für den Datenschutz unterliegt.

Diese Regelung schließt auch die zweckändernde Übermittlung auf Anforderung ein. Die Feststellung der Ehrungswürdigkeit einer Person erfordert eine möglichst umfassende Heranziehung entscheidungsrelevanter Daten, und zwar gerade solcher, die ursprünglich für andere Zwecke erhoben beziehungsweise gespeichert worden sind.

## Zu Absatz 2

Eine zweckändernde Weiterverarbeitung wird für protokollarische Zwecke zugelassen. Damit wird § 5 Absatz 1 verdrängt. Im Übrigen ist diese nur mit Einwilligung zulässig.

## Zu § 17 – Verarbeitung personenbezogener Daten im öffentlichen Interesse

## Zu Absatz 1

Zur datenschutzrechtlichen Absicherung von Zuverlässigkeitsüberprüfungen durch öffentliche Stellen in sicherheits- oder sicherheitstechnisch relevanten Bereichen wird eine gesetzliche Ermächtigungsgrundlage geschaffen. Die personenbezogenen Daten dürfen für den Zweck der Überprüfung der Zuverlässigkeit nur verarbeitet werden, sofern dies erforderlich ist und die Einwilligung der betroffenen Person eingeholt wurde. Wegen der Eingriffstiefe in die Persönlichkeitsrechte der betroffenen Person, insbesondere, wenn Daten über strafrechtliche Verurteilungen und Straftaten bei Dritten abgefragt werden, kann auf die Einwilligung

nicht verzichtet werden. Es ist davon auszugehen, dass der Umfang der Verarbeitung personenbezogener Daten je nach Gefährdungslage zu differenzieren ist. Satz 2 beruht auf Artikel 9 Absatz 2 Buchstabe a und Artikel 10 der Verordnung (EU) 2016/679.

#### Zu Absatz 2

Diese Vorschrift wird auf der Grundlage von Artikel 9 Absatz 2 Buchstabe g der Verordnung (EU) 2016/679 als Auffangtatbestand für die Verarbeitung besonderer Kategorien personenbezogener Daten aufgenommen, falls eine bereichsspezifische Rechtsgrundlage nicht zur Verfügung steht. Sie regelt auch die Zweckänderung besonderer Kategorien personenbezogener Daten unter den genannten Voraussetzungen. Das LDSG a.F. enthielt in § 33 Absatz 3 eine teilweise vergleichbare Regelung.

Diese Regelung ist zulässig, da dieses Gesetz in § 3 angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person anordnet. Diese Maßnahmen sind immer zu treffen, haben aber bei der Verarbeitung besonderer Kategorien personenbezogener Daten besondere Bedeutung, um dem Verhältnismäßigkeitsprinzip Rechnung zu tragen. Sie sind an die jeweilige Schutzbedürftigkeit anzupassen.

#### Zu § 18 – Videoüberwachung öffentlich zugänglicher Räume

Die Regelungsbefugnis für die getroffene Regelung ergibt sich aus Artikel 6 Absatz 1 Buchstabe e in Verbindung mit Absatz 3 Satz 1 bis 3 der Verordnung (EU) 2016/679. Die Videoüberwachung zur Wahrung des Hausrechts wird zusätzlich zur Erfüllung öffentlicher Aufgaben aufgenommen, da sie nur mittelbar der Aufgabenerfüllung der öffentlichen Stelle dient. Öffentliche Stellen können sich in ihrer Eigenschaft als Eigentümer oder Mieter eines Gebäudes auf diese Norm stützen, soweit die Datenverarbeitung, in diesem Fall die Videoüberwachung, erforderlich ist, um ihre berechtigten Interessen zu wahren. Einbezogen ist insoweit auch die unmittelbare Umgebung dieser Objekte, soweit dies zur Erreichung des Ziels erforderlich ist.

Zur Konkretisierung werden die Zwecke, zu denen Videoüberwachung zulässig ist, festgelegt. Diese Regelung erfolgt gemäß Artikel 6 Absatz 3 Satz 2 der Verordnung (EU) 2016/679.

Nach Artikel 6 Absatz 3 Satz 3 der Verordnung (EU) 2016/679 können Vorschriften über die Verarbeitung personenbezogener Daten zur Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe oder in Ausübung öffentlicher Gewalt mit spezifischen Bestimmungen versehen werden. Außerdem müssen die Vorschriften dem Verhältnismäßigkeitsgrundsatz entsprechen (Artikel 6 Absatz 3 Satz 4 der Verordnung [EU] 2016/679).

Anwendungsfälle dieser Norm sind wie bisher (§ 20 a LDSG a.F.) der Personen- und Objektschutz, also der Schutz von Personen, die sich in öffentlichen Objekten oder in deren Nähe aufhalten, sowie der Schutz der öffentlichen Objekte selbst. Als öffentliche Objekte sind Kulturgüter, öffentliche Einrichtungen, Amtsgebäude oder sonstige bauliche Anlagen oder öffentliche Verkehrsmittel erfasst. Da sich die Schutzziele auch auf die unmittelbare Nähe der genannten Einrichtungen und Objekte beziehen, dürfen auch diese Zugangsbereiche videoüberwacht werden, sofern die Voraussetzungen vorliegen, also die Erforderlichkeit gegeben ist.

#### Zu Absatz 1

Normadressaten sind die öffentlichen Stellen im Sinne des § 2 mit Ausnahme der Wettbewerbsunternehmen, für die das Bundesdatenschutzgesetz gilt.

Die in Absatz 1 genannten Voraussetzungen gelten für alle Verarbeitungsschritte der Videoüberwachung. Für die zweckändernde Weiterverarbeitung sowie die Kennzeichnungs-, Informations- und Löschungspflichten enthalten die nachfolgenden Absätze 2 bis 4 zusätzliche Regelungen.

Im Gegensatz zu der bisherigen Regelung werden mit der Regelung in § 18 keine auf das konkrete Objekt bezogenen tatsächlichen Anhaltspunkte für eine Gefährdung mehr verlangt. Die Maßnahme muss zur Erfüllung öffentlicher Aufgaben oder zur Ausübung des Hausrechts erforderlich sein. Dies kann sowohl bei einer konkreten als auch einer abstrakten Gefährdungssituation zu bejahen sein. Die Erforderlichkeit ist aber im Einzelfall, das heißt bezogen auf das Überwachungsobjekt, zu prüfen. Eine rein generalisierende Betrachtung genügt daher nicht. Es müssen tatsächliche Anhaltspunkte bestehen, die den Schluss auf eine abstrakte oder konkrete Gefahrenlage für das einzelne Objekt zulassen. Zudem muss die Videoüberwachung im Einzelfall geeignetes und mildestes Mittel zur Gefahrenabwehr sein.

Ergibt eine Gefahrenprognose, die unter anderem auf der Grundlage von Erfahrungswerten erstellt werden kann, dass ein bestimmtes Gebäude oder eine bestimmte Kategorie von Gebäuden häufiger Angriffen ausgesetzt ist als andere Gebäude, kann dies für die Bejahung der Erforderlichkeit in diesem Sinne ausreichend sein.

Im Rahmen der Verhältnismäßigkeitsprüfung ist das Gewicht der im öffentlichen Interesse liegenden Aufgabe gegen die schutzwürdigen Interessen der betroffenen Personen abzuwägen. Die Videoüberwachung erfasst überwiegend Personen, die in keiner Beziehung zu einem konkreten Fehlverhalten stehen und den Eingriff durch ihr Verhalten nicht veranlasst haben. Dies stellt einen erheblichen Eingriff in das informationelle Selbstbestimmungsrecht des Einzelnen dar. Es ist daher wichtig, dass vor dem Einsatz einer Einrichtung zur Videoüberwachung sorgfältig geprüft wird, ob schutzwürdige Interessen der betroffenen Personen Videoüberwachungsmaßnahmen ausschließen. Da es sich um eine Ex-ante-Beurteilung handelt, ist diesbezüglich nach Anhaltspunkten zu fragen.

#### Zu Absatz 2

Die Kennzeichnungspflicht dient der Erfüllung des Transparenzgebots der Verordnung (EU) 2016/679. Am Ort der Videoüberwachung ist darüber zu informieren, dass eine Videoüberwachung erfolgt und der Verantwortliche anzugeben. Zum frühestmöglichen Zeitpunkt bedeutet, dass die Information möglichst vor dem Betreten videoüberwachter Bereiche erfolgt, damit die betroffene Person ihr Verhalten danach ausrichten kann.

Die sonstigen Angaben nach Artikel 13 der Verordnung (EU) 2016/679 sind der betroffenen Person zur Verfügung zu stellen, sobald die Aufnahme gespeichert und einer bestimmten Person zugeordnet wird.

#### Zu Absatz 3

Zusätzlich zu den Voraussetzungen des Absatz 1 wird die Zweckbindung geregelt. Ein Rückgriff auf andere Tatbestände zulässiger Zweckänderung nach § 5 ist ausgeschlossen. Die Regelungsbefugnis ergibt sich aus Artikel 6 Absatz 4 in Verbindung mit Artikel 23 Absatz 1 Buchstaben c und d der Verordnung (EU) 2016/679.

#### Zu Absatz 4

Diese Regelung hat nur klarstellende Funktion, da Artikel 13 und 14 der Verordnung (EU) 2016/679 direkt gelten.

## Zu Absatz 5

Die Regelung entspricht der bisherigen Regelung in § 20 a LDSG a. F. Sie steht im Einklang mit der Verordnung (EU) 2016/679.

Die Pflicht zur unverzüglichen Löschung, wenn die Daten zur Erfüllung des Zwecks, für den sie erhoben wurden, nicht mehr erforderlich sind, folgt aus Artikel 17 Absatz 1 Buchstabe a der Verordnung (EU) 2016/679. Diese Pflicht entfällt nur, wenn die Daten zur Verfolgung von erheblichen Ordnungswidrigkeiten oder Straftaten sowie zur Geltendmachung von Rechtsansprüchen benötigt werden.

Durch die Aufnahme einer Höchstspeicherfrist wird eine Regelung im Sinne des Artikels 6 Absatz 3 Satz 3 der Verordnung (EU) 2016/679 getroffen. Die gewählte Speicherfrist stellt sicher, dass Videoaufzeichnungen nicht bereits gelöscht sind, bevor sie ausgewertet werden können, was zur effektiven Aufgabenerfüllung der Sicherheits- und Strafverfolgungsbehörden notwendig ist. Anhaltspunkte für die Erfassung einer Straftäterin oder eines Straftäters können sich nämlich erst im Zuge weiterer Ermittlung und damit oft erst mehrere Tage nach der eigentlichen Tatbegehung ergeben. Die unverzügliche Löschungspflicht, wenn die Daten nicht mehr benötigt werden, soll hierdurch aber nicht unterlaufen werden.

Daneben wird für den Fall, dass die Daten für Zwecke der Verfolgung von Straftaten, Ordnungswidrigkeiten von erheblicher Bedeutung oder zur Geltendmachung von Rechtsansprüchen weiterhin benötigt werden, eine auch über die Höchstspeicherfrist hinausgehende Speicherung zugelassen. Damit wird die eigentlich bestehende Löschungspflicht eingeschränkt. Dies ist nach Artikel 17 Absatz 3 Buchstaben b und e der Verordnung (EU) 2016/679 zulässig.

## Zu Absatz 6

In Artikel 35 Absatz 3 Buchstabe c der Verordnung (EU) 2016/679 ist für die systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche eine Datenschutz-Folgeabschätzung vorgeschrieben, die gemäß Absatz 1 vorab vorzunehmen ist. In Absatz 6 wird eine weitere Mitteilungspflicht institutionalisiert, um in jedem Fall sicherzustellen, dass eine interne Vorabkontrolle unter Einbeziehung des jeweiligen Datenschutzbeauftragten stattfindet.

## Zu § 19 – Verarbeitung personenbezogener Daten zu künstlerischen und literarischen Zwecken

Entsprechend dem Regelungsauftrag in Artikel 85 der Verordnung (EU) 2016/679 wird eine Privilegierung für die Verarbeitung personenbezogener Daten zu künstlerischen und literarischen Zwecken geschaffen. Die Erstreckung des Medienprivilegs auf die künstlerische und literarische Betätigung gewährleistet zusammen mit den Regelungen zur Datenverarbeitung zu journalistischen Zwecken einen umfassenden Grundrechtsschutz der Meinungsfreiheit.

Auch den öffentlichen Stellen des Landes, die von dem Recht auf freie Meinungsäußerung und die Informationsfreiheit geschützte Tätigkeiten ausüben, sollen weitreichende Befreiungen von der Beachtung datenschutzrechtlicher Vorgaben gewährt werden. Die Verortung dieser Entscheidung im allgemeinen Datenschutzrecht dient dem Zweck, auch diejenigen Meinungsäußerungen abzudecken, die keinem der Anwendungsbereiche des Medien-Fachrechts zugeordnet werden können. Datenverarbeitungszwecke, die unter die Pressefreiheit fallen, beurteilen sich nach dem Landespressegesetz.

Die Regelung kommt unter anderen den öffentlich-rechtlich organisierten Theatertrieben zugute.

## Zu Absatz 1

Um das Recht auf freie Meinungsäußerung mit dem Schutz der personenbezogenen Daten in Einklang zu bringen, wird für die Datenverarbeitung zu künstlerischen und literarischen Zwecken wie für die Presse und den Rundfunk nur ein Teil der Verordnung (EU) 2016/679 für anwendbar erklärt, da insbesondere die künstlerische und literarische Betätigung mit den Anforderungen der Verordnung (EU) 2016/679 nicht vollends in Einklang zu bringen ist. Nur die dort genannten Vorschriften sind zu beachten, zu denen das in Artikel 6 der Verordnung (EU) 2016/679 normierte Verbot mit Erlaubnisvorbehalt nicht gehört.

Die Abweichungsbefugnisse ergeben sich aus Artikel 85 Absatz 2 der Verordnung (EU) 2016/679. Die betroffene Person wird nicht schutzlos gestellt, da ihr gemäß Artikel 77 der Verordnung (EU) 2016/679 ein Recht auf Beschwerde bei der Aufsichtsbehörde zusteht. Die Aufsicht wird durch die Landesbeauftragte für den Datenschutz oder den Landesbeauftragten für den Datenschutz ausgeübt. Diese oder dieser hat bezogen auf die Datenverarbeitung zu künstlerischen und literarischen Zwecken die Befugnisse nach der Verordnung (Artikel 58), allerdings beschränkt auf die Kontrolle der normierten Pflichten.

## Zu Absatz 2

Im Anwendungsbereich des Medienprivilegs würde das Recht auf freie Meinungsäußerung leerlaufen, wenn Berichtigungs- und Löschungsansprüche vollumfänglich zur Geltung gelangten. Das Recht auf informationelle Selbstbestimmung vermittelt gleichwohl einen Anspruch der betroffenen Person auf Vollständigkeit und Richtigkeit ihrer Daten. Ein Ausgleich dieser Interessen wird mit der Verpflichtung zur parallelen Aufbewahrung und Übermittlung erzielt.

## Zu Absatz 3

Dem Recht auf informationelle Selbstbestimmung wird durch das Auskunftsrecht Rechnung getragen.

## Zu Abschnitt 5 – Unabhängige Aufsichtsbehörden

## Zu §§ 20 bis 27

Abschnitt 5 passt die Regelungen des bisherigen Landesdatenschutzgesetzes zu dem Landesbeauftragten für den Datenschutz an die Vorgaben der Verordnung (EU) 2016/679 sowie der Richtlinie (EU) 2016/680 an. Im Einzelnen geregelt werden die Errichtung, die Zuständigkeit, die Unabhängigkeit, die Ernennung und Amtszeit, das Amtsverhältnis, die Rechte und Pflichten sowie die Aufgaben und Befugnisse. Wiederholende Regelungen aus der Verordnung (EU) 2016/679 werden aufgenommen, um der Umsetzung der Richtlinie (EU) 2016/680 zu genügen.

Nach dem bisherigen Landesdatenschutzgesetz ist die Dienststelle des Landesbeauftragten für den Datenschutz beim Landtag eingerichtet (§ 26 Absatz 3 LDSG a. F.). Die Verordnung (EU) 2016/679 sowie die Richtlinie (EU) 2016/680 normieren die völlige Unabhängigkeit der Aufsichtsbehörden (vgl. Artikel 52 Absatz 2 der Verordnung [EU] 2016/679, Artikel 42 Absatz 1 der Richtlinie [EU] 2016/680). Staatliche Aufsicht ist mit diesem Unabhängigkeitserfordernis nicht vereinbar, wie der Europäische Gerichtshof unter anderem in der Rechtssache C-518/07 vom 9. März 2010 entschieden hat.

Nach § 26 Absatz 3 Satz 3 LDSG a. F. untersteht der Landesbeauftragte für den Datenschutz „der Dienstaufsicht des Präsidenten des Landtags nur insoweit, als seine völlige Unabhängigkeit dadurch nicht beeinträchtigt wird“. Eine solche ein-

geschränkte Dienstaufsicht ist zwar möglicherweise mit der Verordnung (EU) 2016/679 konform, wenn sie europarechtskonform im Hinblick auf die eingeforderte völlige Unabhängigkeit ausgelegt wird. Sie ist in der Praxis aus diesem Grund mit hoher Wahrscheinlichkeit bedeutungslos und damit verzichtbar.

Zur Sicherstellung der völligen Unabhängigkeit wurde im Landesdatenschutzgesetz das Organisationsmodell der Alleinstellung als oberste Landesbehörde gewählt, da dieses besser geeignet ist, den rechtlichen Vorgaben der Verordnung (EU) 2016/679 gerecht zu werden als das Modell der parlamentarischen Anbindung. Es erlaubt den Aufbau einer klaren Organisationsstruktur im Sinne der Verordnung (EU) 2016/679 und vermeidet in der Praxis bedeutungslose und damit überflüssige Regelungen. Die Datenschutzaufsicht soll in Zukunft durch eine eigenständige Behörde wahrgenommen werden, welche nicht in die Verwaltungshierarchie der Landesverwaltung eingebunden ist.

Der demokratischen Legitimation der oder des Landesbeauftragten für den Datenschutz dienen die Befugnisse des Landtags zur Bestellung und Beendigung ihres oder seines Dienstverhältnisses sowie ein parlamentarisches Anfragerecht unmittelbar gegenüber der oder dem Landesbeauftragten für den Datenschutz.

In § 27 werden zudem die Regelungen für den Rundfunkbeauftragten für den Datenschutz des SWR an die Vorgaben der Verordnung (EU) 2016/679 angepasst.

Zu § 20 – Errichtung

Zu Absatz 1

Die oder der Landesbeauftragte für den Datenschutz wird als oberste Landesbehörde eingerichtet, um die größtmögliche Unabhängigkeit, insbesondere die Dienstherreneigenschaft, zu gewährleisten. Die bisherige Dienstbezeichnung und der Dienstsitz werden beibehalten. Unabhängigkeit bedeutet insbesondere Weisungsfreiheit und ist durch die Verordnung (EU) 2016/679 und die Richtlinie (EU) 2016/680 angeordnet.

Zu Absatz 2

Die Personalhoheit obliegt im Hinblick auf die Unabhängigkeit der Aufsichtsbehörde ausschließlich der oder dem Landesbeauftragten für den Datenschutz. Diese oder dieser ist damit Dienstvorgesetzte oder Dienstvorgesetzter ihrer oder seiner Beamtinnen und Beamten sowie oberste Disziplinarbehörde und gegenüber ihren oder seinen Beschäftigten ausschließlich weisungsbefugt.

Zu Absatz 3

Absatz 3 schafft eine Rechtsgrundlage für die Übertragung von Aufgaben der Personalverwaltung und Personalwirtschaft von der oder dem Landesbeauftragten für den Datenschutz auf andere Behörden und die damit einhergehende Übermittlungsbefugnis für die Beschäftigtendaten. Es handelt sich um eine Funktionsübertragung, da das Instrument der Auftragsdatenverarbeitung wegen des selbstständigen Charakters der Aufgabenerledigung nicht in Betracht kommt. Betroffen sind beispielsweise Aufgaben der Reisekostenabrechnung, Gewährung von Trennungsgeld und Umzugskostenerstattung, Geltendmachung von Schadensersatzansprüchen gegenüber Dritten oder Unterstützung bei Stellenbesetzungsverfahren.

## Zu § 21 – Unabhängigkeit

## Zu Absatz 1

Sowohl die Verordnung (EU) 2016/679 (Artikel 52 Absätze 1 und 2) als auch die Richtlinie (EU) 2016/680 (Artikel 42 Absätze 1 und 2) schreiben die völlige Unabhängigkeit der Aufsichtsbehörde fest und konkretisieren diese.

## Zu Absatz 2

Absatz 2 trägt Artikel 52 Absatz 6 Satz 1, erster Satzteil der Verordnung (EU) 2016/679 sowie Artikel 42 Absatz 6, erster Satzteil der Richtlinie (EU) 2016/680 Rechnung. Die Finanzkontrolle findet aber dort ihre Grenze, wo die Unabhängigkeit der Aufsichtsbehörde beeinträchtigt wird.

## Zu Absatz 3

Das Fragerecht der Parlamentarier stärkt die demokratische Legitimation der oder des Landesbeauftragten für den Datenschutz.

## Zu § 22 – Ernennung und Amtszeit

## Zu Absatz 1

Die bisherige Regelung der Wahl durch das Parlament wird beibehalten, da sie die Voraussetzungen der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 zur Ernennung (Artikel 53 Absatz 1, 54 Absatz 1 Buchstabe c der Verordnung [EU] 2016/679 sowie Artikel 43 Absatz 1, 44 Absatz 1 Buchstabe c der Richtlinie [EU] 2016/680) erfüllt. Das Vorschlagsrecht verbleibt bei der Landesregierung. Die Verordnung (EU) 2016/679 oder Richtlinie (EU) 2016/680 sieht auch eine Ernennung durch die Landesregierung als zulässig an (Artikel 53 Absatz 1 der Verordnung [EU] 2016/679, 43 Absatz 1 der Richtlinie [EU] 2016/680). Die Landesregierung kann daher europarechtlich nicht daran gehindert sein, einen Vorschlag zur Wahl vorzulegen.

Die erforderlichen Qualifikationen für das Amt der oder des Landesbeauftragten für den Datenschutz müssen gemäß Artikel 54 Absatz 1 Buchstabe b der Verordnung (EU) 2016/679 sowie Artikel 44 Absatz 1 Buchstabe b der Richtlinie (EU) 2016/680 durch Rechtsvorschrift festgelegt werden. Inhaltlich fordern Artikel 53 Absatz 2 der Verordnung (EU) 2016/679 sowie Artikel 43 Absatz 2 der Richtlinie (EU) 2016/680 zusätzlich fachbezogene Qualifikationen, nämlich Erfahrung und Sachkunde im Bereich des Schutzes personenbezogener Daten.

## Zu Absatz 2

Die Regelung beruht auf Artikel 54 Absatz 2 Buchstabe c der Verordnung (EU) 2016/679 und Artikel 44 Absatz 1 Buchstabe c der Richtlinie (EU) 2016/680. Die Ernennung durch die Landtagspräsidentin oder den Landtagspräsidenten und die Verpflichtung vor dem Landtag stellen die Unabhängigkeit von der Landesregierung sicher.

## Zu Absatz 3

Die Regelung erfolgt zur Ausfüllung von Artikel 54 Absatz 1 Buchstabe e der Verordnung (EU) 2016/679 und Artikel 44 Absatz 1 Buchstabe e der Richtlinie

(EU) 2016/680. Die bisherige Beschränkung auf einmalige Wiederwahl wird zugunsten einer zweimaligen Wiederwahl aufgegeben.

Zu § 23 – Amtsverhältnis

Zu Absatz 1

Wegen der Unabhängigkeit der oder des Landesbeauftragten für den Datenschutz handelt es sich um ein öffentlich-rechtliches Amtsverhältnis sui generis.

Zu Absatz 2

Die Voraussetzungen für eine Amtsenthebung sind wortgleich in Artikel 53 Absatz 4 der Verordnung (EU) 2016/679 und Artikel 43 Absatz 4 der Richtlinie (EU) 2016/680 geregelt. In Entsprechung zur Ernennung wird auch die Amtsenthebung bei Vorliegen der Voraussetzungen durch die Landtagspräsidentin oder den Landtagspräsidenten vorgenommen. Da die Amtsenthebung außer bei dem Wegfall der Voraussetzungen der Amtswahrnehmung nach der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 nur bei Begehung einer schweren Verfehlung vorgenommen werden darf, ist hierdurch zugleich die ordnungsgemäße Durchführung eines Verwaltungsverfahrens gewährleistet. Die Amtsenthebung bedarf der Zustimmung von zwei Dritteln der Mitglieder des Landtags, um einerseits dem Landtag als Wahlorgan ein Mitspracherecht einzuräumen und durch das hohe Quorum andererseits aber eine Amtsenthebung allein aus politischen Gründen zu verhindern.

Zu Absatz 3

Mit der Vertretungsregelung wird in zweckmäßiger Weise die Funktionsfähigkeit und Aufgabenerfüllung bei Verhinderung oder nach Beendigung des Amtsverhältnisses der oder des Landesbeauftragten für den Datenschutz bis zur Bestellung eines neuen Amtsinhabers gewährleistet.

Zu Absatz 4

Hier werden die Bezüge und sonstigen finanziellen Leistungen geregelt, welche die oder der Landesbeauftragte für den Datenschutz erhält. Diese Regelung ist erforderlich, da die oder der Landesbeauftragte für den Datenschutz nach Absatz 1 keine Beamtin oder kein Beamter mehr ist und somit nicht mehr dem Geltungsbereich der für Beamte maßgeblichen Vorschriften unterfällt. Es handelt sich um eine notwendige mitgliedstaatliche Begleitvorschrift zur Errichtung der Aufsichtsbehörden und des Verfahrens für die Ernennung der Leiterin oder des Leiters der Aufsichtsbehörde (vgl. Artikel 54 Absatz 1 Buchstaben a und c der Verordnung [EU] 2016/679 und Artikel 44 Absatz 1 Buchstaben a und c der Richtlinie [EU] 2016/680).

Zu § 24 – Rechte und Pflichten

Zu Absatz 1

Satz 1 enthält ein umfassendes Verbot sämtlicher nicht mit dem Amt zu vereinbarenden Handlungen und Tätigkeiten, gleich ob entgeltlich oder unentgeltlich. Der Wortlaut ist Artikel 52 Absatz 3 der Verordnung (EU) 2016/679 und Artikel 42 Absatz 3 der Richtlinie (EU) 2016/680 entnommen. Sätze 2 und 3 konkretisieren dieses allgemeine Verbot im Sinne des Artikels 54 Absatz 1 Buchstabe f der Ver-

ordnung (EU) 2016/679 sowie des Artikels 44 Absatz 1 Buchstabe f der Richtlinie (EU) 2016/680.

Zu Absatz 2

Die Mitteilungspflicht der oder des Landesbeauftragten für den Datenschutz über Geschenke ist eine Konkretisierung der aus Artikel 52 Absatz 3 und Artikel 54 Absatz 1 Buchstabe f der Verordnung (EU) 2016/679 und Artikel 42 Absatz 3 und Artikel 44 Absatz 1 Buchstabe f der Richtlinie (EU) 2016/680 folgenden mitgliedstaatlichen Regelungsspielräume zu den Pflichten und Handlungsverboten.

Zu Absatz 3

Die Verschwiegenheitspflicht ist in Ausgestaltung der Artikel 54 Absatz 2 der Verordnung (EU) 2016/679 und Artikel 44 Absatz 2 der Richtlinie (EU) 2016/680 geregelt. Das Zeugnisverweigerungsrecht ist in § 13 Absatz 6 in Verbindung mit Absatz 3 des Bundesdatenschutzgesetzes auch für die Aufsichtsbehörden der Länder geregelt.

Zu Absatz 4

Artikel 54 Absatz 1 Buchstabe f der Verordnung (EU) 2016/679 sowie Artikel 44 Absatz 1 Buchstabe f der Richtlinie (EU) 2016/680 verpflichtet die Mitgliedstaaten dazu, Verbote von Handlungen, beruflichen Tätigkeiten und Vergütungen der oder des Landesbeauftragten für den Datenschutz und ihrer oder seiner Bediensteten, die mit den Pflichten unvereinbar sind, auch nach der Amtszeit zu regeln. Von eigenen Regelungen für die Bediensteten der Aufsichtsbehörde wird abgesehen, da die beamtenrechtlichen Regelungen, insbesondere die Verschwiegenheitspflicht, diesbezüglich ausreichen.

Zu Absatz 5

Das Recht zur Zeugenaussage steht in unmittelbarem Bezug zu dem Zeugnisverweigerungsrecht in § 13 des Bundesdatenschutzgesetzes und der Verschwiegenheitspflicht der oder des Landesbeauftragten für den Datenschutz in Absatz 2.

Zu § 25 – Aufgaben und Befugnisse

Zu Absatz 1

In Absatz 1 erfolgt die allgemeine Aufgabenzuweisung für die Aufgabe als unabhängige Aufsichtsbehörde für die öffentlichen Stellen des Landes im Bereich der Verordnung (EU) 2016/679 sowie für den Datenschutz im nichtöffentlichen Bereich bei privaten Stellen an die Landesbeauftragte für den Datenschutz oder den Landesbeauftragten für den Datenschutz. Eine andere Aufsichtszuständigkeit ist für den SWR und seine Beteiligungsunternehmen in § 27 sowie für den privaten Rundfunk bezüglich der Datenverarbeitung zu eigenen journalistischen Zwecken in § 50 Absatz 3 Landesmediengesetz geregelt.

Zu Absatz 2

Die Aufgaben und Befugnisse der oder des Landesbeauftragten für den Datenschutz, ergeben sich aus Artikel 57 und 58 der Verordnung (EU) 2016/679. Ein Regelungsbedarf besteht nur insofern, als öffentliche Stellen nur aufgrund § 2 Absatz 4 die Verordnung (EU) 2016/679 anzuwenden haben. Insoweit wird die oder

der Landesbeauftragte für den Datenschutz ermächtigt, ebenfalls die Aufgaben gemäß Artikel 57 wahrzunehmen und die Befugnisse gemäß Artikel 58 der Verordnung (EU) 2016/679 auszuüben. Die Befugnisse werden gegenüber der öffentlichen Stelle ausgeübt.

Die Zuweisung der Aufgaben und Befugnisse für die Aufsicht der oder des Landesbeauftragten für den Datenschutz über die öffentlichen Stellen, die der Richtlinie (EU) 2016/680 unterliegen, erfolgt nicht in diesem Gesetz, sondern in den Gesetzen, die die Richtlinie (EU) 2016/680 umsetzen.

#### Zu Absatz 3

Die Regelung wird aus § 27 Absatz 1 LDSG a. F. fortgeführt. Sie konkretisiert Artikel 77 der Verordnung (EU) 2016/679 und enthält ein ausdrückliches Benachteiligungsverbot.

#### Zu Absatz 4

Absatz 4 enthält Verfahrensvorschriften im Sinne des Artikels 58 Absatz 4 der Verordnung (EU) 2016/679. Danach erfolgt die Ausübung der den Aufsichtsbehörden übertragenen Befugnisse vorbehaltlich geeigneter Garantien, einschließlich ordnungsgemäßer Verfahren gemäß dem Unionsrecht und dem Recht der Mitgliedsstaaten. Die bisherigen Regelungen des § 30 LDSG a. F. werden aufgegriffen und modifiziert.

Hierdurch wird sichergestellt, dass von der oder dem Landesbeauftragten für den Datenschutz festgestellte Verstöße gegen die Vorschriften des Datenschutzes der jeweils zuständigen Rechts- oder Fachaufsichtsbehörde bzw. dem vertretungsberechtigten Organ mitgeteilt werden und diese vor der Ausübung der aufgezählten Abhilfebefugnisse des Artikels 58 Absatz 2 der Verordnung (EU) 2016/679 unter Setzung einer angemessenen Frist Gelegenheit zur Stellungnahme erhalten. Bei den übrigen Abhilfebefugnissen des Artikels 58 Absatz 2 der Verordnung (EU) 2016/679 besteht hingegen kein Bedarf an einer vorherigen Information der Rechts- oder Fachaufsichtsbehörde. Durch die Mitteilung wird insbesondere gewährleistet, dass die zuständige Rechts- oder Fachaufsichtsbehörde Kenntnis von dem Verstoß erhält und vor der Ausübung weiterer Befugnisse durch die Landesbeauftragte für den Datenschutz oder den Landesbeauftragten für den Datenschutz Anspruch auf rechtliches Gehör findet. Die Gefahr divergierender Anweisungen zwischen Datenschutzaufsicht und Rechts- oder Fachaufsicht wird hierdurch reduziert. Widersprüchliche Auffassungen der Datenschutzaufsicht und der Rechts- oder Fachaufsicht sind auf dem Gerichtsweg zu klären. Widerspricht die Verfügung der oder des Landesbeauftragten für den Datenschutz der Rechtsauffassung der Rechts- oder Fachaufsichtsbehörde, kann diese den Verantwortlichen zur gerichtlichen Klärung anweisen.

Bei Gefahr im Verzug oder entgegenstehenden zwingenden öffentlichen Interessen kann von der Einräumung der Gelegenheit zur Stellungnahme abgesehen werden.

#### Zu Absatz 5

Die Regelung führt § 28 Absatz 2 Satz 1 LDSG a. F. bezüglich der Kontrolle der öffentlichen Stellen im Wesentlichen fort. Für die Kontrolle nichtöffentlicher Stellen ist § 29 Absatz 3 des Bundesdatenschutzgesetzes zu beachten. Wegen ihrer Verschwiegenheitspflicht nach § 18 der Bundesnotarordnung sollen die Notarinnen und Notare des Landes den Rechtsanwältinnen und Rechtsanwälten gleichgestellt werden. Satz 3 verlängert die Geheimhaltungspflicht auf die Aufsichtsbehörde.

## Zu § 26 – Pflicht zur Unterstützung

## Zu Absatz 1

In Absatz 1 werden die gemäß Artikel 58 Absatz 1 Buchstabe f der Verordnung (EU) 2016/679 zur Ausübung der Untersuchungsbefugnisse notwendigen Verfahrensvorschriften für die Zugangs- und Einsichtsrechte geregelt. Die Vorschrift entspricht § 29 Absatz 1 LDSG a. F.

## Zu Absatz 2

Diese Verpflichtung sichert die rechtzeitige datenschutzrechtliche Prüfung aller landesrechtlichen datenschutzrechtlichen Vorschriften, auch der untergesetzlichen.

## Zu § 27 – Rundfunkbeauftragte oder Rundfunkbeauftragter für den Datenschutz

## Zu Absatz 1

Bereits bislang bestellt der SWR entsprechend § 39 SWR-Staatsvertrag einen unabhängigen Rundfunkbeauftragten für den Datenschutz.

Gegenüber dem bisherigen § 38 LDSG a. F. wurde die Klarstellung vorgenommen, dass sich die Kontrolle auf alle Tätigkeiten des SWR und seiner Beteiligungsunternehmen im Sinne des § 16 c Absatz 3 Satz 1 des Rundfunkstaatsvertrages, das heißt auf solche Unternehmen des Privatrechts, an denen der SWR unmittelbar, mittelbar, auch zusammen mit anderen Anstalten oder Körperschaften des öffentlichen Rechts mit Mehrheit beteiligt ist, erstreckt und er in Bezug auf diese die Funktion der Aufsichtsbehörde im Sinne von Artikel 51 der Verordnung (EU) 2016/679 wahrnimmt. Entsprechender Regelungen in den Gesellschaftsverträgen oder Satzungen bedarf es für die Zuständigkeit der oder des Rundfunkbeauftragten für den Datenschutz hingegen nicht.

Die Wahrnehmung der Prüfkompetenz für die erwähnten Beteiligungsgesellschaften durch die jeweilige Rundfunkbeauftragte oder den jeweiligen Rundfunkbeauftragten für den Datenschutz soll sich nach der bisherigen Praxis des Arbeitskreises der Rundfunkdatenschutzbeauftragten richten. Als Ausgangspunkt soll im Grundsatz die Federführung beim Sitzland liegen bei einer Pflicht zur Zusammenarbeit beziehungsweise Beteiligung der ebenfalls betroffenen Aufsichtsbehörden. Einzelfragen sollen im Arbeitskreis der Rundfunkdatenschutzbeauftragten Klärung finden.

Als spezifische Aufsichtsbehörde im Sinne von § 18 Absatz 1 Satz 4 des Bundesdatenschutzgesetzes ist die oder der Rundfunkbeauftragte für den Datenschutz von den Aufsichtsbehörden des Bundes und der Länder zu beteiligen, sofern sie von einer Angelegenheit betroffen ist.

Die Amtszeit soll an die Amtszeit der oder des Landesbeauftragten für den Datenschutz angeglichen werden und nunmehr sechs Jahre betragen. Die Ernennung durch Rundfunkrat und Verwaltungsrat soll beibehalten werden, um die Unabhängigkeit der oder des Rundfunkbeauftragten für den Datenschutz zu sichern und genügt den Anforderungen des Artikels 53 Absatz 1 Verordnung (EU) 2016/679. Im Hinblick auf die Terminologie der Verordnung (EU) 2016/679 wird nunmehr statt von „Bestellung“ von „Ernennung“ gesprochen.

Im Hinblick auf Artikel 54 Absatz 1 Buchstabe e der Verordnung (EU) 2016/679 wird die zweimalige Möglichkeit der Wiederernennung gesetzlich festgelegt. Mit einer dann möglichen Amtszeit von insgesamt 18 Jahren wird die Unabhängigkeit der oder des Rundfunkbeauftragten für den Datenschutz gestärkt. Die Kontinuität bei der Führung des Amtes wird gewährleistet.

## Zu Absatz 2

Die Regelungen in Absatz 2 entsprechen Artikel 53 Absatz 2 der Verordnung (EU) 2016/679. Als erforderliche Qualifikation im Sinne von Artikel 54 Absatz 1 Buchstabe b der Verordnung (EU) 2016/679 wird ein abgeschlossenes Hochschulstudium gesetzlich festgelegt.

## Zu Absatz 3

Absatz 3 konkretisiert die in Artikel 52 Absatz 3 bis 6 der Verordnung (EU) 2016/679 aufgestellten Anforderungen an die Rundfunkbeauftragte für den Datenschutz oder den Rundfunkbeauftragten für den Datenschutz, um ihre oder seine Unabhängigkeit zu gewährleisten. Zu den in einer Satzung zu veröffentlichenden Grundsätzen der Vergütung zählen objektive Parameter und Gehaltsbestandteile. Das konkrete Gehalt ist nicht anzugeben.

Zur Ausgestaltung der Rechtsnatur des Amtsverhältnisses werden keine gesetzlichen Vorgaben getroffen. Entscheidend ist, dass die oder der Rundfunkbeauftragte für den Datenschutz über eine unabhängige Stellung im Sinne des Artikels 52 Absatz 1 der Verordnung (EU) 2016/679 verfügt.

## Zu Absatz 4

In Absatz 4 Satz 1 wird eine Regelung zu Artikel 52 Absatz 3 der Verordnung (EU) 2016/679 getroffen. Um ihre oder seine unabhängige Stellung innerhalb des SWR sicherzustellen, soll die oder der Rundfunkbeauftragte für den Datenschutz keine anderen Aufgaben innerhalb des SWR und seiner Beteiligungs- und Hilfsunternehmen wahrnehmen. Sonstige Aufgaben, also Aufgaben außerhalb des SWR und seiner Beteiligungs- und Hilfsunternehmen müssen mit dem Amt der oder des Rundfunkbeauftragten für den Datenschutz vereinbar sein und dürfen ihre oder seine Unabhängigkeit nicht gefährden. Wann dies der Fall ist, bedarf der Prüfung im Einzelfall.

Darüber hinaus enthält Absatz 4 entsprechend Artikel 53 Absatz 3 der Verordnung (EU) 2016/679 eine in § 38 LDSG a. F. bisher fehlende Regelung zur Beendigung des Amtes, ferner die Zuständigkeitsregelung für den Fall einer Amtsenthebung wegen einer schweren Verfehlung entsprechend Artikel 53 Absatz 4 der Verordnung (EU) 2016/679.

Eine gesetzliche Regelung zum Fortbestand der Amtszeit auch unter Geltung der Verordnung (EU) 2016/679 erfolgt nicht. Aufgrund des Grundsatzes der Staatsferne ist es Angelegenheit des SWR über den Fortbestand der Amtszeit zu befinden.

## Zu Absatz 5

Die Finanzkontrolle soll durch den Verwaltungsrat und nicht durch den Rechnungshof erfolgen. Eine Dienstaufsicht ist wie bei der oder dem Landesbeauftragten für den Datenschutz nicht mehr vorgesehen.

Entsprechend der Regelung für die Landesbeauftragte für den Datenschutz oder den Landesbeauftragten für den Datenschutz wurde aufgenommen, dass Gremienmitglieder des Rundfunk- und des Verwaltungsrats Anfragen an die Rundfunkbeauftragte für den Datenschutz oder den Rundfunkbeauftragten für den Datenschutz richten können.

## Zu Absatz 6

Diese Regelung entspricht im Wesentlichen § 38 Absatz 3 LDSG a. F.

## Zu Absatz 7

Der oder dem Rundfunkbeauftragten für den Datenschutz stehen grundsätzlich dieselben Aufgaben und Befugnisse wie der oder dem Landesbeauftragten für den Datenschutz zu. Besonderheiten bei der Aufsicht über die Datenverarbeitung zu journalistischen Zwecken sind zu beachten. Die Regelung stellt im Übrigen eine Verfahrensregelung gemäß Artikel 58 Absatz 4 der Verordnung (EU) 2016/679 zur Ausübung der Befugnisse dar. Die Einschränkung der Befugnis zur Verhängung eines Bußgelds gegen den SWR ist gemäß Artikel 83 Absatz 7 der Verordnung (EU) 2016/679 zulässig und erfolgt parallel zu der Einschränkung in § 28 gegen Behörden und öffentliche Stellen.

## Zu Absatz 8

In Absatz 8 wird eine Regelung zu Artikel 54 Absatz 1 Buchstabe f in Verbindung mit Artikel 52 Absatz 3 der Verordnung (EU) 2016/679 getroffen. Welche Tätigkeit nach Beendigung des Amtes mit der Tätigkeit als Rundfunkbeauftragte oder Rundfunkbeauftragter für den Datenschutz vereinbar ist, bedarf der Prüfung im Einzelfall.

## Zu Absatz 9

Die Verschwiegenheitspflicht gemäß Artikel 54 Absatz 2 der Verordnung (EU) 2016/679 gilt auch für die Rundfunkbeauftragte für den Datenschutz oder den Rundfunkbeauftragten für den Datenschutz. Sie wird erweitert um eine Pflicht zum Informantenschutz im journalistischen Bereich für die Zusammenarbeit mit anderen Aufsichtsbehörden, die sich aus Kapitel VII der Verordnung (EU) 2016/679 ergibt.

## Zu Absatz 10

Die in § 38 Absatz 5 LDSG a. F. enthaltene Berichtspflicht soll beibehalten werden, wobei entsprechend Artikel 59 der Verordnung (EU) 2016/679 ein Jahresbericht zu erstatten ist. Der Bericht ist zu veröffentlichen und ist den Landtagen und den Landesregierungen der unterzeichnenden Länder des SWR-Staatsvertrags, das sind Baden-Württemberg und Rheinland-Pfalz, zu übermitteln.

## Zu Abschnitt 6 – Sanktionen

## Zu § 28 – (Ergänzung zu Artikel 83 Absatz 7 der Verordnung [EU] 2016/679) – Ordnungswidrigkeiten

Die Vorschrift bezieht sich auf die Bußgeldvorschrift des Artikels 83 der Verordnung (EU) 2016/679. Es wird von der Öffnungsklausel des Artikels 83 Absatz 7 der Verordnung (EU) 2016/679 Gebrauch gemacht, um zu regeln, dass gegen Behörden und sonstige öffentliche Stellen keine Geldbußen verhängt werden können. Dies gilt jedoch nicht für öffentliche Stellen gemäß § 2 Absatz 6, die im Rahmen ihrer Tätigkeit im Wettbewerb mit anderen Verarbeitern stehen, da sie gegenüber ihren Wettbewerbern nicht bessergestellt werden sollen.

Im Übrigen sind die Bußgeldtatbestände abschließend in der Verordnung (EU) 2016/679 geregelt.

Zu § 29 – (Ergänzung zu Artikel 84 der Verordnung [EU] 2016/679) – Strafvorschrift

Zu Absatz 1

Artikel 84 der Verordnung (EU) 2016/679 berechtigt und verpflichtet die Mitgliedstaaten, „andere Sanktionen“ für Verstöße gegen die Verordnung festzulegen. Artikel 84 ist damit insbesondere eine Öffnungsklausel, um neben Geldbußen nach Artikel 83 der Verordnung (EU) 2016/679 strafrechtliche Sanktionen vorzusehen. Hiervon wird Gebrauch gemacht.

Zu Absatz 2

Mit dieser Vorschrift wird insofern ein Gleichlauf zum neugeregelten Bundesdatenschutzgesetz hergestellt, als die Tat nur auf Antrag verfolgt wird und die bisherige Versuchsstrafbarkeit entfällt.

Zu Abschnitt 7 – Übergangsbestimmungen

Zu § 30 – Polizeibehörden und Polizeivollzugsdienst, Justizbehörden, Landesamt für Verfassungsschutz und Vollzug des Landessicherheitsüberprüfungsgesetzes

Zu Absatz 1

Um ein lückenloses Datenschutzrecht zu gewährleisten, ist es erforderlich, die Geltung des bisherigen Landesdatenschutzgesetzes für die Polizeibehörden und den Polizeivollzugsdienst aufrechtzuerhalten, bis die Richtlinie (EU) 2016/680 in Landesrecht umgesetzt ist. Denn das Polizeigesetz verweist in seinen datenschutzrechtlichen Vorschriften (§ 48 Polizeigesetz) ergänzend auf das bisherige Landesdatenschutzgesetz. Der Gesetzgeber ist hierzu befugt, soweit die Verordnung (EU) 2016/679 nicht für die Polizeibehörden und den Polizeivollzugsdienst gilt, das heißt im Anwendungsbereich der Richtlinie (EU) 2016/680.

Zu Absatz 2

Auch die Verarbeitung personenbezogener Daten zu den Zwecken nach Artikel 1 Absatz 1 der Richtlinie (EU) 2016/680 durch die in Absatz 2 genannten Stellen fällt nicht in den Anwendungsbereich der Verordnung (EU) 2016/679. Dementsprechend ist auch insoweit die Fortgeltung des bisherigen Landesdatenschutzgesetzes vorzusehen, bis die Richtlinie (EU) 2016/680 in Landesrecht umgesetzt ist.

Zu Absatz 3

Auch für den Fall der Verarbeitung personenbezogener Daten durch das Landesamt für Verfassungsschutz im Rahmen der Erfüllung seiner Aufgaben nach § 3 des Landesverfassungsschutzgesetzes und beim Vollzug des Landessicherheitsüberprüfungsgesetzes ist die Geltung des bisherigen Landesdatenschutzgesetzes zunächst aufrechtzuerhalten. Sonst ist der Datenschutz nicht lückenlos gewährleistet, bis mit dem Gesetz zur Änderung des Landesverfassungsschutzgesetzes und anderer Gesetze die notwendigen datenschutzrechtlichen Folgeänderungen in diesen Bereichen in Kraft treten. Das Landesverfassungsschutzgesetz verweist ergänzend auf die Vorschriften des bisherigen Landesdatenschutzgesetzes, soweit es keine Regelungen trifft. Das Landessicherheitsüberprüfungsgesetz verweist für die Verarbeitung personenbezogener Daten durch die mitwirkende Behörde ergänzend auf das Landesverfassungsschutzgesetz. Über § 5 Absatz 1 Landesverfassungsschutzgesetz gilt daher ergänzend auch das Landesdatenschutzgesetz.

## Zu § 31 – Überleitungsvorschriften

## Zu Absatz 1

Nach § 26 LDSG a. F. befindet sich der Landesbeauftragte für den Datenschutz in einem Beamtenverhältnis auf Zeit. Infolge dieses Gesetzes wird das Amt der oder des Landesbeauftragten für den Datenschutz als ein öffentlich-rechtliches Amtsverhältnis gestaltet. Infolgedessen muss der Status und der Beginn der laufenden Amtszeit der oder des bei Inkrafttreten dieses Gesetzes amtierenden Landesbeauftragten für den Datenschutz durch das Gesetz klargestellt werden. Die sechsjährige Amtszeit nach § 26 Absatz 1 Satz 3 LDSG a. F. hat mit der Wahl und der darauf folgenden Berufung in das Amt des Landesbeauftragten für den Datenschutz begonnen. Ihr Ablauf wird durch den Wechsel des Amtsverhältnisses nicht berührt. Die zum 1. Januar 2017 begonnene Amtszeit des derzeitigen Amtsinhabers endet daher mit Ablauf des Jahres 2022. Das Amt kann ab Januar 2023 nur nach einer Wiederwahl gemäß § 22 entsprechend den getroffenen Regelungen fortgeführt werden.

## Zu Absatz 2

Erforderlich sind ferner Vorschriften zur Überleitung des Personals des Landesbeauftragten für den Datenschutz, das bisher beim Landtag ressortiert. Damit gehen alle Beschäftigten beim Landtag, die dem Landesbeauftragten für den Datenschutz bei Inkrafttreten der Neuregelungen organisatorisch zuzurechnen sind, auf die neue Behörde des Landesbeauftragten für den Datenschutz über. Dies betrifft zum Beispiel auch solche Beschäftigten, die aus einer Tätigkeit bei dem Landesbeauftragten für den Datenschutz beurlaubt sind oder wegen Abordnung in der Behörde derzeit keinen Dienst leisten.

## Zu Absatz 3

Mit dieser Regelung wird gewährleistet, dass die neue oberste Landesbehörde des Landesbeauftragten für den Datenschutz über einen funktionierenden Personalrat verfügt, bis die reguläre Neuwahl des Personalrats in 2019 stattfindet.

## Zu Artikel 2 – Änderung des Landesverwaltungsgesetzes

## Zu Nummer 1

Als oberste Landesbehörde wird der Landesbeauftragte für den Datenschutz nach den Ministerien und dem Rechnungshof eingefügt.

## Zu Nummer 2

Die Gesetzesänderungen tragen der besonderen unabhängigen und europarechtlich geprägten Stellung des Landesbeauftragten für den Datenschutz Rechnung.

## Zu Nummer 3

## Folgeänderung zu Nummer 2

## Zu Nummer 4

Wegen der europarechtlichen Unabhängigkeit des Landesbeauftragten für den Datenschutz kann die Landesregierung keine Verwaltungsvorschriften für diesen

erlassen. Dies ist hier klarzustellen, da der Landesbeauftragte für den Datenschutz aufgrund dieses Gesetzes als oberste Landesbehörde eingerichtet wird.

#### Zu Artikel 3 – Änderung des Landesbesoldungsgesetzes Baden-Württemberg

Es handelt es sich um eine Folgeregelung zu Artikel 1, § 23 Absatz 1.

#### Zu Artikel 4 – Änderung des Ernennungsgesetzes

Als unabhängiger oberster Landesbehörde kommt der oder dem Landesbeauftragten für den Datenschutz die Personalhoheit zu. Diese umfasst das Recht, ihre oder seine Beamtinnen und Beamte zu ernennen.

Der oder dem Landesbeauftragten für den Datenschutz wird daher wie den Ministerien und dem Präsidenten des Rechnungshofs das Recht zur Ernennung und den damit verbundenen Rechten verliehen. Die Unabhängigkeit nach der Verordnung (EU) 2016/679 (vgl. Artikel 52 Absatz 5), gebietet es nicht, dass die oder der Landesbeauftragte für den Datenschutz diese Rechte für alle in seiner Behörde tätigen Beamtinnen und Beamten unabhängig von der Besoldungsstufe ausübt. Dieses Recht bleibt, wie auch für die Ministerien und den Rechnungshof, ab der Besoldungsgruppe A 15 nach Artikel 51 der Landesverfassung dem Ministerpräsidenten vorbehalten. Dadurch wird die Gleichbehandlung aller Landesbeamten gewährleistet.

Die Vorschrift weicht ab von Artikel 51 Satz 1 der Landesverfassung. Die gesetzliche Übertragung des Ernennungsrechts auf andere Behörden ist aber nach Artikel 51 Satz 2 der Landesverfassung zulässig.

#### Zu Artikel 5 – Änderung des Landesinformationsfreiheitsgesetzes

Nach Artikel 86 der Verordnung (EU) 2016/679 können personenbezogene Daten in amtlichen Dokumenten offengelegt werden, um den Zugang der Öffentlichkeit zu amtlichen Dokumenten mit dem Recht auf Schutz personenbezogener Daten gemäß der Verordnung (EU) 2016/679 in Einklang zu bringen. Dazu wird der Kreis der sensiblen Informationen in § 5 Absatz 2 LIFG an die Neuregelung in Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 angepasst. Im Übrigen werden die Verweisungen auf das außerkrafttretende Landesdatenschutzgesetz durch solche auf die Verordnung (EU) 2016/679 oder durch eine der bisherigen Rechtslage entsprechende Vollregelung ersetzt.

#### Zu Nummer 1

Der bislang im Landesinformationsfreiheitsgesetz verwendete Begriff der betroffenen Person ist nunmehr in Artikel 4 Nummer 1 der Verordnung (EU) 2016/679 ausdrücklich enger definiert, sodass davon nur noch natürliche Personen umfasst sind. Die Terminologie im Landesinformationsfreiheitsgesetz wird daran angepasst und anstatt des bisher im Landesinformationsfreiheitsgesetz verwendeten Begriffs der betroffenen Person tritt der Begriff der geschützten Person, welcher natürliche und juristische Personen umfasst.

#### Zu Nummer 2

Die Bestimmung, welche Behörden als Finanz-, Regulierungs-, Sparkassen-, Versicherungs- oder Wettbewerbsaufsichtsbehörden zu bewerten sind, bereitet in der Praxis teilweise erhebliche Schwierigkeiten. Insbesondere der Begriff der Regulierung wird sehr unterschiedlich interpretiert (in diesem Sinne: Debus, in: ders., Informationszugangsrecht Baden-Württemberg, 2017, § 4 LIFG Rn. 39, sowie

zum Bundesrecht auch: Schirmer, in: Gersdorf/Paal, Informations- und Medienrecht, 2014, § 3 IFG Rn. 74; Schoch, IFG, 2. Aufl. 2016, § 3 Rn. 82 f.). Umstritten ist auch, ob und welche Behörden neben den Kartellbehörden noch als Wettbewerbsbehörden zu qualifizieren sind (dazu Debus, in: ders., Informationszugangsrecht Baden-Württemberg, 2017, § 4 LIFG Rn. 42, sowie zum Bundesrecht auch: Schirmer, in: Gersdorf/Paal, Informations- und Medienrecht, 2014, § 3 IFG Rn 73; Schoch, IFG, 2. Aufl. 2016, § 3 Rn. 80 f.). Da über die ausdrücklich bereits genannten Aufsichtsbehörden hinaus bei allen Aufsichtsbehörden die Gefahr besteht, dass die Aufsichtstätigkeit insbesondere durch das Bekanntwerden von Prüfungsmustern beeinträchtigt wird, soll der Ablehnungsgrund für alle Aufsichtsbehörden gleichermaßen gelten. Damit gilt der Ablehnungsgrund auch für die Landesbeauftragte oder für den Landesbeauftragten für den Datenschutz, wodurch ihre oder seine Unabhängigkeit abgesichert wird.

Zu Nummer 3

Folgeänderung zu Nummer 1

Zu Nummer 4

Zu Buchstabe a

Die Verweisung im Landesinformationsfreiheitsgesetz auf Voraussetzungen der Einwilligung nach § 4 Absatz 2 bis 5 LDSG wird durch die Verweisung auf die entsprechenden Bedingungen für die Einwilligung nach Artikel 7 der Verordnung (EU) 2016/679 ersetzt.

Zu Buchstabe b

§ 5 Absatz 2 LIFG orientiert sich bislang an Artikel 8 der Richtlinie 95/46/EG vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. EG L 281, S. 31) und schützt mit Rücksicht auf die UN-Behindertenrechtskonvention außerdem die Daten im Zusammenhang mit einer Behinderung. Die Regelung wird an die besonderen Kategorien personenbezogener Daten nach Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 angepasst. In Hinblick auf Erwägungsgrund 54 der Verordnung (EU) 2016/679 sind davon auch Daten, aus denen eine Behinderung hervorgeht, umfasst, sodass eine ausdrückliche Erwähnung nicht erforderlich ist. Für die Konkretisierung der Formulierungen „genetische Daten“, „biometrische Daten“ und „Gesundheitsdaten“ sind die Begriffsbestimmungen in Artikel 4 Nummern 13 bis 15 der Verordnung (EU) 2016/679 zu beachten.

Zu Buchstabe c und d

Der Begriff der Betroffenen im Sinne des § 3 Absatz 1 LDSG wird durch die entsprechende Begriffsbestimmung für eine betroffene Person in Artikel 4 Nummer 1 der Verordnung (EU) 2016/679 ersetzt.

Zu Nummer 5

Folgeänderung zu Nummer 1

## Zu Nummer 6

Die Verweisungen im Landesinformationsfreiheitsgesetz auf die Begriffsbestimmung für personenbezogene Daten im bisherigen § 3 Absatz 1 LDSG werden durch die Verweisungen auf die entsprechende Begriffsbestimmung in Artikel 4 Nummer 1 der Verordnung (EU) 2016/679 ersetzt.

## Zu Nummer 7

In Bezug auf die Landesbeauftragte oder den Landesbeauftragten für die Informationsfreiheit wird die bisherige Verweisungsregelung auf das Landesdatenschutzgesetz durch eine weitgehende Übernahme des Wortlauts der bisher entsprechend anwendbaren Regelungen des Landesdatenschutzgesetzes ersetzt. Eine Verweisung auf die Regelungen über die Aufsichtsbehörden nach den Artikeln 51 ff. der Verordnung (EU) 2016/679 ist nicht sinnvoll, weil dort sehr viele detaillierte, datenschutzspezifische Regelungen enthalten sind, die für eine entsprechende Anwendung im Bereich der Informationsfreiheit nicht geeignet sind.

Eine Übernahme der Verweisung zur Rechtsstellung nach der bisherigen Verweisung in § 12 Absatz 3 LIFG in Verbindung mit § 26 Absatz 2 bis 4 LDSG ist nicht erforderlich, weil sich Entsprechendes nunmehr aus der Stellung als oberste Landesbehörde ergibt.

## Zu Buchstabe a

Die bisherige Regelung über die Kontrollaufgaben der oder des Landesbeauftragten für die Informationsfreiheit nach § 12 Absatz 3 LIFG in Verbindung mit § 28 Absatz 1 LDSG wird entsprechend übernommen.

## Zu Buchstabe b

## Zum angefügten Absatz 4

Die bisherige Regelung des § 12 Absatz 3 LIFG in Verbindung mit § 29 Absatz 1 Satz 1 LDSG über die Pflicht zur Unterstützung der oder des Landesbeauftragten für die Informationsfreiheit wird entsprechend übernommen. Die Detailregelungen der Pflicht zur Unterstützung in § 29 Absatz 1 Satz 2 und Absatz 2 LDSG sind für den Bereich der Informationsfreiheit entbehrlich.

## Zum angefügten Absatz 5

Die bisherige Regelung des § 12 Absatz 3 LIFG in Verbindung mit § 30 Absatz 1 Satz 1 LDSG über die Mitteilung des Ergebnisses der Kontrolle der oder des Landesbeauftragten für die Informationsfreiheit wird übernommen. Die Übernahme der Detailregelung zur Verbindung mit Verbesserungsvorschlägen nach § 30 Absatz 1 Satz 2 LDSG ist für den Bereich der Informationsfreiheit entbehrlich.

## Zum angefügten Absatz 6

Die bisherige Regelung des § 12 Absatz 3 LIFG in Verbindung mit § 30 Absatz 2 bis 4 LDSG über die Beanstandungen der oder des Landesbeauftragten für die Informationsfreiheit wird entsprechend übernommen. Die Übernahme der Detailregelung zum Inhalt der Stellungnahme nach § 30 Absatz 4 Satz 1 LDSG ist für den Bereich der Informationsfreiheit entbehrlich.

Die Regelung stellt die Verpflichtung der oder des Landesbeauftragten für die Informationsfreiheit in den Vordergrund, auf eine Verbesserung der Informations-

freiheit bei den informationspflichtigen Stellen hinzuwirken. Damit wird klargestellt, dass nicht jeder festgestellte Mangel mit einer förmlichen Beanstandung zu rügen ist. Insbesondere nach Beseitigung der Mängel hat eine Beanstandung weitgehend ihren Sinn verloren, weil die informationspflichtige Stelle bereits das Notwendige veranlasst hat.

Zum angefügten Absatz 7

Zum angefügten Satz 1

Die bisherige Regelung des § 12 Absatz 3 LIFG in Verbindung mit § 31 Absatz 2 LDSG wird entsprechend übernommen. Danach hat die oder der Landesbeauftragte die weitere Aufgabe, einen Tätigkeitsbericht zu erstellen. Anstatt des bisherigen Termins (1. Dezember jedes zweiten Jahres) wird aus Praktikabilitätsgründen der Berichtszeitraum auf zwei Kalenderjahre angepasst.

Zum angefügten Satz 2

Die Abgabefrist zum 15. Februar wurde gewählt, um einerseits der oder dem Landesbeauftragten mit der Erstellung des Berichtes ausreichend Zeit zu geben und andererseits, um zumeist eine Befassung des Landtags mit dem Bericht und der regelmäßig drei Monate später vorzulegenden Stellungnahme der Landesregierung dazu vor der Sommerpause zu gewährleisten.

Zum angefügten Satz 3

Die Regelung stellt klar, wann der nächste Bericht vorzulegen ist.

Zum angefügten Absatz 8

Die bisherige Regelung des § 12 Absatz 3 LIFG in Verbindung mit § 31 Absatz 3 LDSG wird entsprechend übernommen. Danach hat die oder der Landesbeauftragte die weitere Aufgabe, Gutachten und besondere Berichte zu erstellen und den Austausch mit dem Landtag und dessen Ständigem Ausschuss zu pflegen. Im Unterschied zur bisherigen Regelung wird anstatt der halbjährlichen eine jährliche Unterrichtung des Ständigen Ausschusses des Landtags für ausreichend erachtet.

Zum angefügten Absatz 9

Zu Satz 1

Die bisherige Regelung des § 12 Absatz 3 LIFG in Verbindung mit § 31 Absatz 4 Satz 1 LDSG wird entsprechend übernommen. Danach kann die oder der Landesbeauftragte für die Informationsfreiheit der Landesregierung und den einzelnen Ministerien sowie den anderen öffentlichen Stellen Empfehlungen zur Verbesserung des Datenschutzes geben. Die Übernahme der Regelung zur Beratung (§ 30 Absatz 4 Satz 1 LDSG) ist entbehrlich, weil sich Entsprechendes aus § 12 Absatz 2 LIFG ergibt.

Zu Satz 2

Die bisherige Regelung des § 12 Absatz 3 LIFG in Verbindung mit § 31 Absatz 4 Satz 2 LDSG wird entsprechend übernommen. Danach ist die oder der Landesbe-

auftragte bei der Ausarbeitung von Rechts- und Verwaltungsvorschriften zum Landesinformationsfreiheitsgesetz zu beteiligen.

Zu Artikel 6 – Änderung der Gebührenverordnung Innenministerium

Als oberste Landesbehörde obliegt der oder dem Landesbeauftragten für den Datenschutz die Aufgabe, ihre oder seine Gebühren mittels Verordnung selbst festzulegen, soweit sie oder er hierzu durch die Verordnung (EU) 2016/679 oder sonstige Gesetze ermächtigt ist. Auf § 4 Absatz 2 des Landesgebührengesetzes wird hingewiesen.

Zu Artikel 7 – Änderung der Verordnung der Landesregierung über Zuständigkeiten nach dem Gesetz über Ordnungswidrigkeiten

Gemäß der in Artikel 1 § 25 Absatz 2 Satz 1 vorgenommenen, durch die Verordnung (EU) 2016/679 vorgegebenen Aufgabenzuweisung obliegt der oder dem Landesbeauftragten für den Datenschutz die Verfolgung von Ordnungswidrigkeiten. Die bisherige Zuständigkeit des Regierungspräsidiums Karlsruhe entfällt daher.

Zu Artikel 8 – Änderung des Gesetzes zur Ausführung des Personalausweisgesetzes

Es handelt sich um eine Klarstellung.

Zu Artikel 9 – Änderung des Feuerwehrgesetzes

Zu Nummer 1

Der Verweis auf das Landesdatenschutzgesetz als Auffanggesetz für das Datenschutzrecht ist zu streichen, da dieses mit der Anpassung an die Verordnung (EU) 2016/679 in Artikel 1 nur noch ergänzende Regelungen enthält und im Übrigen die Verordnung (EU) 2016/679 direkt gelten wird. Auch eine Bezugnahme auf die Verordnung (EU) 2016/679 wäre rein deklaratorisch und ist daher nicht vorgesehen.

Zu Nummern 2 bis 6

Es handelt sich um redaktionelle Folgeänderungen zu Nummer 1.

Zu Artikel 10 – Änderung des Rettungsdienstgesetzes

Zu Nummer 1

Zu Buchstabe a und b

Es handelt sich um eine notwendige redaktionelle Bereinigung. Mit unmittelbarer Geltung der Verordnung (EU) 2016/679 ist eine allgemeine Bezugnahme auf Datenschutzregelungen nicht mehr vorzusehen.

Zu Nummer 2

Zu Buchstabe a

Es handelt sich um eine notwendige redaktionelle Änderung. Nach Artikel 4 Nummer 2 der Verordnung (EU) 2016/679 sind mit dem Begriff „Verarbeitung“ alle Vorgangsschritte im Zusammenhang mit personenbezogenen Daten erfasst.

Zu Buchstabe b

Es handelt sich um eine redaktionelle Folgeänderung zu Buchstabe a.

Zu Buchstabe c

Es handelt sich um eine redaktionelle Bereinigung.

Zu Artikel 11 – Änderung des Flüchtlingsaufnahmegesetzes

Zu Nummer 1

Um die Verarbeitung besonders sensibler personenbezogener Daten durch die unteren Aufnahmebehörden im Rahmen deren Aufgabenerfüllung zu ermöglichen, verweist § 16 Absatz 1 FlüAG bislang auf § 33 Absatz 1 LDSG a.F. Von § 33 Absatz 1 LDSG a.F. werden Daten erfasst, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, die Gewerkschaftszugehörigkeit, die Gesundheit oder das Sexualleben hervorgehen. Die Verarbeitung dieser Daten ist gemäß Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 untersagt. In Artikel 9 Absatz 2 der Verordnung (EU) 2016/679 sind jedoch Ausnahmen vom Verbot des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 vorgesehen. Einschlägig in Bezug auf die angeführten personenbezogenen Daten ist Artikel 9 Absatz 2 Buchstabe g der Verordnung (EU) 2016/679.

Die Verarbeitung der in § 33 Absatz 1 LDSG a.F. angeführten Daten ist für die Aufgabenwahrnehmung der Aufnahmebehörden zwingend erforderlich. Die Kenntnis dieser Daten ist etwa Voraussetzung für eine sachgerechte und an den Interessen der Asylsuchenden orientierte Belegung der Unterkünfte, in denen die Flüchtlinge für längere Zeit in enger Nachbarschaft leben. Dasselbe gilt für eine angemessene und effektive Flüchtlingssozialarbeit. Darüber hinaus ist die Verarbeitung biometrischer Daten gemäß Artikel 4 Nummer 14 der Verordnung (EU) 2016/679 für die eindeutige Identifizierung Geflüchteter erforderlich und in Gestalt von Fingerabdruckdaten bereits gemäß § 3 Absatz 2 Nummer 1 des Gesetzes über das Ausländerzentralregister im Ausländerzentralregister gespeichert.

Zur Wahrung der Rechte der betroffenen Personen darf die Verarbeitung nach § 16 Absatz 1 FlüAG lediglich im Einzelfall erfolgen und sofern die Verarbeitung im Rahmen der Aufgabenwahrnehmung der Aufnahmebehörden erforderlich ist. Die Verarbeitung genetischer Daten wird ausgeschlossen, da sie für die Aufgabenwahrnehmung nicht erforderlich ist.

Zu Nummer 2

Es handelt sich um eine redaktionelle Änderung. Nach Artikel 4 Nummer 1 der Verordnung (EU) 2016/679 wird eine natürliche Person, auf die sich personenbezogene Daten beziehen, als betroffene Person bezeichnet. Diese Begrifflichkeit wird daher in § 16 Absatz 2 Satz 4 FlüAG übernommen.

## Zu Nummer 3

Unter Geltung der Verordnung (EU) 2016/679 enthält das Landesdatenschutzgesetz nur noch ergänzende Regelungen. Die Verordnung (EU) 2016/679 ist als EU-Verordnung in den Mitgliedstaaten unmittelbar geltendes Recht. Der bislang in Absatz 3 enthaltene Verweis auf das Landesdatenschutzgesetz a. F. als Auffanggesetz für die Verarbeitung personenbezogener Daten durch die Ausländerbehörden ist daher zu streichen.

## Zu Artikel 12 – Änderung des baden-württembergischen Ausführungsgesetzes zum Bundesmeldegesetz

## Zu Nummer 1

Die Änderung passt den Gesetzestext an die Begriffsbestimmung nach Artikel 4 Nummer 2 der Verordnung (EU) 2016/679 an. Es handelt sich um eine bereichsspezifische Regelung zur Datenverarbeitung gemäß Artikel 6 Absatz 1 Buchstaben c und e in Verbindung mit Artikel 6 Absatz 2, Absatz 3 Satz 1 Buchstabe b und Satz 2 der Verordnung (EU) 2016/679.

## Zu Nummer 2

## Zu Buchstabe a und c

Die Änderung passt den Gesetzestext an die Begriffsbestimmung nach Artikel 4 Nummer 2 der Verordnung (EU) 2016/679 an. Es handelt sich um eine bereichsspezifische Regelung zur Datenverarbeitung gemäß Artikel 6 Absatz 1 Buchstaben c und e in Verbindung mit Artikel 6 Absatz 2, Absatz 3 Satz 1 Buchstabe b und Satz 2 der Verordnung (EU) 2016/679.

## Zu Buchstabe b

Die Änderung passt den Gesetzestext an den in Artikel 16 der Verordnung (EU) 2016/679 verwendeten Begriff der Vervollständigung an.

## Zu Artikel 13 – Änderung der Meldeverordnung

## Zu Nummern 1 und 2

Die Änderung passt den Gesetzestext an den in Artikel 16 der Verordnung (EU) 2016/679 verwendeten Begriff der Vervollständigung an.

## Zu Nummer 3

Die Änderung ist eine Folgeänderung aus der Umstrukturierung des Landesdatenschutzgesetzes. Die bisher in § 9 LDSG a. F. geregelten technischen und organisatorischen Maßnahmen werden künftig in § 3 LDSG geregelt werden.

## Zu Artikel 14 – Änderung des Landesglücksspielgesetzes

## Zu Nummern 1 und 2

Die Änderungen passen den Gesetzestext an die Begriffsbestimmung nach Artikel 4 Nummer 2 der Verordnung (EU) 2016/679 an. Es handelt sich um bereichsspezi-

fische Regelungen zur Datenverarbeitung gemäß Artikel 6 Absatz 1 Buchstabe c in Verbindung mit Artikel 6 Absatz 2, Absatz 3 Satz 1 Buchstabe b und Satz 2 der Verordnung (EU) 2016/679.

Zu Nummer 3

Zu Buchstabe a

Die Änderung in § 32 Absatz 4 Satz 1 passt den Gesetzestext an die Begriffsbestimmung nach Artikel 4 Nummer 2 der Verordnung (EU) 2016/679 an. Es handelt sich um eine bereichsspezifische Regelung zur Datenverarbeitung gemäß Artikel 6 Absatz 1 Buchstabe c in Verbindung mit Artikel 6 Absatz 2, Absatz 3 Satz 1 Buchstabe b und Satz 2 der Verordnung (EU) 2016/679.

Zu Buchstabe b

Da die Informationspflichten mit unmittelbarer Geltung in der Verordnung (EU) 2016/679 geregelt werden, kann der bisherige § 32 Absatz 5 des Landesglücksspielgesetzes aufgehoben werden.

Zu Buchstabe c

Aufgrund der erfolgten Änderungen im Bundesdatenschutzgesetz ist der bisher enthaltene Verweis zu entfernen. An der Verpflichtung der Spielbank, einen betrieblichen Datenschutzbeauftragten zu bestellen, wird festgehalten. Für diesen gelten die Regeln der genannten EU-Verordnung.

Zu Nummer 4

Die Änderung in § 45 Absatz 3 Satz 2 passt den Gesetzestext an die Begriffsbestimmung nach Artikel 4 Nummer 2 der Verordnung (EU) 2016/679 an. Es handelt sich um eine bereichsspezifische Regelung zur Datenverarbeitung gemäß Artikel 6 Absatz 1 Buchstabe c in Verbindung mit Artikel 6 Absatz 2, Absatz 3 Satz 1 Buchstabe b und Satz 2 der Verordnung (EU) 2016/679.

Zu Artikel 15 – Änderung des Abschiebungshaftvollzugsgesetzes Baden-Württemberg

Zu Nummer 1

Die Aufnahme des § 1 Absatz 2 dient der Klarstellung, dass das Abschiebungshaftvollzugsgesetz auch auf den Vollzug des Ausreisegewahrsams im Sinne des § 62 b des Aufenthaltsgesetzes (AufenthG) Anwendung findet. Gemäß § 62 b Absatz 3 AufenthG findet für den Ausreisegewahrsam mit § 62 a AufenthG die Vorschrift über den Vollzug der Abschiebungshaft entsprechende Anwendung. Die Möglichkeit eines Ausreisegewahrsams wurde mit dem Gesetz zur Neubestimmung des Bleiberechts und der Aufenthaltsbeendigung vom 27. Juli 2015 (BGBl. I S. 1386) eingeführt. Die höchstmögliche Dauer des Ausreisegewahrsams wurde mit dem Gesetz zur besseren Durchsetzung der Ausreisepflicht vom 20. Juli 2017 (BGBl. I S. 2780) von vier auf zehn Tage verlängert, sodass der Vorschrift nun mehr praktische Relevanz zukommt. Für den Vollzug des Ausreisegewahrsams kommt gemäß § 62 b Absatz 2 AufenthG neben dem Transitbereich eines Flughafens auch eine Unterkunft in Betracht, von wo aus die Ausreise des Ausländers möglich ist. Nach der Gesetzesbegründung soll der Ausländer die Möglichkeit haben, den Ausreisegewahrsam jederzeit dadurch vorzeitig zu beenden, indem er

eine konkrete Reisemöglichkeit (Flugverbindung) in einen aufnahmebereiten Staat benennt, die er wahrnehmen möchte. In diesem Fall soll ihm die Ausreise ermöglicht werden (Bundestags-Drucksache 18/4097, S. 56). Einer unmittelbaren Nähe zu einem Flughafen bedarf es hierzu jedoch nicht, da eine Ausreise von jedem Ort in Deutschland möglich ist. Zudem ist eine solche Einschränkung dem Wortlaut der Vorschrift nicht zu entnehmen. Somit kann der Ausreisegewahrsam in der Abschiebungshafteinrichtung Pforzheim vollzogen werden. Auch für den Ausreisegewahrsam im Sinne des § 62 b des Aufenthaltsgesetzes bedarf es einer landesgesetzlichen Grundlage für die über die reine Freiheitsentziehung hinausgehenden Einschränkungen für die Unterbrachten.

#### Zu Nummer 2

Im Zeitpunkt des Inkrafttretens des Abschiebungshaftvollzugsgesetzes zum 30. Dezember 2015 (GBl. S. 1187) stellte sich die Frage der Unterbringung von Ausländern, von denen eine erhebliche Gefahr für Leib oder Leben Dritter oder bedeutender Rechtsgüter der inneren Sicherheit ausgeht, noch nicht in dem Maße wie im Zeitpunkt der Verabschiedung dieses Gesetzes. Auch der Bundesgesetzgeber hat auf die aktuelle Entwicklung mit dem Gesetz zur besseren Durchsetzung der Ausreisepflicht vom 20. Juli 2017 (BGBl. I, S. 2780) reagiert. § 62 a Absatz 1 Satz 2 AufenthG sieht nunmehr vor, dass Ausländer, von denen eine erhebliche Gefahr für Leib oder Leben Dritter oder bedeutende Rechtsgüter der inneren Sicherheit ausgeht, abweichend von der Grundregel des Trennungsgebots nach Artikel 16 Absatz 1 Satz 1 der Richtlinie 2008/115/EG des Europäischen Parlaments und des Rates vom 16. Dezember 2008 über gemeinsame Normen und Verfahren in den Mitgliedstaaten zur Rückführung illegal aufhältiger Drittstaatsangehöriger, in regulären Justizvollzugsanstalten untergebracht werden können. Zudem können diese Ausländer gemäß § 62 Absatz 3 AufenthG nunmehr auch dann in Abschiebungshaft genommen werden, wenn die Abschiebung innerhalb der nächsten drei Monate nicht durchgeführt werden kann. Somit bedarf es einer Erweiterung der Beschränkungsbefugnis für die Fälle, in denen vom Unterbrachten eine erhebliche Gefahr für Leib oder Leben Dritter oder bedeutende Rechtsgüter der inneren Sicherheit ausgeht.

#### Zu Nummer 3

Gemäß Artikel 9 der Verordnung (EU) 2016/679 dürfen personenbezogene Daten, aus denen die ethnische Herkunft oder religiöse Überzeugungen hervorgehen, nur dann verarbeitet werden, wenn die Voraussetzungen eines der Ausnahmetatbestände des Artikels 9 Absatz 2 der Verordnung (EU) 2016/679 erfüllt sind. Eine Verarbeitung dieser Daten darf nach Artikel 9 Absatz 2 Buchstabe a der Verordnung (EU) 2016/679 zum Zwecke des Schutzes der betroffenen Person vor religiös oder rassistisch motivierten Übergriffen und zum Zwecke der Ermöglichung der Religionsausübung erfolgen, sofern die betroffene Person eingewilligt hat.

#### Zu Nummer 4

Der neue Absatz 4 erlaubt unter eingeschränkten Voraussetzungen, die dem Gesichtspunkt der Verhältnismäßigkeit Rechnung tragen, die Videoüberwachung und die Anfertigung von Aufzeichnungen hiervon während der Unterbringung in einem besonders gesicherten Raum sowie in Räumen, die lediglich der vorübergehenden Unterbringung dienen, wie Krisenräume, Beobachtungsräume und medizinische Bettenstation. Nach Absatz 4 Satz 3 sind dabei die Persönlichkeitsrechte, die Würde und das Schamgefühl zu achten. Dies kann durch geeignete Maßnahmen, wie die Verpixelung der Bildschirmwiedergabe im Bereich der Intimsphäre, sichergestellt werden. Absatz 4 Satz 4 sieht vor, dass der Unterbrachte auf die Videoüberwachung und die Anfertigung von Aufzeichnungen hingewie-

sen wird. Die Verarbeitung ist gemäß Artikel 6 Absatz 1 Buchstabe d der Verordnung (EU) 2016/679 rechtmäßig. Absatz 4 Sätze 5 und 6 tragen dem Recht der betroffenen Person auf Löschung gemäß Artikel 17 der Verordnung (EU) 2016/679 Rechnung.

Zu Nummer 5

Die Bestimmung entspricht im Wesentlichen § 23 des baden-württembergischen Justizvollzugsgesetzbuchs Buch 1. Es handelt sich hierbei um eine bereichsspezifische Regelung zur Datenverarbeitung gemäß Artikel 6 Absatz 1 Buchstabe e in Verbindung mit Artikel 6 Absatz 2, Absatz 3 Satz 1 Buchstabe b und Satz 2 der Verordnung (EU) 2016/679. Dem Grundsatz der Verhältnismäßigkeit wird durch die engen Voraussetzungen zur Zulässigkeit der Videoüberwachung Rechnung getragen. Sofern die Videoüberwachung zu dem genannten Zweck erforderlich ist, wird sie parallel zur oben genannten Regelung im Justizvollzugsgesetzbuch Buch 1 zugelassen. Eine spezielle Datenschutz-Folgeabschätzung kann gemäß Artikel 35 Absatz 10 der Verordnung (EU) 2016/679 entfallen.

Absatz 1 Satz 4 sieht darüber hinausgehend vor, dass § 10 Absatz 4 unberührt bleibt. Die Videoüberwachung bei der Unterbringung in einem besonders gesicherten Raum sowie in Räumen, die nur einer vorübergehenden Unterbringung dienen, stellt eine Ausnahme von dem Grundsatz dar, dass die Videoüberwachung von Unterbringungsräumen ausgeschlossen ist und steht im Einklang mit Artikel 6 Absatz 1 Buchstabe d der Verordnung (EU) 2016/679. Mit dem Ausschluss von Räumen, die für Kontakte mit Berufsheimlichkeitsgeheimnisträgern (vgl. § 53 Strafprozessordnung), Beiständen und Mitarbeitern von einschlägig tätigen Hilfs- und Unterstützungsorganisationen genutzt werden, wird das Vertrauensverhältnis besonders geschützt. Der Zugang von Mitarbeitern von einschlägig tätigen Hilfs- und Unterstützungsorganisationen hat der Bundesgesetzgeber mit § 62 a Absatz 4 Aufenthaltsgesetz in Umsetzung von Artikel 16 Absatz 4 der Richtlinie 2008/115/EG geregelt. Personen, die nicht unter diese Regelung fallen, können im Rahmen des § 7 Abschiebungshaftvollzugsgesetz in Verbindung mit § 3 Abschiebungshaftvollzugsverordnung die Untergebrachten besuchen.

Absatz 3 trägt dem Recht der betroffenen Person auf Löschung gemäß Artikel 17 der Verordnung (EU) 2016/679 Rechnung.

Zu Artikel 16 – Änderung der Abschiebungshaftvollzugsverordnung

Zu Nummer 1

Die Änderung in § 1 Absatz 2 passt den Gesetzestext an die Begriffsbestimmung in Artikel 4 Nummer 2 der Verordnung (EU) 2016/679 an. Es handelt sich um eine bereichsspezifische Regelung zur Datenverarbeitung im Sinne des Artikels 6 Absatz 1 Buchstabe e in Verbindung mit Artikel 6 Absatz 2, Absatz 3 Satz 1 Buchstabe b und Satz 2 der Verordnung (EU) 2016/679.

Zu Nummer 2

Zu Buchstabe a

In § 10 Absatz 4 Satz 2 wird der nicht mehr aktuelle Verweis auf § 3 Absatz 6 des Landesdatenschutzgesetzes gestrichen.

Bei der Änderung in § 10 Absatz 4 Satz 3 handelt es sich um eine bereichsspezifische Regelung zur Datenverarbeitung im Sinne des Artikels 6 Absatz 1 Buchstabe e in Verbindung mit Artikel 6 Absatz 2, Absatz 3 Satz 1 Buchstabe b und Satz 2 der Verordnung (EU) 2016/679.

Die Änderung in § 10 Absatz 4 Satz 4 passt den Gesetzestext an die Voraussetzungen des Artikels 9 Absatz 2 Buchstabe a der Verordnung (EU) 2016/679 an.

Zu Buchstabe b

Bei der Änderung in § 10 Absatz 6 Satz 3 handelt es sich um eine bereichsspezifische Regelung zur Datenverarbeitung im Sinne des Artikels 6 Absatz 1 Buchstabe e in Verbindung mit Artikel 6 Absatz 2, Absatz 3 Satz 1 Buchstabe b und Satz 2 der Verordnung (EU) 2016/679.

Die Änderung in § 10 Absatz 6 Satz 4 passt den Gesetzestext an die Voraussetzungen des Artikels 9 Absatz 2 Buchstabe a der Verordnung (EU) 2016/679 an.

Zu Artikel 17 – Änderung des Landesbeamtengesetzes

Zu Nummer 1

Folgeänderung zu Nummer 2

Zu Nummer 2

Zu Absatz 1

Zu Satz 1

Artikel 6 und Artikel 88 der Verordnung (EU) 2016/679 erlauben den Mitgliedstaaten die Regelung spezifischer Vorschriften für die Verarbeitung personenbezogener Daten im Beschäftigungskontext. Hiervon soll Gebrauch gemacht werden, indem in § 83 eine spezifische Rechtsgrundlage für jegliche Vorgänge im Zusammenhang mit der Verarbeitung von Personalaktendaten im Beschäftigungsverhältnis geschaffen wird. Der bisherige Regelungsgehalt der Norm bezog sich auf die „Erhebung“ von Personalaktendaten. Der Begriff der „Verarbeitung“ nach der Verordnung (EU) 2016/679 ist jedoch umfassend zu verstehen, vgl. Artikel 4 Nummer 2. Danach umfasst Datenverarbeitung jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten. Der Regelungsumfang der Norm wird daher vom Teilaspekt des „Erhebens“ auf die gesamte „Verarbeitung“ erweitert und die Überschrift entsprechend angepasst. Teilaspekte der Verarbeitung, die bisher ausdrücklich im Gesetz genannt und in verschiedenen Normen enthalten waren (z. B. Erhebung, Speicherung, Nutzung), sind vom Begriff der Verarbeitung umfasst. Das Wort „nur“ ist zu streichen, da sich für bestimmte Verarbeitungssituationen eine Ermächtigung zur Datenverarbeitung direkt aus der Verordnung (EU) 2016/679 ergeben kann. Da Artikel 88 Absatz 1 der Verordnung (EU) 2016/679 auch eine Verarbeitung personenbezogener Beschäftigtendaten auf Grundlage von Dienstvereinbarungen erlaubt, sollen diese als Grundlage für eine Datenverarbeitung aufgenommen werden.

Der Regelungsgehalt von § 84 Absatz 1 LBG a. F. geht in § 83 Absatz 1 auf, so dass § 84 Absatz 1 LBG a. F. zu streichen ist.

Zu Satz 2

Die Verarbeitung besonderer Kategorien personenbezogener Daten (z. B. Gesundheitsdaten, Gewerkschaftszugehörigkeit, Sozialdaten) ist nach Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 grundsätzlich untersagt, da im Zusammenhang mit ihrer Verarbeitung erhebliche Risiken für die Grundrechte der betroffenen

Personen auftreten können. Artikel 9 Absatz 2 der Verordnung (EU) 2016/679 regelt abschließend die Zwecke, in denen eine Verarbeitung ausnahmsweise zulässig ist. § 83 Absatz 1 Satz 2 dient der Durchführung von Artikel 9 Absatz 2 der Verordnung (EU) 2016/679, insbesondere der Buchstaben b und g. Das Landesdatenschutzgesetz macht von den in diesen Regelungen enthaltenen Ermächtigungen zur Regelung von Ausnahmen von dem Verbot der Verarbeitung besonderer Kategorien personenbezogener Daten Gebrauch. Besondere Kategorien personenbezogener Daten dürfen im Rahmen des Dienstverhältnisses insbesondere verarbeitet werden, soweit die Verarbeitung erforderlich ist, um den Rechten und Pflichten des Dienstherrn auf dem Gebiet des Dienstrechts sowie des Rechts der sozialen Sicherheit und des Sozialschutzes zu genügen (Artikel 1 § 15 Absatz 2). Über die entsprechende Anwendung von Artikel 1 § 17 Absatz 2 ist zudem die Verarbeitung von Daten über politische Meinungen sowie religiöse oder weltanschauliche Überzeugungen erfasst, was im Rahmen der Ergreifung disziplinarrechtlicher Maßnahmen relevant werden kann, wenn die betroffene Beamtin bzw. der betroffene Beamte beispielsweise einer verfassungsfeindlichen Organisation angehört. Sofern das Personalaktendatenrecht spezifische Rechtsgrundlagen zur Verarbeitung besonderer Kategorien personenbezogener Daten enthält (beispielsweise zur Verarbeitung von Beihilfedaten bzw. Gesundheitsdaten, § 83 Absätze 2 und 3), finden diese Anwendung.

Zusätzlich wird auf § 3 LDSG Bezug genommen. Darin werden Maßnahmen geregelt, um den strengen datenschutzrechtlichen Anforderungen des Artikels 9 der Verordnung (EU) 2016/679 gerecht zu werden. Diese sollen im Personalaktendatenrecht entsprechend Anwendung finden.

Zu Absatz 2 bis 4

Die Begrifflichkeiten in Absatz 2 und 3 sind an die Verordnung (EU) 2016/679 anzupassen. Die Bearbeitung von Beihilfeprozessen an sich ist bereits nach Absatz 1 zulässig. Absatz 2 unterwirft die Verwendung von Personalaktendaten über Beihilfe für andere als für Beihilfeszwecke über die Verweisung auf § 85 Absatz 2 und 3 besonderen Voraussetzungen. Die Begriffe der „Speicherung“, der „Veränderung“ und der „Nutzung“ sind von dem umfassenden Verarbeitungsbegriff des Artikels 4 Nummer 2 der Verordnung (EU) 2016/679 mitumfasst.

Absatz 3 konkretisiert die Verarbeitung von Gesundheitsdaten (Artikel 4 Nummer 15 der Verordnung [EU] 2016/679) und kann als zulässige mitgliedstaatliche Regelung auf Grundlage von Artikel 9 Absatz 2 Buchstaben b und h der Verordnung (EU) 2016/679 beibehalten werden. Der umfassende Verarbeitungsbegriff der Verordnung (EU) 2016/679 umfasst die bisher genannten Teilschritte mit.

Absatz 4 entspricht der bisherigen Fassung von § 84 Absatz 4 und kann aufrechterhalten werden.

Zu Nummer 3

Automatisierte Verfahren gewinnen mit fortschreitender Digitalisierung an Bedeutung. Gerade in Massenverfahren sind sie unabdingbarer Bestandteil der Verwaltungsarbeit. Im Beamtenrecht bestehen Massenverfahren insbesondere im Beihilfe- und Reisekostenbereich. Nach Artikel 22 Absatz 2 Buchstabe b der Verordnung (EU) 2016/679 sind automatisierte Entscheidungen nur zulässig, wenn dies durch Rechtsvorschrift ausdrücklich angeordnet ist. Mit der Vorschrift des § 84 werden beamtenrechtliche Entscheidungen, die auf einer ausschließlich automatisierten Verarbeitung beruhen, zugelassen, wenn es sich weder um eine Ermessensentscheidung handelt noch ein Beurteilungsspielraum besteht. Nach § 84 können insbesondere auch geplante, mit automatisierten Verfahren einhergehende Risikomanagementsysteme im Beihilfeverfahren zulässig sein. § 84 ist damit sowohl in Bezug auf Artikel 22 Absatz 2 Buchstabe b in Verbindung mit Artikel 9

Absatz 2 Buchstabe g der Verordnung (EU) 2016/679 eine mitgliedstaatliche Rechtsvorschrift, als auch Rechtsgrundlage für die Zulassung von vollständig automatisiert erlassenen Verwaltungsakten im Sinne des inhaltsgleich zum Verwaltungsverfahrensgesetz des Bundes in Umsetzung begriffenen § 35 a des Landesverwaltungsverfahrensgesetzes. Danach kann ein Verwaltungsakt vollständig durch automatische Einrichtungen erlassen werden, sofern dies durch Rechtsvorschrift zugelassen ist und weder ein Ermessen noch ein Beurteilungsspielraum besteht. Angemessene Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Beihilfeberechtigten sind insbesondere in § 83 Absatz 2 und § 86 Absatz 5 getroffen.

Zu Nummer 4

Zu Buchstabe a

Redaktionelle Anpassungen an die Begrifflichkeiten der Verordnung (EU) 2016/679.

Zu Buchstabe b

Redaktionelle Anpassung an die Begrifflichkeiten der Verordnung (EU) 2016/679.

Zu Nummer 5

Die Verordnung (EU) 2016/679 stellt in den Artikeln 28 und 29 Vorgaben hinsichtlich der Modalitäten und Anforderungen der Datenverarbeitung im Auftrag auf. Artikel 88 der Verordnung (EU) 2016/679 erlaubt, dass spezifische Vorschriften zu Zwecken des Beschäftigungsverhältnisses getroffen werden.

Zu Absatz 1

Absatz 1 bestimmt als spezifischere Vorschrift im Sinne von Artikel 88 der Verordnung (EU) 2016/679, in welchen Fällen Datenverarbeitung im Auftrag zulässig sein soll. Eine mögliche Verarbeitung im Auftrag mit Einwilligung der Beamtin oder des Beamten bleibt hiervon unberührt. Die Verarbeitung erfolgt dabei im Auftrag derjenigen Stellen, welchen die Personalverantwortung zugewiesen ist. Die Wahrnehmung von Aufgaben der Personalverwaltung durch eine Behörde auf Grundlage öffentlich-rechtlicher Zuständigkeit mit Außenwirkung stellt keine Verarbeitung von Personalaktendaten im Auftrag dar. Die Norm beschränkt die zulässige Auftragsverarbeitung auf Fälle, in denen die genannten Stellen die technischen Möglichkeiten von Drittanbietern in Anspruch nehmen, um automatisierte oder in diesem Zuge automatisierbare Verarbeitungsprozesse auszulagern. Die Regelung hat damit die technischen Vorteile einer Automatisierung im Blick. Die Formulierung „überwiegend automatisierte“ stellt klar, dass zwingende manuelle Verarbeitungsschritte (etwa Ergebniskontrollen und andere maschinell nicht lösbare Zwischenschritte) den ansonsten automatisierten Charakter einer Datenverarbeitung nicht in Frage stellen.

Zu Absatz 2

Nach Absatz 2 bedarf die Auftragserteilung der vorherigen Zustimmung der obersten Dienstbehörde.

## Zu Absatz 3

Die Auslagerung an nichtöffentliche Stellen kommt nur zur Vermeidung übermäßiger Belastungen im Geschäftsablauf oder sonstiger wirtschaftlicher Gesichtspunkte in Betracht. Hierbei wird an die Verpflichtung angeknüpft, bei der Durchführung haushaltsrechtlicher Vorgaben die Grundsätze der Wirtschaftlichkeit und Sparsamkeit zu beachten. Diese Grundsätze verpflichten auch zur Prüfung, inwieweit staatliche Aufgaben oder öffentlichen Zwecken dienende wirtschaftliche Tätigkeiten durch Ausgliederung und Entstaatlichung oder Privatisierung erfüllt werden können (vgl. § 7 Absätze 1 und 3 der Landeshaushaltsordnung für Baden-Württemberg). Ein möglicher Anwendungsfall ist das Scannen von bestehenden Personalakten in Papier zur vollständigen Überführung in die elektronisch geführten Akten.

## Zu Nummer 6

Die Bestimmung spezifischer Löschungsvoraussetzungen und Lösungsfristen ist auf Grundlage von Artikel 17 Absatz 1 Buchstaben a und e und Artikel 88 der Verordnung (EU) 2016/679 zulässig.

## Zu Buchstabe a

Der Regelungsgehalt von Absatz 1 ergibt sich unmittelbar aus Artikel 17 Absatz 1 der Verordnung (EU) 2016/679, sodass Absatz 1 zu streichen ist.

## Zu Buchstaben b bis d

Folgeänderungen zu Buchstabe a

## Zu Nummer 7

Die Absätze 1 bis 4 werden zur systematischen und sprachlichen Anpassung an Artikel 15 der Verordnung (EU) 2016/679 neu gefasst. Die Überschrift wird entsprechend angepasst.

## Zu Absatz 1

Aus Artikel 15 Absatz 1 der Verordnung (EU) 2016/679 ergibt sich ein umfassendes Auskunftsrecht der betroffenen Person darüber, ob sie betreffende personenbezogene Daten verarbeitet werden. Dieses Auskunftsrecht gilt auch für die Auskunftserteilung in Beschäftigungsverhältnissen. Wegen des abschließenden Charakters der Betroffenenrechte der Artikel 13 ff. der Verordnung (EU) 2016/679 kommen bereichsspezifische Regelungen nur im Rahmen der Öffnungsklauseln der Betroffenenrechte selbst bzw. im Rahmen des Artikels 23 der Verordnung (EU) 2016/679 in Betracht.

Im Rahmen des Artikels 15 der Verordnung (EU) 2016/679 ergibt sich ein zulässiger ausgestaltungsfähiger Regelungsspielraum für den nationalen Gesetzgeber insofern, als die Art und Weise der Auskunftserteilung, also die Modalitäten zur Ausschöpfung des Betroffenenrechts, näher spezifiziert werden können. Der so eröffnete Regelungsspielraum soll zugunsten der Beamtinnen und Beamten genutzt werden, indem ihr bisher bestehendes Recht auf Einsicht in über sie gespeicherte Personalaktendaten aufrechterhalten wird. Durch die Möglichkeit, Einsicht in die physische (oder elektronische) Personalakte zu verlangen, wird das Betroffenenrecht aus Artikel 15 der Verordnung (EU) 2016/679 umfassend realisiert. Durch die Formulierung wird zudem klargestellt, dass die Einsichtnahme ei-

ne mögliche Form der Auskunftserteilung ist. Unbesehen vom Recht auf Einsichtnahme können Beamtinnen und Beamten nach Artikel 15 der Verordnung (EU) 2016/679 Auskunft über gespeicherte Personalaktendaten auf den üblichen Wegen, also per E-Mail, postalisch oder fernmündlich verlangen.

Zu Absatz 2

Absatz 2 ist redaktionell anzupassen.

Zu Absatz 3

Zu Satz 1

Absatz 3 Satz 1 wird mit Änderungen aufrechterhalten. Die Bestimmungsbefugnis der personalverwaltenden Stelle trägt Gründen der Praktikabilität Rechnung. Da die Verordnung (EU) 2016/679 die Einsicht als Form der Auskunft nicht explizit regelt, verbleibt für den nationalen Gesetzgeber Raum, die notwendigen Verfahrensvorschriften zu treffen.

Zu Satz 2

Der bisherige Absatz 3 Satz 2 schränkt das Recht auf Erhalt einer Kopie nach Artikel 15 Absatz 3 Satz 1 der Verordnung (EU) 2016/679 ein. Mangels einer naheliegenden Rechtfertigung dieser Einschränkung nach Artikel 23 Absatz 1 der Verordnung (EU) 2016/679 wird an der Einschränkung nicht festgehalten. Die Formulierung in Satz 2 stellt klar, dass der Erhalt einer Kopie einen Antrag der Beamtin oder des Beamten voraussetzt. Denkbarem Missbrauch (z. B. durch unbegründete wiederholte Kopie-Anforderungen) wäre durch Kostenerstattungen nach Artikel 15 Absatz 3 Satz 2 der Verordnung (EU) 2016/679 sowie auf Grundlage der speziell auf Missbrauchsfälle zugeschnittenen Regelung des Artikels 12 Absatz 5 der Verordnung (EU) 2016/679 zu begegnen.

Zu Absatz 4

Absatz 4 entspricht der bisherigen Fassung von Absatz 1 Satz 2 und 3. Das Recht, Auskunft in Form der Einsichtnahme zu verlangen, besteht nicht uneingeschränkt. Absatz 4 Satz 1 regelt den Fall, in dem die Einsichtnahme unzulässig ist. An die Stelle der Einsicht tritt hier die Auskunftserteilung. Die Beschränkung der Einsichtnahme entspricht dem bisherigen Recht und ist auch durch Artikel 23 Absatz 1 Buchstabe i der Verordnung (EU) 2016/679 gerechtfertigt.

Zu Absatz 5

Das bisherige Anhörungsrecht nach § 87 Absatz 4 LBG a. F. soll vor dem Hintergrund des abschließenden Charakters der Betroffenenrechte in der Verordnung (EU) 2016/679 stärker an den vorhandenen Betroffenenrechten der Verordnung (EU) 2016/679 ausgerichtet werden. Das Anhörungsrecht wird daher als zusammengesetztes Betroffenen- und Verfahrensrecht im Hinblick auf die beabsichtigte Speicherung von ungünstigen bzw. belastenden Personalaktendaten ausgestaltet. In der Anhörung treffen Informationspflichten über die Erhebung dieser Daten, insbesondere nach Artikel 14 der Verordnung (EU) 2016/679, auf das Recht der Beamtin oder des Beamten, zu ungünstigen Behauptungen, Bewertungen oder Beschwerden Stellung zu nehmen. Zudem kommt der Beamtin oder dem Beamten nach Artikel 16 der Verordnung (EU) 2016/679 – neben der Möglichkeit zur Gegendarstellung – das Recht zu, die über sie oder ihn gespeicherten Daten be-

richtigen oder durch eigene Ergänzungen vervollständigen zu lassen. Daran angeschlossen wird eine Verfahrensvorschrift, wonach Äußerungen der Beamtin oder des Beamten zu den Personalaktendaten zu speichern sind.

In dieser begrifflichen Einbettung in die Verordnung (EU) 2016/679 kann an der unter rechtsstaatlichen Grundsätzen (Recht auf rechtliches Gehör, Fürsorgeprinzip, Grundsatz der Personalaktenwahrheit) unverzichtbaren Anhörungsregelung festgehalten werden.

Der bisherige § 87 Absatz 5 LBG geht im Wesentlichen in den Informationspflichten der Artikel 13 und 14 der Verordnung (EU) 2016/679 auf und ist daher zu streichen.

Zu Nummer 8

Die Inhaltsübersicht soll entsprechend angepasst werden.

Zu Artikel 18 – Änderung des Landesdisziplinargesetzes

Zu Nummer 1

Zu Buchstabe a

Die Vorschrift verwendet in Absatz 1 den Begriff der Vorlage von Personalakten. Die Verordnung (EU) 2016/679 verwendet hingegen Begriffe, die durchweg trägermedienneutral sind. Der Begriff der Vorlage wird daher durch den in der Verordnung (EU) 2016/679 hierfür verwendeten Begriff der Übermittlung ersetzt. Auskünfte aus Personalaktendaten sind als geringerer Eingriff in das Persönlichkeitsrecht der betroffenen Person ausdrücklich mit eingeschlossen. Die weiteren Änderungen dienen der Vereinheitlichung einer Begrifflichkeit und der Anpassung an die Verordnung (EU) 2016/679.

Zu Buchstabe b

Anpassung an die Begrifflichkeit der Verordnung (EU) 2016/679.

Zu Nummer 2

§ 42 regelt die Modalitäten der Löschung von Personalaktendaten über den Disziplinarvorgang. Die Bestimmung spezifischer Löschungsvoraussetzungen und Lösungsfristen ist auf Grundlage von Artikel 17 Absatz 1 Buchstabe e der Verordnung (EU) 2016/679 zulässig. Die Terminologie ist jedoch anders als die der Verordnung (EU) 2016/679 nicht medienneutral und wird daher angepasst. Der Begriff der Löschung umfasst sowohl die physische Entfernung und Vernichtung von Papierakten als auch die Beseitigung von Akten in digitalisierter Form.

Zu Artikel 19 – Änderung des Landespersonalvertretungsgesetzes

Zu Nummer 1

Die Regelung über das Einwilligungserfordernis, wenn dienststellenexterne Vertreter zu Beratungen im Personalrat zugezogen werden, ist eine zulässige bereichsspezifische Ausgestaltung der zur Wahrnehmung der Aufgaben der Personalvertretung erforderlichen Datenverarbeitung im Beschäftigungsverhältnis nach Artikel 88 sowie Artikel 6 Absätze 2 und 3 in Verbindung mit Absatz 1 Buchsta-

ben c und e der Verordnung (EU) 2016/679. Es bedarf jedoch der redaktionellen Anpassung an die Begrifflichkeit der Verordnung (EU) 2016/679.

Zu Nummer 2

Die Regelung über die Einsicht von Mitgliedern der Personalvertretung in Personalaktendaten wird als zulässige bereichsspezifische Ausgestaltung der zur Wahrnehmung der Aufgaben der Personalvertretung erforderlichen Datenverarbeitung im Beschäftigungsverhältnis aufrechterhalten. Öffnungsklausel ist Artikel 88 sowie Artikel 6 Absätze 2 und 3 in Verbindung mit Absatz 1 Buchstaben c und e der Verordnung (EU) 2016/679. Es bedarf jedoch der redaktionellen Anpassung an die Begrifflichkeit der Verordnung (EU) 2016/679.

Zu Nummer 3

Zu Buchstabe a

Die Regelung, wonach der Personalrat bei Gewährung von Unterstützungen, Vorschüssen, Darlehen und entsprechenden sozialen Zuwendungen nach § 74 Absatz 1 Nummer 1 nur mitbestimmt, wenn die betroffenen Beschäftigten nicht widersprechen, genügt den Anforderungen der Verordnung (EU) 2016/679 an die Datenverarbeitung auf Grundlage einer Einwilligung nicht. Das bisherige Widerspruchsrecht ist daher, wie auch in den anderen Fällen des § 76 Absatz 2 Satz 1, durch ein Antragsrecht zu ersetzen.

Zu Buchstabe b

Folgeänderung zu Buchstabe a

Zu Artikel 20 – Inkrafttreten, Außerkrafttreten

Das Gesetz tritt gleichzeitig mit der Verordnung (EU) 2016/679 am 25. Mai 2018 in Kraft. Ab diesem Zeitpunkt tritt das Landesdatenschutzgesetz a. F. außer Kraft. Für die Polizeibehörden und den Polizeivollzugsdienst sowie für die Verarbeitung personenbezogener Daten durch das Landesamt für Verfassungsschutz im Rahmen der Erfüllung seiner Aufgaben nach § 3 des Landesverfassungsschutzgesetzes und beim Vollzug des Landessicherheitsüberprüfungsgesetzes enthält Artikel 1 § 30 eine Sonderregelung für die Weitergeltung des bisherigen Landesdatenschutzgesetzes.



**Anwaltsverband Baden-Württemberg**  
im Deutschen **Anwalt**Verein e. V.

Anwaltsverband Baden-Württemberg – Postfach 1221 – 70808 Korntal-Münchingen

Ministerium für Inneres, Digitalisierung und Migration BW

Willy-Brandt-Straße 41

70173 Stuttgart

Hasenbergsteige 5  
70178 Stuttgart

Geschäftsstelle:  
Johannes-Daur-Straße 10  
70825 Korntal-Münchingen

Postfach 1221  
70808 Korntal-Münchingen

Telefon 0711 / 2 36 59 63  
Telefax 0711 / 2 55 26 55

[www.av-bw.de](http://www.av-bw.de)  
[info@av-bw.de](mailto:info@av-bw.de)

31. Januar 2018

**Per E-Mail**

**Az.: 2-0557.8/1**

**Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679**

**- Stellungnahme des Anwaltsverbandes BW im DAV e. V. -**

Sehr geehrte Frau  
sehr geehrte Damen und Herren,

für die Übermittlung der Anhörungsunterlagen zum Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679 mit Schreiben vom 19.12.2017 danken wir Ihnen. Der Anwaltsverband nimmt die Gelegenheit zur Stellungnahme gern wahr.

Der Anwaltsverband Baden-Württemberg e. V. ist der freiwillige Zusammenschluss der Rechtsanwältinnen und Rechtsanwälte im Land Baden-Württemberg. Er repräsentiert weit mehr als die Hälfte aller Kolleginnen und Kollegen in Baden-Württemberg und vertritt als größte Anwaltsorganisation dieses Bundeslandes die Interessen der Anwaltschaft in unserem Bundesland und – in Zusammenarbeit mit dem Deutschen Anwaltverein (DAV) – auch auf nationaler und internationaler Ebene.

## 1. Allgemeine Bewertung

- a) Mit der Neufassung des Landesdatenschutzgesetzes BW (LDSG neu) sollen die erforderlichen Anpassungen an die europäische Datenschutzgrundverordnung (DS-GVO) – VO (EU) Nr. 2016/679, die zum 25.05.2018 in Kraft treten wird, erfolgen. Ebenfalls zum 25.05.2018 in Kraft treten wird das neue Bundesdatenschutzgesetz (BDSG neu) vom 30.06.2017 (BGBl. I, S. 2097 ff.).

Die DS-GVO gilt als unmittelbar anwendbares Recht in den Mitgliedstaaten (Art. 99 Abs. 2 DS-GVO) und bedarf daher keines staatlichen Umsetzungsakts. Ihr kommt gegenüber entgegenstehendem nationalem Recht Anwendungsvorrang zu,

grundlegend EuGH, Urteil vom 15.07.1964 - C-6/64 -, Slg. 1964, 1251 (1269 f.) – Costa/E. N. E. L.; vgl. ferner Ruffert: in Calliess/Ruffert (Hrsg.), EUV/AEUV, 5. Aufl., München 2016, Art. 1 Rdnr. 16 ff.

Mit der Anpassungsgesetzgebung setzen die deutschen Bundes- und Landesgesetzgeber letztlich Regelungsaufträge der DS-GVO um und nutzen zudem Öffnungsklauseln, die den Mitgliedstaaten einen eigenständigen Gestaltungsspielraum einräumen. Dieser ist vergleichsweise großzügig bemessen in Art. 23 DS-GVO unter der Überschrift „Beschränkungen“. Demnach können die Mitgliedstaaten von Kerninhalten der Grundverordnung – wie etwa Benachrichtigungs-, Informations- und Auskunftspflichten sowie Berichtigungs- und Löschungspflichten – abweichen, sofern die Maßnahme **„den Wesensgehalt der Grundrechte und Grundfreiheiten achtet“** und sich in einer „demokratischen Gesellschaft“ als notwendig und verhältnismäßig erweist (Art. 23 Abs. 1 DS-GVO). Zu den dort genannten Schutzgütern zählen insbesondere die öffentliche Sicherheit, die Verhütung und Verfolgung von Straftaten sowie sonstige wichtige öffentliche Interessen der Union oder eines Mitgliedstaates. Es zeigt sich, dass die formale Wahl einer Grundverordnung erhebliche Auswirkungen auf den materiellen – grundrechtlich vorgeprägten – Datenschutz hat. Die „Öffnungsklauseln“ definieren nicht nur einen Raum für den einfachgesetzlichen Datenschutz in den Mitgliedstaaten, sondern auch für grundrechtliche Abwägungsentscheidungen (vgl. Art. 1 Abs. 1 DS-GVO). Etwasige Beschränkungen zulasten betroffener Personen stehen jedenfalls unter dem **Vorbehalt der Zulässigkeit nach den europäischen Grundrechten sowie den grundrechtlichen Verbürgungen des Grundgesetzes** und sind eng auszulegen,

so auch Greve, NVwZ 2017, 737 (739); ähnlich Buchholtz, DÖV 2017, 837 (838).

- b) Nunmehr soll – zum einen - das bisherige Landesdatenschutzgesetz aufgehoben werden. Zum anderen sollen im neuen LDSG (Art. 1 des Gesetzentwurfs) im Wesentlichen folgende Bereiche geregelt werden:

- Zulässigkeit der Datenverarbeitung, insbesondere zu anderen Zwecken (§ 5 LDSG – neu).
- Einschränkungen der Betroffenenrechte i. S. v. Art.23 DS-GVO zur Wahrung öffentlicher Interessen (in Abschnitt 3 LDSG neu, wie § 8 LDSG neu Informationspflicht oder § 9 LDSG neu Auskunftsrecht).
- Besondere Verarbeitungssituationen, soweit sie nicht bereichsspezifisch geregelt sind; zu diesen zählt neben der Privilegierung von Wissenschaft und Forschung auch die Videoüberwachung durch öffentliche Stellen und der Beschäftigtendatenschutz (§ 14 LDSG neu).
- Sanktionen bei Verstößen.

Der Entwurf des neuen Landesdatenschutzgesetzes mag in weiten Teilen als gelungen betrachtet werden. Auch verkennen wir nicht, dass sich an vielen Stellen sorgsam austarierte Abwägungsergebnisse finden. Unserer Verbandssatzung gemäß betrachten wir den Entwurf des neuen Landesdatenschutzgesetzes vor allem unter zwei Gesichtspunkten:

- aa) Rechtsanwältinnen und Rechtsanwälte sind **Organe der Rechtspflege**. Dabei haben sie u. a. die Aufgabe, zur Wahrung eines sachgerechten Ausgleichs der geschützten Rechte der Betroffenen im Sinne eines **funktionierenden Rechtsstaats** beizutragen. Die Tätigkeit von Rechtsanwälten liegt daher genauso im öffentlichen Interesse. Zu deren Ausübung brauchen sie für sich und ihre Mandanten einen vertraulichen Schutzraum.
- bb) Darüber hinaus achtet die Anwaltschaft aber auch auf das bedeutsame allgemeine Interesse an der integren Datenverarbeitung durch die öffentlichen Stellen. Die im neuen LDSG zu findenden Regelungen müssen sich daran messen lassen, ob sie zu den Grundrechten und zur DS-GVO konform sind. Sollte dies nicht der Fall sein, wären sie nicht anwendbar. Gerade im Bereich der Datenverarbeitung durch öffentliche Stellen hält sich die DS-GVO zurück. Bei der etwa erforderlich werdenden Auslegung der landesgesetzlichen Datenschutzregelungen ist so zu verfahren, dass die Interpretation unter **Beachtung der Grundrechte der betroffenen Personen** im „Geiste der DS-GVO“ erfolgt und die Ziele erreicht werden, die mit ihr verfolgt werden sollen.
- c) Der vorliegende Entwurf nutzt die Gestaltungsspielräume, die ihm die DS-GVO eröffnet, zum Teil sehr weitgehend aus. Gleichwohl sind die neuen Regelungen und damit auch der vorliegende Entwurf im Vergleich zu den früheren Datenschutzvorschriften keine „Vollregelungen“ mehr, sondern ergänzen die DS-GVO als Annexmaterien; hierbei ist darauf zu achten, dass sich in der Zusammenschau mit der DS-GVO und etwaigen bereichsspezifischen Datenschutzrecht insgesamt ein „rundes“ Bild ergibt. Das Zusammenspiel der einzelnen Regelungsbereiche bestimmt sich nach dem jeweiligen Anwendungsbereich.

- d) Von besonderem Gewicht ist, ob und – bejahendenfalls – inwieweit Berufe mit besonderer Verschwiegenheit wie Ärzte, Anwälte, Steuerberater u. ä. durch Regelungen der in Rede stehenden Art betroffen sind. Aus diesem Grund weisen wir auf deren besondere Situation anhand des Beispiels der Rechtsanwältinnen und Rechtsanwälte, insbesondere die Wahrung des Mandatsgeheimnisses (§ 43a BRAO, § 2 BORA, § 203 StGB), hin. Die berufliche Verschwiegenheit wurde in Art. 90 DS-GVO (Geheimhaltungspflichten als Ausnahme zu Art. 58 DS-GVO) als besonders schutzwürdig anerkannt und durch entsprechende Ermächtigungen der Mitgliedstaaten respektiert. Auf Bundesebene wird diesen Erfordernissen in **§ 29 Abs. 3 BDSG n. F.** Rechnung getragen. Eine vergleichbare Regelung vermissen wir im Entwurf des Landesdatenschutzgesetzes; **§ 12 Abs. 1 LDSG neu bleibt hinter der bundesrechtlichen Lösung deutlich zurück.** Dies fällt umso mehr auf, als der Gesetzentwurf in anderen Punkten über den Regelungsumfang des BDSG hinausgeht.
- aa) Danach wird beispielsweise hinsichtlich der Befugnisse der Aufsichtsbehörden danach unterschieden, ob es sich in einer Kanzlei um personenbezogene Daten aus der – mit einem anderen Unternehmen vergleichbaren – „normalen Kanzleiorganisation“, wie der Beschäftigung von Mitarbeitern oder Bestellung von Büromaterial, handelt oder ob es um mandatsbezogene Daten geht. Bei letzterem sind die Informations- und Auskunftspflichten gegenüber einzelnen Betroffenen beschränkt. Der deutsche Gesetzgeber hat folgerichtig im neuen § 29 BDSG das Recht zum Zugang zu Anwaltskanzleien, -akten und -computern für die Aufsichtsbehörden beschränkt, nicht jedoch das Recht auf Auskunft gem. Art. 58 DS-GVO.

Die besondere Behandlung mandatsbezogener personenbezogener Daten rechtfertigt sich aus der Eigenart der Besorgung von Rechtsgeschäften für Dritte. Typischerweise kommt ein Mandant zum Anwalt mit einem Sachverhalt, in dem er auch die Lebensumstände von Personen schildert, die dem Anwalt gerade nicht das Mandat erteilen wollen, z. B. bei Verkehrsunfällen, Nachbarschaftsstreitigkeiten oder familienrechtlichen Fragen. Es würde die erfolgreiche Tätigkeit eines Anwalts geradezu konterkarieren, müsste er dem potentiellen späteren „Gegner“ oder der Datenschutzbehörde vollumfänglich Auskunft über die in der Kanzlei hinterlegten und verarbeiteten Daten geben. Ein Anwalt kann es auch kaum steuern, welche Informationen ihm sein Mandant, Kollegen oder sonstige Dritte zukommen lassen.

Damit liegt der Sachverhalt anders als z. B. im Verhältnis Patient – Arzt. Ein Patient wird seinem Arzt typischerweise vorwiegend personenbezogene Daten nur von sich selbst preisgeben, eventuell auch über ihm bekannte Blutsverwandte hinsichtlich etwaiger vererbbarer Krankheiten. Damit ist der Kreis von Personen, über die personenbezogene Daten zum – ebenfalls zur Verschwiegenheit verpflichteten – Arzt gelangen naturgemäß viel

ANWALTSVERBAND BADEN-WÜRTTEMBERG E. V.

Schr. vom 31. Januar 2018, Seite 5

enger als eben beim Rechtsanwalt, der im konkreten Mandat Informationen über einen enorm weitreichenden – bis dahin unbekannt – Personenkreis, z. B. bei Massentlassungen, erhalten kann.

Ähnlich wäre auch die Situation beim Steuerberater, der vom Mandanten nur Informationen über Personen erhält, mit denen dieser in Verbindung steht, wie ein Vertragspartner und der diese auch nur gegenüber den Finanzbehörden anwenden soll.

- bb) Aus diesen Gründen hatte das Kammergericht Berlin im Jahr 2010 noch zu §§ 38 Abs. 3 Satz 1, 43 Abs. 1 Nr. 10 BDSG a. F. (bußgeldbewehrtes Auskunftsverlangen der Aufsichtsbehörde) entschieden, dass ein Rechtsanwalt nicht verpflichtet ist, dem Datenschutzbeauftragten mandatsbezogene Informationen zu erteilen, die seiner Verschwiegenheitspflicht unterliegen,

vgl. KG Berlin, Beschluss vom 20.08.2010 - 1 Ws (B) 51/07 -, AnwBl. 2010, 802

Die grundlegenden Gedanken, die zu dieser Entscheidung führten, sollten auch zukünftig beachtet werden. **Das LDSG ist deshalb um eine § 29 Abs. 3 BDSG n. F. entsprechende Regelung zu ergänzen.**

Die einzurichtende unabhängige Aufsichtsbehörde sollte darüber hinaus entsprechend sensibilisiert sein. Nach Art. 40 DS-GVO soll die Ausarbeitung von Verhaltensregeln (Codes of Conduct), u. a. von Berufsverbänden, gefördert werden. Sollte die Anwaltschaft zu solchen, ihre besonderen Interessen wahren, Verhaltensregeln gelangen, sollten diese bei der Handhabung des Gesetzes auch entsprechend Anwendung finden.

- e) Der Gesetzentwurf setzt die **bedenkliche Tendenz, den Rechtsschutz der Betroffenen und damit den Datenschutz selbst einzuschränken**, fort, die wir bereits im Zusammenhang mit der Novellierung des Landespolizeigesetzes und des Landesverfassungsschutzgesetzes beanstandet hatten. Auf unsere diesbezüglichen Stellungnahmen vom 08.08.2017 zum Polizeigesetz und vom 14.08.2017 zum Verfassungsschutzgesetz nehmen wir Bezug.

Der Auskunftsanspruch betroffener Personen dient der Verwirklichung ihrer Grundrechte, namentlich des Grundrechts auf informationelle Selbstbestimmung, und auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme; mit diesem Auskunftsanspruch soll die Betroffenen in die Lage versetzt werden im Nachhinein Rechtsschutz zu erlangen. Die Effektivität ihres Rechtsschutzes wird durch die erst nachträgliche Gewährung ohnehin zugunsten der Aufgabenwahrnehmung der öffentlichen Stellen zurückgedrängt. Diesen Auskunftsanspruch – wie hier –

teils mit einer nicht tragfähigen oder gar gänzlich ohne Begründung zusätzlich einzuschränken, ist unvertretbar und findet im Rahmen einer Abwägung des Grundrechtsschutzes des Betroffenen gegen das öffentliche Interesse an der Aufgabenerfüllung keine Stütze.

## 2. Im Einzelnen

Wegen des Umfangs des Gesetzentwurfs und seiner Begründung beschränken wir uns nachfolgend auf diejenigen Punkte, in denen wir dringenden Korrekturbedarf sehen.

### a) LDSG – neu

#### aa) Zu § 1 – Zweck des Gesetzes

Positiv zu vermerken ist hier, dass nicht nochmals die Zwecke wiederholt werden, sondern der rechtstechnische Bezug zur DS-GVO hergestellt wird. Deutlich wird so der ergänzende Charakter der Normen.

#### bb) Zu § 2 Abs. 3 – Subsidiarität

Ausweislich der Begründung des Gesetzentwurfs gehen spezifische Rechtsvorschriften des Bundes und des Landes den allgemeinen Regelungen des Landesdatenschutzgesetzes grundsätzlich vor. Im Übrigen kommt dem Landesdatenschutzgesetz lückenfüllende Auffangfunktion zu, soweit keine oder keine vollständige bereichsspezifische Regelung vorliegt. Eine solche Subsidiaritätsklausel ist aus Gründen der Rechtsklarheit und damit der Rechtssicherheit zu begrüßen.

Allerdings ergibt sich gerade insoweit ein Problem mit Blick auf die **Berufsverschwiegenheit**:

Gemäß § 29 Abs. 3 BDSG n. F. bestehen gegenüber den in § 203 Absatz 1, 2a und 3 des Strafgesetzbuchs genannten Personen oder deren Auftragsverarbeitern die Untersuchungsbefugnisse der Aufsichtsbehörden gemäß Art. 58 Abs. 1 Buchst. e und f VO (EU) 2016/679 nicht, soweit die Inanspruchnahme der Befugnisse zu einem Verstoß gegen die Geheimhaltungspflichten dieser Personen führen würde. Erlangt eine Aufsichtsbehörde im Rahmen einer Untersuchung Kenntnis von Daten, die einer Geheimhaltungspflicht im Sinne des Satzes 1 unterliegen, gilt die Geheimhaltungspflicht auch für die Aufsichtsbehörde.

Diese Bestimmung, die die Berufsverschwiegenheit auf der Ebene des Bundesrechts wahrt, gilt für öffentliche Stellen der Länder nur, soweit der Datenschutz nicht durch Landesgesetz geregelt ist, und diese Stellen Bundesrecht ausführen oder als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt (§ 1 Abs. 1 Nr. 2 BDSG n. F.). Sie gilt somit gerade nicht im hier interessierenden Zusammenhang. Folglich bedarf es – wie zuvor ausgeführt – eine § 29 Abs. 3 BDSG n. F. entsprechenden Regelung auch im Landesdatenschutzgesetz.

cc) **§ 5 – Datenverarbeitung zu anderen Zwecken**

Der hier anzulegende Maßstab ergibt sich aus Art. 6 Abs. 4 DS-GVO; danach begegnet die Regelung in zweifacher Hinsicht erheblichen Bedenken:

- Nach § 5 Abs. 1 Nr. 3 LDSG neu soll die Datenverarbeitung zu einem anderen als dem Erhebungszweck ohne Einwilligung des Betroffenen zulässig sein, wenn sich bei der rechtmäßigen Aufgabenerfüllung Anhaltspunkte für Straftaten oder **Ordnungswidrigkeiten** ergeben und die Unterrichtung der für die Verhütung, Verfolgung oder Vollstreckung zuständigen Behörden geboten erscheint. Art. 6 Abs. 4 Buchst. c DS-GVO verweist auf § 10 DS-GVO und erklärt damit nur Straftaten zum Rechtfertigungsgrund, nicht aber bloße Ordnungswidrigkeiten. Dies geht angesichts der Bandbreite möglicher Ordnungswidrigkeitstatbestände zu weit. Es ist zumindest eine Beschränkung auf Ordnungswidrigkeiten von erheblicher Bedeutung vorzunehmen, wie dies etwa in § 17 Abs. 3 LDSG neu geschehen ist.
- Nach § 5 Abs. 3 LDSG neu soll eine Information der betroffenen Person über die Datenverarbeitung nach Absatz 1 Nummern 1 bis 4 nicht erfolgen, soweit und solange hierdurch der Zweck der Verarbeitung gefährdet würde und die Interessen der öffentlichen Stelle an der Nichterteilung der Information die Interessen der betroffenen Person überwiegen. Dies vermag nicht zu überzeugen, weil nicht ersichtlich ist, welche Interessen die öffentliche Stelle haben könnte, die über den Zweck der Datenverarbeitung hinausgehen oder sich von diesem unterscheiden könnten.

Der Verwaltungsaufwand, der – sofern er unverhältnismäßig ist - nach Art. 14 Abs. 5 Buchst. b DS-GVO einen Wegfall der Informationspflicht begründet kann,

wird im Entwurf des Landesgesetzes noch nicht einmal erwähnt. Die deshalb europarechtlich zu stellende Frage nach dem Verhältnis zwischen dem letztlich grundrechtlich geschützten Auskunftsbegehren des Betroffenen und dem Verwaltungsaufwand der Behörde kann nur im Einzelfall im Rahmen einer konkreten Abwägung getroffen werden. Dies kommt weder im Gesetzentwurf noch in dessen Begründung zum Ausdruck; für den Gesetzesvollzug ist deshalb zu befürchten, dass die öffentliche Stelle auf nur den ihr entstehenden Aufwand abstellt.

Diese Alternative ist im Hinblick auf das Grundrecht der informationellen Selbstbestimmung unverhältnismäßig und deshalb abzulehnen.

Außerdem sollte in diesem Zusammenhang noch den innerbehördlichen Datenaustausch zu regeln. Dabei sollten Gesichtspunkte, wie das sog. „Once Only Prinzip“, also die Frage, welche öffentliche Stelle mit welcher anderen öffentliche Stelle unter welchen Bedingungen Daten austauschen darf, berücksichtigt werden. Wir können derzeit nicht erkennen, dass dies etwa in § 7 LDSG neu geregelt ist. Zu beachten sein werden hierbei der Grundsatz der Zweckbindung (Art. 5 DS-GVO), die Zulässigkeit einer etwaigen Zweckänderung bei Vereinbarkeit mit Erhebungszweck (Art. 6 DS-GVO) sowie die Fragen nach der Notwendigkeit und Verhältnismäßigkeit (Art. 23 DS-GVO).

**dd) § 7 – Datenverarbeitung in der gemeinsamen Dienststelle**

Wie zuvor ausgeführt, vermissen wir eine Regelung über den innerbehördlichen Datenaustausch, die den Anforderungen der DS-GVO genügt.

**ee) § 8 – Beschränkungen der Informationspflicht (Rechte der Betroffenen)**

Die geplanten Beschränkungen der Betroffenenrechte sind aufgrund von Art. 23 DS-GVO möglich, müssen sich aber an Art. 13 und 14 DS-GVO und dem Transparenzgebot des Art. 5 DS-GVO sowie den Grundrechten messen lassen. Danach sind die Einschränkungen als zu weit reichend abzulehnen:

- § 8 Abs. 1 Satz Nr. 2 LDSG neu rechtfertigt einen Wegfall der Informationspflicht auch bei der Verfolgung von Ordnungswidrigkeiten. Dies geht deutlich über Art. 23 DS-GVO hinaus; dort ist nur von der Verfolgung von Straftaten oder der Strafvollstreckung die Rede. Es kann nicht sein, dass jede Ordnungswidrigkeit zu einer Ausnahme berechtigt. Erforderlich sein müssen schon Ordnungswidrigkeiten von erheblicher Bedeutung sein wie etwa in § 17 Abs. 3 LDSG neu.

- Bedenklich erscheint auch § 8 Abs. 1 Satz 1 Nr. 3 LDSG neu, denn welche Interessen kann die öffentliche Stelle an der Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche haben, die durch die Information der betroffenen Person beeinträchtigen würden? Art. 23 Abs. 1 Buchst. j DS-GVO ermächtigt zwar insoweit zu einer Beschränkung, diese Ermächtigung vermag aber eine Begründung nicht zu ersetzen! Eine Begründung nennt jedoch weder der Entwurf noch dessen Begründung noch ist sonst eine ersichtlich. Regelmäßig ist eine öffentliche Stelle an einer zivilrechtlichen Auseinandersetzung unter Privaten nicht beteiligt; sie hat insoweit folglich keine eigenen Interessen. Aus diesem Grund ist es ihr verwehrt, durch Unterlassen der Auskunft den Ausgang einer zivilrechtlichen Auseinandersetzung unter Privaten zu beeinflussen.

Die Beteiligung einer öffentlichen Stelle an einer zivilrechtlichen Auseinandersetzung ist dagegen insbesondere bei Amtshaftungs-, Entschädigungs- und ähnlichen Prozessen denkbar, mithin im Rahmen der Staatshaftung. Gerade hier wäre es mit dem Rechtsstaatsprinzip, dem Gebot eines fairen Verfahrens und dem Gebot der Waffengleichheit unvereinbar, wenn die öffentliche Stelle ihr eigenes Interesse bzw. dasjenige ihres Trägers (an einer Vermeidung der Haftung bzw. Entschädigung) höher gewichten dürfte als das Informationsinteresse des Betroffenen.

Dies zeigt, dass die beabsichtigte Regelung dringend einer tragfähigen Begründung bedarf und ohne eine solche nicht Gesetz werden darf.

Die in diesem Zusammenhang vorgesehene Dokumentationspflicht ist in der Tat unverzichtbar, um die Möglichkeit nachteilenden Rechtsschutzes zu gewährleisten, vermag aber die zuvor gerügten Defizite nicht auszugleichen.

**ff) § 9 – Beschränkungen des Auskunftsrechts**

§ 9 LDSG neu soll Art. 15 DS-GVO ergänzen und bezieht sich auf die für den Wegfall der Informationspflicht in § 8 Abs. 1 LDSG neu genannten Gründe, die um die Datensicherung und die Datenschutzkontrolle erweitert werden.

- Nach § 9 Abs. 1 Satz 2 LDSG neu soll die betroffene Person keine Auskunft verlangen können, soweit und solange die personenbezogenen Daten ausschließlich zu Zwecken der Datensicherung oder der Datenschutzkontrolle gespeichert sind und eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist und deswegen das Interesse der betroffenen Person an der Auskunftserteilung zurücktreten muss.

In dieser Form ergibt die Regelung keinen Sinn. Die Begründung stellt nur auf Sicherungsdaten ab und ist insoweit möglicherweise noch nachvollziehbar. Inwiefern aber die Datenschutzkontrolle einen Wegfall der Auskunftspflicht rechtfertigen können soll, erschließt sich nicht. Etwas anderes könnte gegebenenfalls gelten, wenn sich diese Kontrolle auf die Sicherungsdaten erstrecken sollte - was sinnvoll wäre -, aber so nicht im Gesetz steht.

- Gemäß § 9 Abs. 2 LDSG neu kann die öffentliche Stelle – sofern sie eine große Menge von Informationen über die betroffene Person verarbeitet - verlangen, dass die betroffene Person präzisiert, auf welche Information oder welche Verarbeitungsvorgänge sich ihr Auskunftsersuchen bezieht. Kommt die betroffene Person dem Verlangen nicht nach, kann die Auskunft verweigert werden, soweit die Auskunftserteilung einen unzumutbaren Aufwand auslösen würde.

Die Begründung verweist insoweit auf den Erwägungsgrund Nr. 63, der jedoch selbst **keine Ermächtigungsgrundlage** darstellt. Überdies muss die betroffene Person überhaupt wissen, welche Informationen und Verarbeitungsvorgänge von der öffentlichen Stelle gespeichert bzw. vorgenommen wurden, um eine Präzisierung vornehmen zu können. Folglich kann die Stelle die Auskunft nicht einfach mit der Begründung verweigern, die Datenmenge sei riesig; sie muss der betroffenen Person zumindest übersichtsartig der Art nach mitteilen, welche Daten gespeichert bzw. verarbeitet wurden, damit diese eine Präzisierung vornehmen kann.

- § 9 Abs. 5 LDSG neu sieht vor, dass – wenn der betroffenen Person keine Auskunft erteilt wird – die Auskunft ist auf deren Verlangen der oder dem Landesbeauftragten für den Datenschutz zu erteilen, soweit nicht die jeweils zuständige oberste Landesbehörde im Einzelfall feststellt, dass dadurch die Sicherheit des

ANWALTSVERBAND BADEN-WÜRTTEMBERG E. V.

Schr. vom 31. Januar 2018, Seite 11

Bundes oder eines Landes gefährdet würde. Die Mitteilung der oder des Landesbeauftragten für den Datenschutz an die betroffene Person über das Ergebnis der datenschutzrechtlichen Prüfung darf keine Rückschlüsse auf den Erkenntnisstand der öffentlichen Stelle zulassen, sofern diese nicht einer weiter gehenden Auskunft zustimmt.

Das Bundesverfassungsgericht hat in seiner Entscheidung

BVerfG, Urteil vom 15.12.1970 – 2 BvF 1/69 –, BVerfGE 30, 1,

ausgeführt, dass das Prinzip der Gewaltenteilung es erlaube, dass Rechtsschutz gegenüber Maßnahmen der Exekutive ausnahmsweise nicht durch Gerichte, sondern durch vom Parlament bestellte oder gebildete unabhängige Institutionen innerhalb des Funktionsbereichs der Exekutive gewährt wird. Diese Ausnahme vom Richtervorbehalt ist demgemäß nach Art. 10 Abs. 2 GG zum „Schutze der freiheitlichen demokratischen Grundordnung oder des Bestandes oder der Sicherung des Bundes oder eines Landes“ zulässig.

Das Bundesverfassungsgericht stellt somit sehr hohe Anforderungen, wenn der Rechtsschutz durch Gerichte ausgeschlossen werden soll, denen allenfalls § 8 Abs. 1 Nr. 1 LDSG neu genügen dürfte, keinesfalls aber § 8 Abs. 1 Nr. 2, 3 und 4 LDSG neu. Damit stellt sich die Frage nach dem Rechtscharakter dieser Beschwerde und seiner Entscheidung durch die oder den Landesdatenschutzbeauftragten. Letztere dürfte wohl Verwaltungsaktscharakter haben und den hierfür gegebenen Rechtsweg eröffnen.

Dies beantwortet aber noch nicht die vorgängige Frage nach dem Charakter der behördlichen Ablehnungsentscheidung. Auch hier wird von einem Verwaltungsakt auszugehen sein. Insofern drängt sich die Parallele zu der Entscheidung über ein Auskunftsbegehren nach dem Informationsfreiheitsgesetz des Landes Baden-Württemberg (LIFG) auf, für die in der Rechtsprechung geklärt ist, dass sie alle Voraussetzungen eines Verwaltungsakts nach § 35 S 1 LVwVfG erfüllt,

vgl. VG Freiburg, Urteil vom 17.05.2017 – 1 K 1802/16 – juris.

Der Anwendungsbereich für die Beschwerde an die oder den Landesdatenschutzbeauftragten erscheint deshalb eng. Dies wirft die Frage auf, mit welcher Berechtigung nach der durch die Verwaltungsgerichtsordnung vorgenommenen

Vereinheitlichung durch Abschaffung unterschiedlicher Verwaltungsbeschwerde und Einführung des einheitlichen Widerspruchsverfahrens die Regelung getroffen wird. Sie kann allenfalls mit einer Entlastung der Verwaltungsgerichte begründet werden; ob eine solche tatsächlich eintritt, kann bezweifelt werden.

Dass es sich bei der Entscheidung der oder des Landesdatenschutzbeauftragten um einen Verwaltungsakt handelt, ergibt sich aus Folgendem: Die oder der Landesdatenschutzbeauftragte hat umfassend zu prüfen, ob und inwieweit die rechtlichen Voraussetzungen eines Informationsanspruchs gegeben sind und ihm gegebenenfalls Verweigerungsgründe entgegenstehen. Dabei hat sie oder er eine umfassende Güter- und Interessenabwägung zu treffen. In dieser differenzierten Entscheidung liegt die Regelung, die entscheidend für das Vorliegen eines Verwaltungsakts i. S. des § 35 LVwVfG spricht. Sie oder er trifft jedenfalls eine Einzelfallregelung auf dem Gebiet des öffentlichen Rechts mit unmittelbarer Rechtswirkung nach außen.

Dieses Verständnis steht im Einklang mit Art. 79 Abs. 1 DS-GVO. Danach hat jede betroffene Person hat unbeschadet eines verfügbaren verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs einschließlich des Rechts auf Beschwerde bei einer Aufsichtsbehörde gemäß Artikel 77 das Recht auf einen wirksamen gerichtlichen Rechtsbehelf, wenn sie der Ansicht ist, dass die ihr aufgrund dieser Verordnung zustehenden Rechte infolge einer nicht im Einklang mit dieser Verordnung stehenden Verarbeitung ihrer personenbezogenen Daten verletzt wurden.

Auf dem Gebiet des öffentlichen Rechts ist der gerichtliche Rechtsbehelf die Klage zum Verwaltungsgericht, die als Anfechtungs- und Verpflichtungsklage gemäß § 42 VwGO einen Verwaltungsakt und die Durchführung eines Widerspruchsverfahrens voraussetzt.

**gg) § 12 – Amtsgeheimnis, Berufsgeheimnis**

Wie bereits eingangs ausgeführt, ist die Regelung in § 12 Abs. 1 LDSG neu unzureichend, den sie betrifft nur die Übermittlung von Daten einer zur Verschwiegenheit verpflichteten Person an eine öffentliche Stelle, nicht aber die Aufsicht über die berufsverschwiegenen Berufsträger bzw. die in § 203 StGB genannten Personen. Deren Grundrechtsschutz ge-

bietet jedoch eine Regelung entsprechend § 29 Abs. 3 BDSG neu auch im Landesdatenschutzrecht. Zur Vermeidung unnötiger Wiederholungen verweisen wir auf die einleitenden Ausführungen unter Nr. 1 d dieser Stellungnahme Bezug.

hh) **§ 13 - Wissenschaftliche Forschung privilegiert (Art. 5 DS-GVO)**

Die hier getroffene Regelung scheint grundsätzlich mit Art. 9 DS-GVO vereinbar. Allerdings erschließt sich der Sinn des § 13 Abs. 4 LDSG neu nicht; danach werden die Rechte der Betroffenen insoweit beschränkt, als die Wahrnehmung dieser Rechte die jeweiligen Forschungs- oder Statistikzwecke unmöglich machen oder ernsthaft beeinträchtigen würde und die Beschränkung für das jeweilige Forschungs- oder Statistikinteresse erforderlich ist.

Die Beschränkungen erscheinen mit Art. 9 DS-GVO vereinbar, soweit anderenfalls Forschungs- oder Statistikzwecke vereitelt oder ernsthaft beeinträchtigt würden. Inwiefern aber die Beschränkung für das jeweilige Forschungs- oder Statistikinteresse erforderlich sein kann, wird nicht deutlich. Es wird weder begründet noch ist sonst nicht ersichtlich, inwieweit Interesse an Forschung und Statistik über das durch die erste Alternative geschützte Interesse an der Aufgabenerfüllung hinausgehen können sollte.

ii) **§ 16 – Verarbeitung besonderer Kategorien personenbezogener Daten**

§ 16 LDSG neu will die Verarbeitung besonderer Kategorien personenbezogener Daten Erhebliches gestatten, wenn erhebliches öffentliches Interesse besteht oder dies zur Abwehr einer erheblichen Gefahr für öffentliche Sicherheit erforderlich und die die Interessen der öffentlichen Stelle an der Datenverarbeitung die Interessen der betroffenen Person überwiegen.

Mit der Verwendung des Begriffs der besonderen Kategorien personenbezogener Daten knüpft die Bestimmung an Art. 9 Abs. 1 DS-GVO; mithin an ein Verbot mit Erlaubnisvorbehalt an, wobei sich Letzterer konkret ausweislich der Begründung aus Art. 9 Abs. 2 Buchst. g DS-GVO ergeben soll. § 16 LDSG neu verweist aber auf §§ 13 bis 15 LDSG neu und die „Bestimmungen der Verordnung (EU) 2016/679“ und somit ihrerseits wiederum auf etliche Normen, die rechtstechnisch als Verbote mit Erlaubnisvorbehalte ausgestaltet sind. Dies macht die Rechtsanwendung unnötig kompliziert, vorzugswürdig erscheint deshalb etwa folgende Formulierung:

*„Abweichend von Art. 9 Abs. 1 der Verordnung (EU) 2016/679 ist die Verarbeitung der dort genannten besonderen Kategorien personenbezogener Daten durch öffentliche Stellen zulässig, wenn ...“*

§ 22 BDSG n. F. ist ähnlich formuliert.

jj) **§ 17 - Videoüberwachung öffentlich zugänglicher Räume**

Die Regelung dürfte mit den Vorgaben der Art. 6, 13, 14 und 17 DS-GVO übereinstimmen und erscheint infolgedessen grundsätzlich zulässig.

Bei der nach § 17 Abs. 1 LDSG neu vorzunehmenden Interessenabwägung gemäß § 6b Abs. 1 und Abs. 3 BDSG in der derzeit noch geltenden Fassung, ist die durch das Videoüberwachungsverbesserungsgesetz vom 28.04.2017 (BGBl. I 968) eingeführte normative Gewichtungsvorgabe zugunsten der Zulässigkeit einer Videoüberwachung zu beachten,

vgl. NdsOVG, Urteil vom 07.09.2017 – 11 LC 59/16 –, juris,

§ 6b BDSG der gegenwärtigen Fassung stimmt mit § 4 BDSG in der ab 25.05.2018 geltenden Fassung überein; sie ist hinsichtlich ihres Anwendungsbereichs wesentlich konkreter gefasst und lautet:

**„§ 4 Videoüberwachung öffentlich zugänglicher Räume**

(1) Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit sie

1. zur Aufgabenerfüllung öffentlicher Stellen,
2. zur Wahrnehmung des Hausrechts oder
3. zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke

erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Bei der Videoüberwachung von

1. öffentlich zugänglichen großflächigen Anlagen, wie insbesondere Sport-, Versammlungs- und Vergnügungstätten, Einkaufszentren oder Parkplätzen, oder
2. Fahrzeugen und öffentlich zugänglichen großflächigen Einrichtungen des öffentlichen Schienen-, Schiffs- und Busverkehrs

gilt der Schutz von Leben, Gesundheit oder Freiheit von dort aufhältigen Personen als ein besonders wichtiges Interesse.

(2) Der Umstand der Beobachtung und der Name und die Kontaktdaten des Verantwortlichen sind durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt erkennbar zu machen.

(3) Die Speicherung oder Verwendung von nach Absatz 1 erhobenen Daten ist zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Absatz 1 Satz 2 gilt entsprechend. Für einen anderen Zweck dürfen sie

nur weiterverarbeitet werden, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist.

(4) Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, so besteht die Pflicht zur Information der betroffenen Person über die Verarbeitung gemäß den Artikeln 13 und 14 der Verordnung (EU) 2016/679. § 32 gilt entsprechend.

(5) Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.“

(§ 4 BDSG in der Fassung vom 30.6.2017)

Der Vergleich veranschaulicht die Weite des Anwendungsbereichs, den § 17 Abs. 1 LDSG neu eröffnen will. Auf „öffentlich zugängliche Räume“ wird nur in der Überschrift verwiesen; jegliche Konkretisierung unterbleibt hingegen. Die Begründung nennt als Anwendungsfälle dieser Norm Personen- und Objektschutz, also den Schutz von Personen, die sich in öffentlichen Objekten oder in deren Nähe aufhalten, sowie den Schutz der Objekte selbst sein, soweit sie die Funktionsfähigkeit der öffentlichen Stellen gewährleisten und damit mittelbar auch deren Aufgabenerfüllung dienen. Als öffentliche Objekte können Kulturgüter, öffentliche Einrichtungen, Dienstgebäude oder öffentliche Verkehrsmittel angesehen werden.

Problematisch kann diese Weite des Anwendungsbereichs werden, wenn – wie in einem Fall in Weimar, in dem die Videoüberwachung einer öffentlichen Straße am 20.02.2004 die Eingangstür einer Rechtsanwaltskanzlei umfasste – in die geschützte Kommunikationssphäre zur Verschwiegenheit verpflichteter Berufsträger eingreift. Das Zeugnisverweigerungsrecht des Berufsträgers und seine Verschwiegenheitspflicht umfassen aus guten Grund nicht nur jede Information aus dem Inhalt des Mandantenverhältnisses, sondern bereits den Umstand des Bestehens eines Mandatsverhältnisses als solchen. Darüber hinaus birgt die Überwachung etwa der Eingangstür zur Rechtsanwaltskanzlei einen mittelbaren Eingriff in die durch Art. 12 GG geschützte Berufsausübungsfreiheit der betroffenen Rechtsanwälte.

Der Gesetzentwurf betont zwar auch in diesem Zusammenhang die schutzwürdigen Interessen betroffener Personen – hier: der betroffenen Berufsträger –, im Gesetzesvollzug ist auf diesen Aspekt jedoch in besonderem Maße zu achten.

Unabhängig davon vermissen wir die Anordnung einer vorherigen **Datenschutz-Folgenabschätzung**, die Art. 35 Abs. 3 Buchst. c DS-GVO bei systematischer Überwachung öffentlich zugänglicher Bereiche zwingend vorsieht. Der Gesetzentwurf und dessen Begründung vermitteln den Eindruck, als solle lediglich rückblickend eine Interessenabwägung

ANWALTSVERBAND BADEN-WÜRTTEMBERG E. V.

Schr. vom 31. Januar 2018, Seite 16

vorgenommen werden. Eine solche Praxis würde Art. 35 Abs. 3 Buchst. c DS-GVO nicht gerecht.

**b) Änderungen anderer Gesetze**

Gegen die vorgesehenen Folgeänderungen weiterer Gesetze bestehen unsererseits keine grundsätzlichen Bedenken.

**3. Ergebnis**

Nach allem erscheint der Gesetzentwurf im Wesentlichen gelungen. Defizite offenbart das Landesdatenschutzgesetz in der Entwurfsfassung jedoch in Bezug auf den Schutz der in § 203 StGB genannten Berufsträger im Besonderen und hinsichtlich des (Grundrechts-)Schutzes der betroffenen Personen im Allgemeinen. Erforderlich ist deshalb zum einen die Ergänzung des LDSG um eine § 29 Abs. 3 BDSG n. F. entsprechende Regelung. Zum anderen sind die vorgesehenen Beschränkungen der Rechte Betroffener durch den beabsichtigten Wegfall von Informations- und Auskunftspflichten öffentlicher Stellen nicht hinnehmbar; es fehlt zum Teil an Konkretisierungen vor dem Hintergrund des Grundrechts auf informationelle Selbstbestimmung, die eine sachgerechte Interessenabwägung überhaupt erst ermöglichen; zum Teil mangelt es tragfähigen Begründungen für die offenbar gewollten Einschränkungen.

Wir würden uns freuen, wenn unsere Hinweise und Vorschläge Berücksichtigung finden würden. Für etwaige Rückfragen oder auch Gespräche stehen wir selbstverständlich gerne zur Verfügung. Sollte im Laufe des weiteren Verfahrens eine weitere Anhörung durchgeführt werden, bitten wir um eine Unterrichtung und die Gelegenheit zur Äußerung.

Mit freundlichen Grüßen



Prof. Dr. Peter Kothe  
Präsident



BADEN-WÜRTTEMBERG

AOK Baden-Württemberg  
Postfach 10 29 54 · 70025 Stuttgart

**per E-Mail**  
Ministerium für Inneres, Digitalisie-  
rung und Migration  
Baden-Württemberg

Postfach 10 34 65  
70029 Stuttgart

**Hauptverwaltung**

Presselstraße 19 · 70191 Stuttgart  
Postfach 10 29 54 · 70025 Stuttgart  
Telefon 0711 2593-0  
Telefax 0711 2593-100  
www.aok-bw.de

Unser Zeichen  
I.05.2/cr/kir  
Ihr Zeichen/Ihre Nachricht vom

Datum  
31.01.2018

**Anhörung zum Entwurf eines Gesetzes zur Anpassung des allgemeinen Daten-  
schutzes und sonstiger Vorschriften an die Verordnung (EU) 2016/679**

Sehr geehrte Damen und Herren,  
sehr geehrte Frau

wir möchten uns für die Möglichkeit der Stellungnahme bedanken und nutzen diese  
um zum § 27 des oben genannten Entwurfes Stellung zu nehmen:

Der § 27 des Entwurfes behandelt die Geldbußen bei Verstößen. Hier ist folgender  
Text vorgesehen:

*„Gegen öffentliche Stellen im Sinne des § 2 Absatz 1 und 2 dürfen keine Geldbußen  
verhängt werden, **es sei denn, die öffentlichen Stellen nehmen als Unternehmen  
mit eigener Rechtspersönlichkeit am Wettbewerb teil.**“*

Der fett gekennzeichnete Teil ist aus unserer Sicht problematisch, wenn die AOK Ba-  
den-Württemberg als ein Unternehmen mit eigener Rechtspersönlichkeit und Teil-  
nahme am Wettbewerb gilt. Im Falle von Datenschutzverstößen wäre das Verhängen  
eines Bußgeldes gegen die AOK Baden-Württemberg möglich, wenn sie dem Lan-  
desdatenschutzgesetz (LDSG) unterliegt. Dies ist beispielsweise der Fall, wenn sie  
als Arbeitgeber handelt.

Handelt die AOK Baden-Württemberg im Rahmen der Sozialgesetzbücher (SGB)  
(z. B. als Kranken- oder Pflegekasse) sind Bußgelder ausgeschlossen. Der § 85a  
Absatz 3 des neuen SGB X regelt hier folgendes:

*„Gegen Behörden und sonstige öffentliche Stellen werden keine Geldbußen ver-  
hängt.“*

Vorsitzende des Verwaltungsrates  
Peer-Michael Dick < > Monika Lersmacher

Vorstand  
Dr. Christopher Hermann – Vorsitzender –  
Siegmar Nesch – Stellvertretender Vorsitzender –

Seite 1 von greenAOK



Auch das neue Bundesdatenschutzgesetz (BDSG-neu), welches für Krankenkassen gilt die in mehr als drei Bundesländern tätig sind, regelt in § 43 Abs. 3 folgendes:

*„Gegen Behörden und sonstige öffentliche Stellen im Sinne des § 2 Absatz 1 werden keine Geldbußen verhängt.“*

§ 2 Abs. 1 lautet wie folgt:

*„Öffentliche Stellen des Bundes sind Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Bundes, der bundesunmittelbaren Körperschaften, der Anstalten und Stiftungen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform.“*

In der Konsequenz würde die AOK Baden-Württemberg gegenüber Krankenkassen, die unter das BDSG-neu oder unter ein LDSG, welches die Zahlung von Bußgeldern ausschließt, fallen, benachteiligt werden. Diese Benachteiligung gilt aus unserer Sicht auch für alle anderen gesetzlichen Krankenkassen die unter das LDSG Baden-Württemberg fallen.

Wir schlagen deshalb vor, dass die Formulierung des BDSG-neu (ggf. zusätzliche Aufnahme des 2. Absatzes des § 2) auch für das LDSG-neu in Baden-Württemberg übernommen wird. Mindestens sollte jedoch klargestellt werden, was unter den „öffentlichen Stellen die als Unternehmen mit eigener Rechtspersönlichkeit am Wettbewerb teilnehmen“ verstanden wird und, dass die gesetzlichen Krankenkassen im Zusammenhang mit dem LDSG hiermit ausdrücklich nicht gemeint sind.

Wir hoffen Ihnen mit unserer Stellungnahme bei der Erstellung dieses wichtigen Gesetzes behilflich zu sein und stehen für Fragen gerne zur Verfügung.

Mit freundlichen Grüßen  
Im Auftrag

A handwritten signature in blue ink, appearing to read 'Simone Szabo', written over a light blue circular stamp.

Simone Szabo  
Datenschutzbeauftragte



## Baden-Württemberg

MINISTERIUM FÜR INNERES, DIGITALISIERUNG UND MIGRATION  
Arbeitsgemeinschaft der Hauptpersonalratsvorsitzenden des Landes Baden-Württemberg (ARGE-HPR)

ARGE-HPR beim Innenministerium Baden-Württemberg  
• Pf. 10 34 65 • 70029 Stuttgart

Datum 31. Januar 2018

Name Tilly Bair

Abteilung 2  
im Hause

Aktenzeichen ARGE-HPR-055/zu 6639  
(Bitte bei Antwort angeben)

—  
 Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679

—  
Sehr geehrte Damen und Herren,

vielen Dank für die Übersendung der Unterlagen zur o.g. Anpassung des allgemeinen Datenschutzrechts. Die ARGE-HPR nimmt hierzu wie folgt Stellung:

Grundsätzlich sei angemerkt, dass die vorgenannte beabsichtigte Neuregelung des allgemeinen Datenschutzrechts durch die vorgesehene Regelungstechnik zu erheblicher Intransparenz führt. Das neue Landesdatenschutzgesetz enthält keine vollständige Regelung der allgemeinen datenschutzrechtlichen Anforderungen mehr. Stattdessen ist wegen der unmittelbaren Geltung der EU-Verordnungen beabsichtigt, lediglich ergänzende Regelungen vorzunehmen, soweit diese aufgrund des verbleibenden Regelungsspielraums möglich sind. Wer die Rechtslage nun erfassen möchte, muss deshalb sowohl die EU Datenschutzverordnung (DSGVO) als auch das neue Landesdatenschutzgesetz (LSDG – neu) im Blick haben. Dies führt unserer Ansicht nach sowohl für die Bürger und Bürgerinnen als auch für die Mitarbeitenden der Landesverwaltung, die das Datenschutzrecht umsetzen und anwenden müssen, zu einer erheblichen Erschwernis. Aus Sicht der ARGE-HPR kann nicht ausgeschlossen wer-

- 2 -

den, dass das Datenschutzniveau dadurch eher sinkt als steigt. So ist es beispielsweise wesentlich schwieriger als zuvor, herauszufinden, dass die Dienststellen ein Verzeichnisse führen müssen, obwohl sich die Dokumentationspflichten verschärft haben. Die Dokumentationspflichten sind ausschließlich in der DSGVO im Art. 30 zu finden, wobei die Art. 5 und 24 ebenfalls zu beachten sind. Des Weiteren sei darauf hingewiesen, dass in vielen Teilen die EU-Verordnung abschließend ist, in anderen Bereichen so z.B. im Art. 88 (Beschäftigtendatenschutz) gibt es keine klaren Vorgaben sondern es wird den Mitgliedstaaten überlassen, entsprechende eigene Regelungen zu verabschieden. Es gibt also wieder keinen einheitlichen Beschäftigtendatenschutz was aus Sicht der ARGE-HPR weder im Interesse der Personalvertretungen noch im Interesse des Landes Baden-Württemberg sein sollte.

#### **Artikel 1 (Landesdatenschutzgesetz)**

##### **§ 5 Absatz 1 Ziffer 1**

Es wird vorgeschlagen die Formulierung „oder einer Gefahr“ zu ersetzen durch „oder einer unmittelbar drohenden Gefahr“.

Diese eingeschränkte Formulierung ist aus unserer Sicht unabdingbar um die Schwelle für eine mögliche Datenverarbeitung zu anderen Zwecken im Sinne der Grundprinzipien nach Artikel 5 der EU Datenschutzgrundverordnung zu erhöhen.

##### **§ 6 Absatz 1 Ziffer 1**

Der Satz ein ist deutlicher zu formulieren, der Wort grundsätzlich ist einzufügen.

Der Satz lautet dann:

Die Verantwortung für die Zulässigkeit der Übermittlung personenbezogener Daten trägt grundsätzlich die übermittelnde öffentliche Stelle.

##### **§ 7**

Der Begriff „örtlich zuständige öffentliche Stelle“ ist nicht definiert.

Dies ist noch zu ergänzen.

- 3 -

#### **§ 14**

Im LDSG-neu findet sich der Beschäftigtendatenschutz im § 14. Die ARGE-HPR würde es begrüßen, wenn in § 14, entsprechend des § 26 Abs. 5 BDSG-neu ein Hinweis oder vergleichbar ein Absatz eingefügt würde, der besonders den Artikel 5 – Grundsätze für die Verarbeitung personenbezogener Daten – hervorhebt. So wird u.E. eher gewährleistet, dass die Grundsätze auch im Bereich des Beschäftigtendatenschutzes von besonderer Bedeutung sind.

§ 14 ist um eine Regelung für Bewerbungsunterlagen von Bewerbenden mit denen kein Beschäftigungsverhältnis begründet wurde zu ergänzen.

Vorschlag:

„Bewerbungsunterlagen von Bewerbern bei denen kein Beschäftigungsverhältnis begründet wurde sind nach einem Jahr zu löschen, es sei denn, dass die betroffene Person einer längeren Speicherung eingewilligt hat, oder die Datenhaltung wegen eines anhängigen Rechtsstreites erforderlich ist.“

#### **Abs. 6**

Absatz 6 erscheint und noch nicht deutlich genug formuliert. Die ARGE-HPR schlägt folgende Formulierung vor: „Eine Überwachung von Beschäftigten mit Hilfe optisch-elektronischer oder sonstiger technischer Einrichtungen, die eine Verhaltens- oder Leistungskontrolle ermöglichen, ist verboten.“

Die Einschränkungen im Bereich Informations- und Auskunftspflicht in §§ 8 und 9 sowie die Beschränkung des Rechts auf Löschung sieht die ARGE-HPR kritisch. Beispielfähig möchte er auf § 9 Abs. 2 hinweisen. Woher soll eine betroffene Person im Voraus wissen, in welchem Umfang Daten über sie gespeichert sind, und wie soll sie dann präzisieren, über welche der Daten, die gespeichert sind, sie Auskunft haben möchte? Wenn sie es wüsste, bräuchte sie die Anfrage nicht stellen. Wer entscheidet, ob die Auskunftserteilung einen unzumutbaren Aufwand auslöst? U. E. wird hier die informationelle Selbstbestimmung massiv eingeschränkt und auch Art. 5 Abs. 2 der EU-DSGVO nicht beachtet.

- 4 -

Ein weiteres Beispiel, für Beschränkungen findet sich in § 10 Abs. 3 LDSG-neu. Wer entscheidet, ob der Aufwand personenbezogene Daten zu löschen, unverhältnismäßig hoch ist? Wann ist ein Aufwand höher zu bewerten als Persönlichkeitsrechte? Damit wird den Grundsätzen für die Verarbeitung personenbezogener Daten (Art. 5 EU-DSGVO) nicht entsprochen.

Die ARGE-HPR begrüßt die eigenständige Stellung des Landesdatenschutzbeauftragten in einer eigenen Behörde. Er schlägt ferner vor, ausdrücklich auch Interessensvertretungen, aber auch jeder natürlichen Person die Möglichkeit zu bieten, den Landesbeauftragten direkt anzurufen (siehe auch §§ 55 Nr. 4 und 60 Abs. 1 BDSG-neu).

#### **Artikel 17(Änderung des Landesbeamtengesetzes)**

##### **§ 83 Absatz 1**

Aufgrund der besonderen Sensibilität der Personalaktendaten lehnen wir jegliche Verarbeitung von Personalaktendaten im Auftrag ab. Es sollte im Interesse des Landes und der betroffenen Mitarbeitenden sein, dass die besonders schützenswerten Personalaktendaten nicht durch mittels Externer bearbeitet oder aufgearbeitet werden. Mögliche Kostenvorteile sollten in diesem Fall als nachrangig angesehen werden.

Durch die Änderung des Landesbeamtengesetzes wird ermöglicht, dass mit den besonders schützenswerten Personalakten der Beschäftigten ein ähnlicher Umgang erfolgt, wie mit den Grundbüchern, die im Ausland eingescannt wurden

##### **§ 84**

Durch die Formulierung wird eine generelle Einführung von automatisierten Entscheidungen ermöglicht, nicht nur im Bereich der Reisekosten (wie in der Begründung ausgeführt). Dies sieht die ARGE-HPR kritisch. Wir fordern eine datenschutzrechtliche Vorabkontrolle und die Einbeziehung der zuständigen Personalvertretung vor Einführung jedes einzelnen automatisierten Entscheidungsverfahrens. Nach der Frei-

- 5 -

gabe des Verfahrens sollte nach einem angemessenen Zeitraum eine erneute datenschutzrechtliche und personalvertretungsrechtliche Kontrolle sichergestellt sein. Außerdem fehlt eine Evaluation des Erfolgs der automatisierten Vorgehensweise. Bei strittigen Fällen sollte ein definierter Prozess der Schichtung vorgesehen werden.

#### **§ 87 Absatz 4 Ziffer 1**

Wir halten diese Einschränkung des informationellen Selbstbestimmungsrechts für verfassungswidrig. Natürlich ist es wichtig, einen Abwägungsprozess zwischen dem konkreten Schutz der Gesundheit und dem Informationsinteresse des Beschäftigten vorzunehmen, dieser darf aber nicht zur „Entmündigung“ führen. Eine derart ermöglichte Auskunftsverweigerung lehnen wir ab.

#### **Finanzielle Auswirkungen**

In der Gesetzgebungsbegründung unter Ziff. IV sind die finanziellen Auswirkungen dargelegt. Insbesondere die gegenüber der bisherigen Rechtslage erweiterten Pflichten der öffentlichen Stellen als Verantwortliche führen in der Verwaltung zu höheren Kosten. Nach der Verordnung EU 216/679 ist jede öffentliche Stelle ab dem Inkrafttreten der EU-Verordnung 2017/679 verpflichtet, einen Datenschutzbeauftragten zu benennen. Eine solche Verpflichtung gab es im bisherigen Landesdatenschutzgesetz nicht. Die dadurch entstehenden zusätzlichen Kosten sind jedoch durch die Verordnung und nicht durch das Gesetz verursacht. Die ARGE-HPR hält es deshalb für erforderlich, dass das Land zusätzliche Mittel zur Umsetzung des Datenschutzgesetzes zur Verfügung stellt. Nur so kann die Qualifizierung und Arbeitsentlastung der Datenschutzbeauftragten sichergestellt werden.

Abschließend sei darauf hingewiesen, dass die ARGE-HPR es begrüßt hätte, wenn der Gesetzgeber die gegebenen Chancen und Spielräume, den die DSGVO im Bereich des Beschäftigtendatenschutzes bietet, die Beschäftigtendaten besser zu

- 6 -

schützen, auch genutzt hätte. So sucht man Mitbestimmungsrechte der Interessenvertretungen zum Beschäftigtendatenschutz leider vergeblich. Es ist weiterhin festzustellen, dass die Landesregierung lediglich das Nötigste unternommen hat, um das alte Landesdatenschutzgesetz dem EU-Recht anzupassen.

Mit freundlichen Grüßen

gez.

Tilly Bair

Vorsitzende

**Architektenkammer  
Baden-Württemberg**

Recht und Wettbewerb

Ministerium für Inneres, Digitalisierung  
und Migration Baden-Württemberg  
Willy-Brandt-Str. 41  
70173 Stuttgart



**Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679  
Ihr Schreiben vom 19. Dezember 2017 (AZ: 2-0557.8/1)**

31. Januar 2018  
G2R0054-12-  
1/4889598/MC

Sehr geehrter Herr

die Architektenkammer Baden-Württemberg bedankt sich für die Möglichkeit zum Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016-679 angehört zu werden und eine Stellungnahme abgeben zu können.

Gerne nehmen wir zum geplanten Entwurf wie folgt Stellung:

1. Fehlende Ausnahmeregelung zu Art. 18 EU DSGVO („Recht auf Einschränkung der Verarbeitung“).

Art. 18 Abs. 1 i. V. m. Abs. 2 EU DSGVO gibt der betroffenen Person das Recht auf Einschränkung der Verarbeitung ihrer persönlichen Daten.

Im vorliegenden Entwurf des LDSG findet sich aus unserer Sicht keine Regelung, die den betroffenen Institutionen die Möglichkeit einräumt, Ausnahmen für die Anwendung des Art. 18 EU DSGVO vorzunehmen.

Wir regen aus diesem Grund an, dass in einem etwaigen neuen § 10a LDSG Beschränkungen auf das Recht auf Einschränkung der Verarbeitung vorgenommen werden. Der Wortlaut könnte sich an den §§ 4, 5 LDSG orientieren.

2. § 11 LDSG („Beschränkung der Benachrichtigungspflicht“)

Wir regen an, dass § 11 LDSG um eine eigene Nr. 4 ergänzt wird, in der aus Gründen der Unverhältnismäßigkeit die öffentliche Stelle von einer Benachrichtigung der betroffenen Person absehen kann.

Aus unserer Sicht ist es verhältnismäßig und interessengerecht, dass bei einem unverhältnismäßigen Aufwand eine solche Benachrichtigung nicht erfolgen muss.

Architektenkammer Baden-Württemberg, Körperschaft des öffentlichen Rechts  
Danneckerstr. 54, 70182 Stuttgart, [www.akbw.de](http://www.akbw.de), [info@akbw.de](mailto:info@akbw.de)  
BW-Bank Stuttgart, BIC: SOLADEST600, IBAN: DE86 6005 0101 0001 2950 10

Seite 2 zum Schreiben vom 31. Januar 2018

Architektenkammer  
Baden-Württemberg

3. Einschränkungen des Art. 21 EU DSGVO („Widerspruchsrecht“)

Wir regen an, dass in das LDSG eine weitere Regelung noch aufgenommen wird, die für die Institutionen, die unter das LDSG fallen, Ausnahmen zu Art. 21 EU DSGVO vorsehen und zulassen. Auch hier geht es darum, dass zu überprüfen ist, ob die vom LDSG umfassten Institutionen ihre Tätigkeiten ordnungsgemäß ausüben können, wenn sie vollständig den Pflichten aus Art. 21 EU DSGVO ausgesetzt sind.

Aus unserer Sicht ist es notwendig, dass es ähnliche Ausnahmen im Sinne der §§ 4, 5 LDSG auch für das Widerspruchsrecht gibt.

Mit freundlichen Grüßen



Hans Dieterle  
Hauptgeschäftsführer



Ulrich Emmert  
Rechtsanwalt und Datenschutzbeauftragter der AKBW



BWKG e.V. · Postfach 100428 · 70003 Stuttgart

[Per Mail Registratur2@im.bwl.de](mailto:PerMail.Registratur2@im.bwl.de)

Ministerium für Inneres, Digitalisierung und Migration  
Baden-Württemberg

Postfach 10 34 65  
70029 Stuttgart

Pflegeeinrichtungen,  
Personal und Recht

**Ursula Ungerer**  
stv. Geschäftsführerin

Unser Zeichen  
1950 Th/Un/Le  
101\_109\_Stellungnahm  
e Datenschutzrecht.docx

31.01.2018

### **Stellungnahme der BWKG zu dem Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679**

Sehr geehrter Herr

vielen Dank für die Übermittlung des Entwurfs des Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679 und die Möglichkeit der Stellungnahme.

Die Vielschichtigkeit des künftigen Datenschutzrechts und die Notwendigkeit, verschiedene Normen parallel zu lesen, erschweren die Anwendung deutlich. Um den Gebrauch des Landesdatenschutzgesetzes (LDSG) für den Normanwender zu erleichtern, wird vorgeschlagen, grundsätzlich im jeweiligen Normtext einen Bezug zu dem zu konkretisierenden Artikel der Verordnung (EU) 2016/679 (DSGVO) herzustellen. Dies erleichtert dem Anwender die parallele Beachtung der verschiedenen Datenschutzregelungen (DSGVO, BDSG, LDSG, Spezialgesetze). Eine Aufnahme in den Begründungstext des LDSG wird nicht für ausreichend erachtet, da sich hierdurch der Aufwand für den Anwender weiter erhöht.

Wünschenswert wäre insofern, dass der Anwender (ähnlich wie bei dem am 23.05.2018 in Kraft tretenden Bundesdatenschutzgesetz (BDSG-neu)) im konkreten Normtext den Verweis auf den/die geltenden Artikel der DSGVO an die Hand bekommt.

#### **Zu § 3 Abs. 1 Satz 1 und Satz 2 Nrn. 6 - 9 – Sicherstellung des Datenschutzes**

Bei § 3 Abs. 1 Satz 1 und Satz 2 Nrn. 6 - 9 handelt es sich nach unserer Auffassung nicht um zulässige Konkretisierungen, sondern um Wiederholungen der DSGVO, die jedoch nicht wortgleich übernommen werden. Dies kann in der Umsetzung zu neuen Auslegungsspielräumen und damit eher zu Verwirrungen in der Anwendung führen und schadet der Normenklarheit. Insofern sollte der Abschnitt aus der DSGVO (Art. 32 Abs. 1 a - d) zur Verständlichkeit wortgleich aufgenommen oder alternativ auf Artikel 32 Abs. 1 a - d

Baden-Württembergische  
Krankenhausgesellschaft e.V.  
[www.bwkg.de](http://www.bwkg.de)

Birkenwaldstraße 151  
70191 Stuttgart  
Postfach 100428  
70003 Stuttgart

Telefon 0711 25777-0  
Telefax 0711 25777-99  
[info@bwkg.de](mailto:info@bwkg.de)

Schreiben "Stellungnahme der BWKG zu dem Entwurf eines Gesetzes zur Anpassung des allgemeinen Daterger Vorschriften an die Verordnung (EU) 2016/679" vom 31.01.2018

Seite 2

verwiesen werden.

#### **Zu § 5 – Datenverarbeitung zu anderen Zwecken**

Anhand des § 5 Abs. 1 wird nochmals beispielhaft darauf hingewiesen werden, dass im Normtext selbst ein direkter Bezug auf die konkretisierten Regelungen der DSGVO wünschenswert ist. § 5 Abs. 1 führt aus, dass eine Verarbeitung unter bestimmten Voraussetzungen „unbeschadet der Bestimmungen der Verordnung (EU) 2016/679 zulässig“ ist. Der Bezug auf Art. 6 Abs. 4 DSGVO findet sich aber bislang nur in der Begründung des Gesetzentwurfs und nicht direkt im Gesetzestext.

#### **Zu § 6 (Begründung) – Übermittlung personenbezogener Daten**

In der Entwurfsbegründung zu § 6 wird ausgeführt, dass nach der Verordnung (EU) 2016/679 die Übermittlung personenbezogener Daten wie eine Zweckänderung behandelt werde.

Hier wird für erforderlich gehalten, eine Klarstellung aufzunehmen, auf welchen Artikel oder Erwägungsgrund der Verordnung sich dies bezieht.

#### **Zu § 8 – Beschränkung der Informationspflicht**

§ 8 LDSG-E enthält Regelungen, in welchen Fällen auf eine Information der betroffenen Person gem. Artikel 13 und 14 DSGVO verzichtet werden kann.

Die eigentliche Zielrichtung von Krankenhäusern, Patienten zu behandeln, tritt angesichts stetig wachsenden Verwaltungsaufgaben zunehmend in den Hintergrund. Die in Art. 13 Abs. 1 und 2 DSGVO vorgesehenen Informationspflichten stellen einen ganz erheblichen weiteren bürokratischen Zusatzaufwand für die Krankenhäuser dar. Krankenhäuser unterliegen schon heute zahlreichen Informations-, Hinweis-, Unterrichts- sowie Aufklärungspflichten. Werden die nach der DSGVO vorgesehenen neuen Informationspflichten nicht eingeschränkt, wird das Maß des Zumutbaren deutlich überschritten. Dem steht kein erkennbarer Nutzen für die Patienten gegenüber, die ihrerseits eher verwirrt und verunsichert werden.

Nach Art. 13 Abs. 1 und 2 DSGVO muss u. a. insbesondere Folgendes mitgeteilt werden:

- die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen
- die Rechtsgrundlage für die Verarbeitung und
- die Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer
- ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche möglichen Folgen die Nichtbereitstellung hätte.

Schreiben "Stellungnahme der BWKG zu dem Entwurf eines Gesetzes zur Anpassung des allgemeinen Datener Verordnungen an die Verordnung (EU) 2016/679" vom 31.01.2018

Seite 3

Dies stellt sich insbesondere im System der gesetzlichen Krankenversicherung als äußerst komplex sowie kaum umsetzbar dar.

Hinsichtlich der „Zwecke“ lässt sich festhalten, dass die erhobenen Daten für eine sehr große Vielzahl von Zwecken verarbeitet werden (wie z.B. Abrechnung mit der Krankenkasse oder der Kassenärztlichen Vereinigung oder dem Patienten selbst oder weiteren Kostenträgern wie Berufsgenossenschaft oder Sozialhilfe, Qualitätssicherungsmaßnahmen und -prüfungen, Wirtschaftlichkeitsprüfungen, Übermittlungspflichten gegenüber speziellen Registern wie z. B. dem Endoprothesenregister, Informationsübermittlung an Mitbehandler und Nachbehandler usw.). Die Rechtsgrundlagen hierfür sind dabei von unterschiedlichster Natur. Eine entsprechende Mitteilung überfordert die Patienten letztlich und lässt die Sinnhaftigkeit sehr zweifelhaft erscheinen.

Schon fast absurde Züge gewinnt es, wenn die Krankenhäuser den Patienten tatsächlich die „Dauer, für die die personenbezogenen Daten gespeichert werden, oder falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer“ mitzuteilen haben. Als Standardwerk hinsichtlich der Frage von „Aufbewahrungspflichten und -fristen“ im Krankenhausbereich gilt ein 27-seitiger Leitfaden (DKG-Leitfaden Aufbewahrungspflichten und -fristen von Dokumenten im Krankenhaus, Stand: 2015), der die spezialgesetzlichen Aufbewahrungsfristen darstellt und dabei nicht einmal Anspruch auf Vollständigkeit erhebt. Müssten Krankenhausträger die Dauer der Aufbewahrung gegenüber dem Patienten mitteilen, müssten sie ihm sämtliche dieser Daten mitteilen, was das Maß des Zumutbaren überschreiten dürfte.

Exemplarisch genannt seien Aufbewahrungsfristen aus folgenden Gesetzen: BGB, RöV, StrlSchV, BtMVV, BtMBinHV, ApoBetrO, AMWHV, AMHV, TFG, TPG, IfSG, Verletzungsverfahren-VAV, GenDG, SGB I usw. Hinzu kommt, dass die meisten dieser Gesetze nicht nur eine Aufbewahrungsfrist beinhalten, sondern in der Regel mehrere Fristen von Krankenhausrelevanz.

Eine Eingrenzung der Informationspflichten für den Fall, dass die Verarbeitung der personenbezogenen Daten ausdrücklich durch Rechtsvorschriften geregelt ist, sieht Erwägungsgrund 62 der Verordnung (EU) 2016/679 im Übrigen explizit vor. Eine entsprechende Klarstellung in § 8 LDSG-E sollte unbedingt aufgenommen werden.

§ 8 Abs. 1 sollte um folgende Nummer 5 ergänzt werden:

*„Eine Pflicht zur Information der betroffenen Personen besteht nicht, soweit und solange [...]*

- 5. die Information einen unverhältnismäßigen Aufwand erfordern würde und das Interesse der betroffenen Person an der Informationserteilung nach den Umständen des Einzelfalls, insbesondere wegen des Zusammenhangs, in dem die Daten erhoben wurden, als gering anzusehen ist, oder sich erübrigt, da die Datenverarbeitung in Rechtsvorschriften geregelt ist.“**

Schreiben "Stellungnahme der BWKG zu dem Entwurf eines Gesetzes zur Anpassung des allgemeinen Datener Verordnungen an die Verordnung (EU) 2016/679" vom 31.01.2018

Seite 4

#### **Zu § 9 Abs. 1 – Beschränkung des Auskunftsrechts**

Vor dem Hintergrund der Vielfalt und Komplexität der Datenbestände in Krankenhäusern ist es sehr erfreulich, dass das Auskunftsrecht hinsichtlich großer Informationsmengen auf konkrete präzisierbare Informationen oder Verarbeitungsvorgänge begrenzt wird.

Ergänzend sollte allerdings in Anlehnung an § 34 Abs. 1 Nr. 2 BDSG-neu das Auskunftsrecht auch insoweit beschränkt werden, wenn die Daten nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen.

§ 9 Abs. 1 sollte daher wie folgt gefasst werden:

*„(1) Die Auskunftserteilung kann wie die Informationserteilung aus den in § 8 Absatz 1 genannten Gründen abgelehnt werden. Die betroffene Person kann ferner keine Auskunft verlangen,*

- 1. wenn die Daten nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder**
- 2. soweit und solange die personenbezogenen Daten ausschließlich zu Zwecken der Datensicherung oder der Datenschutzkontrolle gespeichert sind**

*und eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist und deswegen das Interesse der betroffenen Person an der Auskunftserteilung zurücktreten muss.“*

#### **Zu § 12 – Verarbeitung personenbezogener Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen**

##### **Zu § 12 Abs. 2**

In § 5 Abs. 2 LDSG-E wurde bezüglich der Beschreibung einer Zweckänderung das bislang in § 15 Abs. 3 LDSG enthaltene Forschungsprivileg weggelassen. Dies zum Einen, da die DSGVO eine Privilegierung wissenschaftlicher Forschung vorsieht und zum anderen in § 13 LDSG-E geregelt wird. § 12 Abs. 2 regelt die Datenverarbeitung zu anderen Zwecken „nur“ in den sodann genannten Ausnahmen. Um einen Bruch zur Verarbeitung zu Forschungszwecken zu vermeiden, sollte der Absatz 2 um einen Verweis auf § 13 ergänzt werden.

§ 12 Abs. 2 Nr. 2 sollte daher wie folgt gefasst werden:

*„2. die Voraussetzungen des § 5 Absatz 1 Nummern 1 oder 2 oder § 13 Absatz 1 vorliegen und die zur Verschwiegenheit verpflichtete Stelle eingewilligt hat.“*

Schreiben "Stellungnahme der BWKG zu dem Entwurf eines Gesetzes zur Anpassung des allgemeinen Datener Verordnungen an die Verordnung (EU) 2016/679" vom 31.01.2018

Seite 5

### Zu § 12 Abs. 3 (neu)

§ 22 BDSG-neu sowie die überarbeiteten Kirchengesetze geben die Erlaubnistatbestände des Art. 9 Abs. 2 DSGVO nochmals wieder. Eine solche Wiedergabe erscheint zumindest in den Fällen angezeigt, in denen die DSGVO auf nationales Gesetz als Rechtsgrundlage verweist.

Dies betrifft insbesondere den Tatbestand des Art. 9 Abs. 2h DSGVO, mit dem die Verarbeitung zu Zwecken der Versorgung im Gesundheits- und Sozialbereich und zu der Verwaltung von Systemen und Diensten in der Gesundheitsversorgung geregelt wird. Die Zulässigkeit setzt eine Regelung im Unionsrecht, im nationalen Recht oder einen Vertrag mit einem Angehörigen eines Gesundheitsberufs voraus.

Zwar wird es oft so sein, dass die Verarbeitung auch auf einen Vertrag mit einem Angehörigen eines Gesundheitsberufs gestützt werden kann. Es gibt aber auch Fallkonstellationen, in denen dies nicht der Fall sein wird, z. B. weil der „Kunde“ wegen seines Gesundheitszustands gar nicht in der Lage ist, einen Vertrag abzuschließen oder weil der Vertragsschließende (z. B. Pflegeheim) kein Angehöriger eines Gesundheitsberufs ist. Um hier keine „Lücken“ entstehen zu lassen, sollte jedenfalls der Tatbestand des Art. 9 Abs. 2h DSGVO wie in § 22 Abs. 1 Nr. 1b BDSG-neu als neuer Absatz 3 des § 12 LDSG übernommen werden.

Um mögliche weitere Lücken von vornherein auszuschließen, würden wir befürworten, entsprechend auch Artikel 9 Abs. 2i DSGVO in das LDSG aufzunehmen.

§ 12 Abs. 3 sollte daher wie folgt gefasst werden:

**„(3) Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 zulässig**

- (a) zum Zweck der Gesundheitsvorsorge, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- und Sozialbereich oder aufgrund eines Vertrags der betroffenen Person mit einem Angehörigen eines Gesundheitsberufs erforderlich ist, und diese Daten von ärztlichem Personal oder durch sonstige Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen, oder unter deren Verantwortung verarbeitet werden, oder**
- (b) aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten erforderlich ist; ergänzend zu den in Absatz 2 genannten Maßnahmen sind insbesondere die berufsrechtlichen und strafrechtlichen Vorgaben zur Wahrung des Berufsgeheimnisses einzuhalten.“**

Schreiben "Stellungnahme der BWKG zu dem Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenerheber Vorschriften an die Verordnung (EU) 2016/679" vom 31.01.2018

Seite 6

Alternativ könnte auch ein eigener gesonderter Paragraph eingefügt werden.

#### **Zu § 13 – Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken**

##### **Zu § 13 Abs. 1**

Die vorgesehene Regelung in § 13 Abs. 1 lehnt sich eng an das BDSG (neu) und die bisherigen Regelungen im LDSG an. Allerdings ist im Vergleich zur bisherigen Rechtslage an mehreren Stellen eine Verschlechterung für die Forschung festzustellen:

- Sofern eine Abwägung verlangt wird, muss derzeit nach §§ 19 und 35 LDSG das **wissenschaftliche** Interesse an der Durchführung der Forschung das Betroffeneninteresse erheblich überwiegen. § 13 Abs. 1 LDSG-E verlangt nun aber, dass das Interesse der öffentlichen **Stelle** an der Verarbeitung das Betroffeneninteresse erheblich überwiegen muss. Dies verengt den bisherigen Fokus eines Interesses der Allgemeinheit auf das individuelle Interesse (z. B. der Universität).
- Während in § 13 Abs. 3 LDSG-E im Kontext der Veröffentlichung von personenbezogenen Daten im Rahmen von Forschungsergebnissen explizit auf die **Einwilligung** als mögliche Rechtsgrundlage hingewiesen wird, fehlt ein Hinweis auf die Einwilligung in § 13 Abs. 1 LDSG-E als generell mögliche Rechtsgrundlage für eine Verarbeitung im Rahmen der Forschung, was auf jeden Fall zu ergänzen wäre. Bislang verlangt § 35 LDSG allerdings bei der Erhebung nur im Fall einer **Nichtkenntnis** der Erhebung durch den Betroffenen, dass der Zweck nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann. Nach § 13 Abs. 1 LDSG-E wäre auch für eine Erhebung, die dem Betroffenen bekannt ist, eine entsprechende Abwägung erforderlich.
- Bislang ist nach § 19 Abs. 1 LDSG bei einer Übermittlung zwischen öffentlichen Stellen auch eine Anonymisierung durch den Empfänger der Daten möglich, wenn die übermittelnde Stelle dies aus personellen Gründen nicht leisten kann.

Diese Verschärfungen sind vor dem Hintergrund, dass die Regelungen in Art. 9 Abs. 2j und Art. 89 DSGVO ausdrücklich deutlich forschungsfreundlichere Regelungen zulassen, nicht nachvollziehbar. Die Forschung ist für Baden-Württemberg ein wichtiger Standortfaktor. Andere Bundesländer wie z. B. Bayern schränken daher die durch Art. 9 Abs. 2j und Art. 89 DSGVO eröffneten Möglichkeiten nicht weiter ein. Andere Bundesländer wie z. B. Brandenburg und Sachsen stellen zumindest bei der Interessensabwägung nicht auf die öffentliche Stelle, sondern auf das öffentliche Interesse ab und dieses muss dem Betroffeneninteresse nur „einfach“ und nicht erheblich überwiegen.

Es wird für § 13 Abs. 1 folgende Formulierung in Anlehnung an Art. 25 des Gesetzesentwurfs für ein Bayerisches Datenschutzgesetz vorgeschlagen:

- (1) ***Für Zwecke der wissenschaftlichen oder historischen Forschung erhobene oder gespeicherte personenbezogene Daten dürfen nur für diese Zwecke verarbeitet werden.***

Schreiben "Stellungnahme der BWKG zu dem Entwurf eines Gesetzes zur Anpassung des allgemeinen Datener Vorschritten an die Verordnung (EU) 2016/679" vom 31.01.2018

Seite 7

- (1a) Die personenbezogenen Daten sind zu anonymisieren, sobald dies nach dem Forschungszweck möglich ist. Bis dahin sind die Merkmale, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer Person zugeordnet werden können, gesondert zu speichern. Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungszweck dies erfordert.**

Die allgemeinen Vorgaben zur Verarbeitung in der DSGVO sowie die Vorgabe zur frühestmöglichen Anonymisierung tragen dem Interesse der Betroffenen ausreichend Rechnung. Denkbar wäre auch eine Regelung, wonach Voraussetzung für die Verknüpfung unterschiedlicher Forschungsdaten eine Pseudonymisierung ist. Dies kann z. B. bei der immer größeren Zahl medizinischer Register eine Rolle spielen.

#### **Zu § 13 Abs. 4**

In der Begründung zu der Einschränkung der Betroffenenrechte wird auf die entsprechende Regelung in § 27 Abs. 2 BDSG (neu) verwiesen und diese mit dem Ziel der Rechtsvereinheitlichung aufgenommen. Anders als das BDSG (neu) wird jedoch die Beschränkung des Auskunftsrechts, wenn die Daten für Zwecke der wissenschaftlichen Forschung erforderlich sind und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde (§ 27 Abs. 2 Satz 2 BDSG-neu), nicht mit aufgenommen. Die allgemeine Beschränkung des Auskunftsrechts in § 9 Abs. 2 LDSG-E für den Fall der Verarbeitung großer Informationsmengen reicht hierfür nicht aus.

§ 13 Abs. 4 sollte analog § 27 Abs. 2 S. 2 BDSG-neu um folgenden Satz ergänzt werden:

**„Das Recht auf Auskunft gemäß Artikel 15 der Verordnung (EU) 2016/679 besteht darüber hinaus nicht, wenn die Daten für Zwecke der wissenschaftlichen Forschung erforderlich sind und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde.“**

#### **Zu § 17 – Videoüberwachung**

Bislang war die Videoüberwachung zur Wahrung des Hausrechts im LDSG geregelt. Auch das BDSG (neu) nimmt sie in § 4 Abs. 1 S.1 direkt mit auf. In der Gesetzesbegründung zu § 17 LDSG-E wird darauf verwiesen, dass sich eine Videoüberwachung zur Wahrung des Hausrechts künftig allein nach Artikel 6 Abs. 1f DSGVO richten soll.

Der Vollständigkeit, Klarheit und Nachvollziehbarkeit halber wird für zulässig und wünschenswert erachtet, die Videoüberwachung zur Wahrung des Hausrechts direkt in das LDSG-E aufzunehmen.

§ 17 Abs. 1 sollte wie folgt gefasst werden:

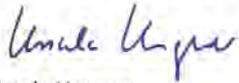
- (1) Die Verarbeitung personenbezogener Daten mit Hilfe optisch-elektronischer Einrichtungen (Videoüberwachung) zur Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe ~~oder~~, in Ausübung öffentlicher Gewalt, die einer öffentlichen Stelle übertragen wurde, ~~oder zur Wahrung des Hausrechts~~ ist zulässig, wenn schutzwürdige Interessen betroffener Personen nicht überwiegen.**

Schreiben "Stellungnahme der BWKG zu dem Entwurf eines Gesetzes zur Anpassung des allgemeinen Dater  
ger Vorschriften an die Verordnung (EU) 2016/679" vom 31.01.2018

Seite 8

Wir bitten, diese Änderungen in dem Gesetz zur Anpassung des allgemeinen Daten-  
schutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679 zu berücksich-  
tigen.

Mit freundlichem Gruß



Ursula Ungerer



**Baden-Württembergischer  
Handwerkstag e.V.**  
Zusammenschluss  
sämtlicher Organisationen  
des Handwerks von Baden-Württemberg

Heilbronner Straße 43  
70191 Stuttgart  
Telefon: 0711 263709-0  
Telefax: 0711 263709-100  
E-Mail: [info@handwerk-bw.de](mailto:info@handwerk-bw.de)  
<http://www.handwerk-bw.de>



BWHT Postfach 10 06 36 70005 Stuttgart

Ministerium für Inneres, Digitalisierung  
und Migration Baden-Württemberg  
Postfach 103465

70029 Stuttgart

Ihre Nachricht  
2-0557.8/1

Unsere Zeichen  
6.4130 OV

Bearbeiter/Durchwahl  
Oskar Vogel

Datum  
31.01.2018

*Entwurf eines Gesetzes zur Anpassung des Allgemeinen Datenschutzrechts  
und sonstiger Vorschriften an die Verordnung (EU) 2016/679*

Sehr geehrte Damen und Herren,

wir danken für die Anhörung zu dem im Betreff genannten Gesetzentwurf und nehmen wie folgt dazu Stellung:

1. Wir regen an, das Widerspruchsrecht wie in § 36 BDSG n.F. zu beschränken, also eine Regelung wie folgt aufzunehmen:

„Das Recht auf Widerspruch gemäß Artikel 21 Abs. 1 der Verordnung (EU) 2016/679 gegenüber einer öffentlichen Stelle besteht nicht, soweit an der Verarbeitung ein zwingendes öffentliches Interesse besteht, das die Interessen der betroffenen Person überwiegt, oder eine Rechtsvorschrift zur Verarbeitung verpflichtet.“

Ohne eine solche Beschränkung, die nach der Öffnungsklausel des Artikel 23 Abs. 1e DSGVO zulässig ist, könnten die Handwerkskammern ihre Aufgaben gemäß § 91 Handwerksordnung nicht oder nur mit erheblichem administrativen Mehraufwand gegenüber ihren Mitgliedern nachkommen. Dem Anspruch der Kammern, ihre Entscheidungsprozesse nach innen und außen transparent abzubilden, würde das Widerspruchsrecht in der bislang vorliegenden Fassung kontraproduktiv entgegenstehen.

Vereinsregisternummer:  
VR 1338, Amtsgericht Stuttgart

Steuernummer:  
99015/06101

Bankverbindung:  
IBAN: DE90 6005 0101 0001 3671 06 (BIC: SOLADEST600)



2. § 28 Abs. 1 LDSG-Entwurf sollte in den Sanktionen lediglich auf Geldbußen beschränkt werden. Wir sehen keinen Anlass, eine strengere Regelung im Vergleich zur EU-Verordnung vorzunehmen (vgl. dort Artikel 83).
3. Im Übrigen schließen wir uns der separaten Stellungnahme des Landesinnungsverbandes des Schornsteinfegerhandwerks Baden-Württemberg voll inhaltlich an.

Abschließend drücken wir unsere Erwartung aus, dass die notwendigen Anpassungen an die Datenschutzgrundverordnung insgesamt zur Harmonisierung des Datenschutzrechts in den 16 Bundesländern genutzt wird.

Mit freundlichen Grüßen



Oskar Vogel  
Hauptgeschäftsführer

**STELLUNGNAHME**

Stuttgart, 29. Januar 2018

---

**Baden-Württembergischer Industrie- und Handelskammertag**

---

**Stellungnahme zum Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679****Wer wir sind:**

Der Baden-Württembergische Industrie- und Handelskammertag (BWIHK) ist eine Vereinigung der zwölf baden-württembergischen Industrie- und Handelskammern (IHK). In Baden-Württemberg vertreten die zwölf IHKs die Interessen von mehr als 650.000 Mitgliedsunternehmen. Zweck des BWIHK ist es, in allen die baden-württembergische Wirtschaft und die Mitgliedskammern insgesamt betreffenden Belangen gemeinsame Auffassungen zu erzielen und diese gegenüber der Landes-, Bundes- und Europapolitik sowie dem Deutschen Industrie- und Handelskammertag (DIHK) und anderen Institutionen zu vertreten.

Wir nehmen Bezug auf die E-Mail des Ministerium für Inneres, Digitalisierung und Migration Baden-Württemberg vom 22. Dezember 2017, in welcher wir aufgefordert worden sind bis zum 31. Januar 2018 Stellung zum Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679 zu nehmen.

Grundsätzlich möchten wir anmerken, dass wir als bundesweite Organisation die Hoffnung hatten, dass die notwendigen Anpassungen an die Datenschutzgrundverordnung genutzt wird, um das Datenschutzrecht in den einzelnen Bundesländern zu harmonisieren. Nach unseren Kenntnissen weichen die einzelnen Entwürfe der Landesdatenschutzgesetze allerdings erheblich voneinander ab. Länderspezifisch unterschiedliche, voneinander abweichende Datenschutzvorgaben erschweren insbesondere bundesweite und länderübergreifende IHK-Projekte und verursachen einen erhöhten Kostenaufwand. Ein Abstimmungsprozess wäre deshalb in jedem Fall wünschenswert.

- Gemäß Art. 5 LDSG-E ist eine Zweckänderung der Datenverarbeitung zu kompatiblen Zwecken möglich. Allerdings ist die Kompatibilitätsprüfung für öffentliche Stellen schwierig, insbesondere bei Verarbeitungen öffentlicher Stellen wie der IHK aufgrund von vielfältigen gesetzlichen Aufgaben. Auch bei der Verarbeitung von Daten aus öffentlich zugänglichen Quellen, wäre eine Abwägung nach dem Muster von § 23 BDSG-neu hilfreich. Daher regen wir an, eine Regelung wie in § 23 Absatz 1 Ziff.1 BDSG-neu aufzunehmen, wonach die Datenverarbeitung durch öffentliche Stellen zu anderen Zwecken zulässig ist, wenn



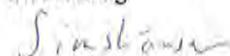
1. offensichtlich ist, dass sie im Interesse der betroffenen Person liegt und kein Grund zu der Annahme besteht, dass sie in Kenntnis des anderen Zwecks ihre Einwilligung verweigern würde,
  2. Angaben der betroffenen Person überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen.
- Eine Regelung zur Beschränkung des Widerspruchsrecht wie in § 36 BDSG-neu geregelt, ist auch für das LDSG-E sinnvoll:  
„Das Recht auf Widerspruch gemäß Artikel 21 Absatz 1 der Verordnung (EU) 2016/679 gegenüber einer öffentlichen Stelle besteht nicht, soweit an der Verarbeitung ein zwingendes öffentliches Interesse besteht, das die Interessen der betroffenen Person überwiegt, oder eine Rechtsvorschrift zur Verarbeitung verpflichtet.“  
Andernfalls könnten die Industrie und Handelskammern ihre Aufgaben aus § 1 IHKG – zum Beispiel auch die Pflicht nach dem BVerfG–Urteil Mindermeinungen abzubilden –nicht, oder nur mit erheblichem Verwaltungsmehraufwand gegenüber ihren Mitgliedern erfüllen. Wir stützen uns bei der Anregung nach einem Widerspruchsrecht auf die Öffnungsklausel des Art. 23 Abs.1 Buchstabe e DSGVO.
  - § 28 Abs. 1 LDSG-E: Wir weisen darauf hin, dass diese Vorschrift unter anderem eine Freiheitsstrafe von bis zu zwei Jahren vorsieht. Zwar regelt Art. 84 der Verordnung (EU) 2016/679 ausdrücklich, dass die Mitgliedstaaten die Vorschriften über andere Sanktionen für Verstöße gegen die Verordnung festlegen können, wobei diese Sanktionen unter anderem abschreckend sein müssen. Auch wird in § 28 Abs. 1 HS. 2 des Gesetzesentwurfs der Erhalt eines Entgelts oder eine Bereicherungs- oder Schädigungsabsicht vorausgesetzt. Dennoch handelt es sich um eine im Vergleich zur EU-Verordnung strengere Regelung, die in Art. 83 lediglich Geldbußen vorsieht. Sie birgt für jene ein Haftungsrisiko, die mit den geschützten personenbezogenen Daten in Kontakt sind. Wir gehen davon aus, dass die abschreckende Wirkung auch durch Geldbußen ausreichend erzielt werden wird. Es wird daher vorgeschlagen, die Sanktionen lediglich auf Geldbußen zu beschränken.
  - Zu § 14 LDSG-E: Der Gesetzestext selbst sieht die Schriftform für Einwilligungen im Beschäftigtenverhältnis nicht vor. Nach der Gesetzesbegründung soll im Beschäftigtenverhältnis eine Einwilligung im Regelfall schriftlich erfolgen. Das Schriftformerfordernis als Regelfall empfinden wir im Zuge zunehmender Digitalisierung - auch am Arbeitsplatz - nicht mehr als zeitgemäß.
  - Zur Änderung des Landesglücksspielgesetzes Baden-Württemberg (LGlüG), Art. 14 Nr. 3, § 32 Ziff. c) LDSG-E: Es wird darauf hingewiesen, dass dieser Absatz dem betrieblichen Datenschutzbeauftragten von Spielbanken die entsprechende Pflicht auferlegt das Konzept zur Videoüberwachung vor Umsetzung zu überprüfen, insb. ob die technisch-organisatorischen Maßnahmen eingehalten worden sind und ob den schutzwürdigen Interessen der Betroffenen Rechnung getragen wird. Die „Überprüfung“ der Videoüberwachung legt dem Datenschutzbeauftragten eine größere Pflicht, auf als die Datenschutz-Folgeabschätzung gemäß Art. 35 Abs. 2 der Verordnung (EU) 2016/679 vorsieht: Danach hat der Datenschutzbeauftragte eine beratende Funktion. Die Überprüfung selbst ist vom Verantwortlichen durchzuführen.



Gemäß der in § 32 Abs. 1 LGlüG geregelten Pflicht zur Videoüberwachung treffen den Datenschutzbeauftragten von Spielbanken somit größere Pflichten als den anderer IHK-Mitglieder.

- Wir bewerten die Regelung in § 9 Abs. 2 LDSG-E als positiv, da sie die Möglichkeit einräumt, eine Präzisierung des Auskunftersuchens zu verlangen. Dies trägt zu einer effizienten und zeitnahen Bearbeitung der Anfrage bei und entlastet die jeweilige öffentliche Stelle.
- Wir begrüßen die Regelung in § 8 LDSG-E zur Ausnahme von der Informationspflicht, so dass zum Beispiel Beschwerdeführer im Bereich des Wettbewerbsrechts oder im Sachverständigenwesen nicht genannt werden müssen.

Mit freundlichen Grüßen  
IHK Region Stuttgart  
Im Auftrag

  
Rainer Simshäuser  
Bereich Recht und Steuern

## BADISCHER NOTARVEREIN E. V. Die Präsidentin

Badischer Notarverein, Am Marktplatz 9, 77652 Offenburg

Ministerium für Inneres, Digitalisierung  
Migration Baden-Württemberg  
Abt. 2, Verfassung, Kommunal- und  
Sparkassenwesen, Recht  
Willy-Brandt-Str. 41  
70173 Stuttgart

Offenburg, den 04.02.2018

Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften  
an die Verordnung (EU) 2016/679  
Ihr Schreiben vom 19.12.2017, Az. 2-0557.8/1

Sehr geehrter Herr  
sehr geehrte Frau  
sehr geehrte Damen und Herren,

der Badische Notarverein dankt für die Gelegenheit zur Stellungnahme zum Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679. Wir beschränken uns im Folgenden auf den in Art. 1 dieses Gesetzentwurfs enthaltenen Entwurf des Landesdatenschutzgesetzes („LDSG-E“).

### 1. Notare als öffentliche Stellen und notarielle Verschwiegenheitspflicht

Notare sind Träger eines öffentlichen Amtes (§ 1 BNotO), die durch Hoheitsakt bestellt werden (§ 3 Abs. 1 BNotO) und der Dienstaufsicht der Landesjustizverwaltung (§§ 92 ff. BNotO) unterliegen; sie sind daher öffentliche Stellen, die dem LDSG unterliegen.<sup>1</sup> Auch das neugefasste LDSG wäre – wie das bisherige – auf Notare anwendbar (§ 2 Abs. 1 LDSG-E).

Wir begrüßen generell die Stärkung des Datenschutzes. Denn für Notare als „geborene Datenschützer“<sup>2</sup> spielt der Datenschutz seit jeher eine herausragende Rolle. Eine der wesentlichen Amtspflichten des Notars und Grundpfeiler des Notariats ist die notarielle Verschwiegenheitspflicht nach § 18 BNotO, die den Notaren strenge und zudem strafbewehrte Pflichten auferlegt. Einzelne

<sup>1</sup> BGH vom 30.07.1990 – NotZ 19/89, NJW 1991, 568.

<sup>2</sup> Klingler, RNotZ 2013, 57.

Bestimmungen des LDSG-E bedürfen insofern der Anpassung an diese Besonderheiten, so wie sie auch im BDSG in der ab dem 25.5.2018 geltenden Fassung<sup>3</sup> („BDSG-neu“) vorgesehen sind.

## 2. Beschränkung der Informationspflichten und des Auskunftsrechts

### 2.1. Informationspflicht, Auskunftsrecht und Benachrichtigungspflicht nach DSGVO

Nach Art. 14 Abs. 1 DSGVO<sup>4</sup> ist der Verantwortliche (also auch der Notar) grundsätzlich verpflichtet, einer Person bestimmte Informationen mitzuteilen, wenn ihre personenbezogenen Daten nicht bei ihr erhoben wurden. Zusätzlich gewährt Art. 15 DSGVO ein entsprechendes Auskunftsrecht der betroffenen Person gegenüber dem Verantwortlichen. Darüber hinaus ist bei einer Verletzung des Schutzes personenbezogener Daten die betroffene Person gemäß Art. 34 DSGVO zu benachrichtigen.

### 2.2. Fatale Ergebnisse bei unbesehener Anwendung auf Notare

So sinnvoll diese Regelungen bei anderen Verantwortlichen sein mögen, so fatal wäre ihre uneingeschränkte Anwendung bei Notaren. Dazu ein Beispiel:

*Eine ältere Dame errichtet beim Notar ein Testament. Darin setzt sie ihre Kinder mit unterschiedlichen Quoten zu Erben ein, zugunsten einer Enkelin setzt sie ein Vermächtnis aus. Dazu nimmt der Notar die persönlichen Daten der Begünstigten auf. Vor ihrem Tod sollen aber weder ihre Kinder noch die Enkelin von dem Testament erfahren, weil sie wegen der unterschiedlichen Erbquoten und des Vermächtnisses familiäre Schwierigkeiten befürchtet.*

Würde der Notar uneingeschränkt den genannten Pflichten nach Art. 14, 15 und 34 DSGVO unterliegen, müsste er im Beispielsfall die Kinder und die Enkelin informieren bzw. benachrichtigen und diese hätten jeweils einen entsprechenden Auskunftsanspruch gegen den Notar u. a. darauf, welche personenbezogenen Daten der Notar für welchen Zweck verarbeitet hat.

Es liegt auf der Hand, dass entsprechende Pflichten nicht mit der notariellen Verschwiegenheitsverpflichtung nach § 18 BNotO vereinbar wären. Dabei ist zu berücksichtigen, dass diese Verschwiegenheitsverpflichtung letztlich auch Ausfluss des Grundrechts auf informationelle Selbstbestimmung (Art. 2 Abs. 1 LV BaWü i. V. m. Art. 2 und 1 GG) der Beteiligten ist. Die Dame im Beispielsfall übt ihr Recht dahingehend aus, dass die von ihr im Testament genannten Personen nichts vom Testament erfahren sollen. Eine entsprechende Verpflichtung des Notars bzw. entsprechende Auskunftsrechte würden dieses Grundrecht der Beteiligten am notariellen Verfahren verletzen.

Hier zeigt sich exemplarisch, dass dem Notar von den Bürgerinnen und Bürgern häufig hochsensible personenbezogene Information anvertraut werden, die oft privaten Charakter haben. Diesem Umstand hat der Gesetzgeber in der Bundesnotarordnung, ähnlich auch im

<sup>3</sup> BGBl. I 2017, 2097.

<sup>4</sup> Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.4.2016 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, S. 1.

Beurkundungsgesetz, durch sehr genaue Regeln über Speicherung, Übermittlung und Löschung von Informationen Rechnung getragen.<sup>5</sup> Die dem Notar auferlegte strenge Verschwiegenheitspflicht, die über allgemeines Datenschutzrecht weit hinausreicht und angesichts der strafrechtlichen Sanktionsvorschrift (§ 203 Abs. 1 Nr. 3 StGB) und der mit ihm korrelierenden Zeugnisverweigerungsrechte (§ 53 Abs. 1 Nr. 3 StPO) höchsten Rang genießt,<sup>6</sup> wäre gefährdet. Es bedarf daher besonderer Regelungen, um die Regelungen des Datenschutzes in dieses System einzupassen.

### 2.3. Ausdrückliche Ausnahmen für Geheimhaltungsverpflichtete im BDSG-neu

Für die Informationspflicht nach Art. 14 DSGVO sieht Art. 14 Abs. 5 lit. d) DSGVO eine ausdrückliche Ausnahme vor, wenn die Daten nach Unionsrecht oder dem Recht der Mitgliedstaaten dem Berufsgeheimnis unterliegen und daher vertraulich behandelt werden müssen. Diese Ausnahme wird in § 29 Abs. 1 Satz 1 BDSG-neu aufgegriffen. Darüber hinaus sieht § 29 Abs. 1 Satz 2 BDSG-neu zudem vor, dass ein Recht auf Auskunft nach Art. 15 DSGVO nicht besteht, soweit durch die Auskunft Informationen offenbart würden, die „nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen“. Gleiches gilt nach § 29 Abs. 1 Satz 3 BDSG-neu für die Benachrichtigungspflicht nach Art. 34 DSGVO. Durch diese Regelung ist es möglich, dass § 18 BNotO als Rechtsvorschrift auch im Rahmen der genannten Normen der DSGVO angemessen berücksichtigt werden kann. Die entsprechenden Ausnahmen können auf die Öffnungsklauseln in Art. 23 Abs. 1 lit. e) und i) DSGVO gestützt werden.

### 2.4. Keine ausreichende Lösung durch § 2 Abs. 3 LDSG-E

Nach § 8 Abs. 1 Nr. 4 LDSG-E besteht eine Informationspflicht nicht, soweit und solange die Daten oder die Tatsache der Verarbeitung zum Schutze der betroffenen Person oder der Rechte anderer Personen geheim gehalten werden müssen. Dies gilt entsprechend auch für das Auskunftsrecht (Art. 15 DSGVO) gemäß § 9 Abs. 1 Satz 1 LDSG-E sowie für die Benachrichtigungspflicht (Art. 34 Nr. 2 DSGVO) gemäß § 11 Nr. 2 LDSG-E.

In dieser Norm fehlt also das Tatbestandsmerkmal „nach einer Rechtsvorschrift“, das § 29 Abs. 1 BDSG enthält. Entsprechend stützt die Begründung die Ausnahme nur auf die Öffnungsklausel des Art. 23 Abs. 1 lit. i) DSGVO (die nur den Schutz der betroffenen Person oder der Rechte und Freiheiten anderer Personen erfasst)<sup>7</sup> und nicht auch auf Art. 23 Abs. 1 lit. e) DSGVO (Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats).

Die Entwurfsverfasser gehen offenbar davon aus, dass eine entsprechende Erwähnung (der Geheimhaltungspflichten) nach anderen Rechtsvorschriften in § 8 Abs. 1 LDSG-E nicht notwendig sei. So findet sich in der Entwurfsbegründung der Hinweis, dass gesetzliche Geheimhaltungsvorschriften bei den Fällen, in denen eine Informationspflicht nach § 8 Abs. 1 LDSG-E nicht besteht, deshalb nicht genannt werden, weil diese „die Informationspflicht kraft ihres Vorrangs gemäß § 2 Absatz 3 [LDSG-E] ebenfalls entfallen lassen“. § 2 Abs. 3 Satz 1 LDSG-

<sup>5</sup> Rüpke, NJW 1991, 548,

<sup>6</sup> Rüpke, NJW 1991, 548,

<sup>7</sup> Siehe S. 18 ff. der Begründung zum LDSG-E.

E lautet wie folgt: „Soweit besondere Rechtsvorschriften des Bundes oder des Landes auf personenbezogene Daten anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor.“

- § 18 BNotO (notarielle Verschwiegenheitspflicht) geht als Rechtsvorschrift des Bundes nach § 2 Abs. 3 LDSG-E nur den Vorschriften *dieses Gesetzes* – also dem LDSG-E – vor, nicht aber der DSGVO. § 2 Abs. 3 LDSG-E selbst kann damit keine Ausnahme von den Pflichten bzw. Rechten nach Art. 14, 15 und 34 DSGVO statuieren.
- Allerdings kann § 18 BNotO selbst als entsprechende „Beschränkungsnorm“ i. S. d. Art. 23 Abs. 1 lit. i) und e) DSGVO angesehen werden, die die Pflichten und Rechte nach Art. 14, 15 und 34 DSGVO einschränkt. § 2 Abs. 3 LDSG-E hätte bei diesem Verständnis lediglich den Zweck klarzustellen, dass die Regelungen des LDSG-E nicht wiederum die Pflichten aus § 18 BNotO einschränken. Dieses Verständnis des § 18 BNotO ist zwar u. E. richtig. Allerdings ist sie nicht zwingend und rein tatsächlich gesehen, hat sich zumindest der Gesetzgeber des BDSG-neu für eine entsprechende Klarstellung entschieden. Aus unserer Sicht sollte daher auch im LDSG-E eine entsprechende Klarstellung erfolgen, um Missverständnisse – etwa dahingehend, dass § 8 Abs. 1 Nr. 4 LDSG-E eine abschließende Regelung enthält – von vornherein zu vermeiden. Denn über das Ergebnis, dass entsprechende Pflichten und Rechte nach der DSGVO bei einer Geheimhaltungsverpflichtung nicht bestehen – so ergibt es sich aus der Entwurfsbegründung – dürfte kein Dissens bestehen.

## 2.5. Vorschlag

Der LDSG-E sollte um eine Regelung ergänzt werden, die § 29 Abs. 1 BDSG-neu entspricht. Da § 12 LDSG-E ohnehin eine besondere Regelung zur Verarbeitung personenbezogener Daten enthält, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, bietet es sich an, diese Norm um einen entsprechenden Absatz zu ergänzen.

## 3. Zugangs- und Durchsuchungsbefugnisse des Landesbeauftragten für Datenschutz

### 3.1. Befugnisse der oder des Landesbeauftragten für Datenschutz nach Art. 58 DSGVO

Nach Art. 58 Abs. 1 DSGVO hat die Aufsichtsbehörde (hier also der oder die Landesbeauftragte für Datenschutz nach § 19 LDSG-E) Untersuchungsbefugnisse, die es ihr u. a. gestatten, Zugang zu allen personenbezogenen Daten und Informationen, die zur Erfüllung ihrer Aufgaben notwendig sind (lit. e), und Zugang zu den Geschäftsräumen, einschließlich aller Datenverarbeitungsanlagen und –geräte (lit. f), zu erhalten.

Nach Art. 90 Abs. 1 DSGVO können die Mitgliedstaaten diese Befugnisse gegenüber Verantwortlichen, die einem Berufsgeheimnis unterliegen, regeln, um das Recht auf Schutz personenbezogener Daten mit der Pflicht zur Geheimhaltung in Einklang zu bringen.

### 3.2. Keine Einschränkung der Befugnisse nach dem LDSG-E im Gegensatz zu § 29 Abs. 3 BDSG-neu

Von der Öffnungsklausel in Art. 90 DSGVO hat § 29 Abs. 3 BDSG in der ab dem 25.5.2018 geltenden Fassung<sup>8</sup> („BDSG-neu“) zu Recht Gebrauch gemacht. Danach bestehen diese Untersuchungsbefugnisse der Aufsichtsbehörden gegenüber den in § 203 Abs. 1, 2a und 3

<sup>8</sup> BGBl. I 2017, 2097.

StGB genannten Personen (also auch Notaren) nicht, soweit die Inanspruchnahme der Befugnisse zu einem Verstoß gegen die Geheimhaltungspflichten dieser Personen führen würde.

Der LDSG-E enthält hingegen keine entsprechende besondere Ausnahmeregelung. Im Gegenteil, die Kontrolle der oder des Landesbeauftragten für Datenschutz erstreckt sich nach § 24 Abs. 5 LDSG-E ausdrücklich auch auf personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen.

### 3.3. Ausnahme analog § 29 Abs. 3 BDSG-neu unbedingt geboten

Die Zugangs- und Durchsuchungsbefugnisse der oder des Landesbeauftragten für Datenschutz berücksichtigen nicht die besondere Stellung der Notare als Organ der vorsorgenden Rechtspflege und die Besonderheiten der notariellen Verschwiegenheitspflicht. Die Normen greifen in unangemessener Weise in die Geheimhaltungsbedürfnisse der Bürgerinnen und Bürger ein, die Notaren und anderen Berufsgeheimnistägern schützenswerte, hochsensible und persönliche Informationen in dem Wissen anvertrauen, dass sie absolut geheim behandelt und streng vor dem Zugriff Dritter geschützt werden. Die Verschwiegenheitspflichten sollen das Recht auf informationelle Selbstbestimmung gerade auch gegenüber dem Staat gewährleisten, der hier in Form einer Aufsichtsbehörde auftritt. Hier tritt die ureigene Funktion dieses Grundrechts als Abwehrrecht gegenüber dem Staat zutage, der der Entwurf bisher nicht hinreichend Rechnung trägt.

Das Vertrauen der Bürgerinnen und Bürger in Notare und andere in § 203 StGB genannte Berufsgeheimnisträger würde erheblich beschädigt, wenn der oder die Landesbeauftragte für Datenschutz voraussetzungslos und schrankenlos die Geschäftsräume und Datenverarbeitungsanlagen und -geräte durchsuchen dürfte. Eine entsprechende Regelung wäre auch verfassungswidrig, weil es sich um einen unverhältnismäßigen Eingriff nicht nur in die Grundrechte der Berufsgeheimnisträger, sondern auch mittelbar in die Grundrechte der Betroffenen handelte.

- Notare unterliegen der Verschwiegenheitspflicht nach § 18 BNotO, deren pflichtgemäße Erfüllung von den Aufsichtsbehörden i. S. d. §§ 92 BNotO geprüft (und sanktioniert) werden kann. Zudem sind etwaige Verletzungen strafbewehrt nach § 203 StGB.
- Die Gesetzesbegründung zum Gesetzentwurf des BDSG-neu geht zu Recht davon aus,<sup>9</sup> dass es „ohne eine Einschränkung der Befugnisse der Aufsichtsbehörden [...] zu einer Kollision mit Pflichten des Geheimnisträgers [käme]. Gerade bei den freien Berufen schützt die berufsrechtliche Schweigepflicht das Vertrauen des Mandanten und der Öffentlichkeit in den Berufsstand. Nach bundesverfassungsgerichtlicher Rechtsprechung darf das Mandatsverhältnis nicht mit Unsicherheiten hinsichtlich seiner Vertraulichkeit belastet sein (vgl. BVerfG, Urteil vom 12. April 2005 – 2 BvR 1027/02).“
- Schließlich haben es die Bürgerinnen und Bürger selbst in der Hand, eine entsprechende Überprüfung durch den Staat zu ermöglichen. Denn sie sind insoweit dispositionsbefugt und berechtigt, den Notar von seiner Verschwiegenheitspflicht zu entbinden. In diesem Fall kann die oder der Landesbeauftragte für Datenschutz

<sup>9</sup> BT-Drucks. 18/11325, S. 101.

problemlos die Einhaltung des Datenschutzrechts überprüfen. Erfolgt hingegen keine Entbindung von der Schweigepflicht, ist kein Grund ersichtlich, warum der Staat gegen den Willen der Betroffenen den Geheimnisschutz brechen können soll.

#### 3.4. Vorschlag

Im Ergebnis ist daher unbedingt eine Ausnahmeregelung analog § 29 Abs. 3 BDSG-neu in den LDSG-E aufzunehmen. Auch insoweit bietet es sich aus unserer Sicht an, § 12 LDSG-E um einen entsprechenden Absatz zu ergänzen.

Wenn Sie Fragen haben oder weitere Informationen benötigen, erreichen Sie mich am besten telefonisch oder per E-Mail.

Mit freundlichen Grüßen

  
Florence Wetzel



**BBW**  
Beamtenbund  
Tarifunion

BBW – Beamtenbund Tarifunion, Postfach 103011, 70005 Stuttgart

Ministerium für Inneres, Digitalisierung und  
Migration Baden-Württemberg

- per E-Mail -

Der Vorsitzende

Arni Hebenberger TZ  
70188 Stuttgart

Telefon 0711/1 68 76-0

Telefax 0711/1 68 76-76

Internet <http://www.bbwtarifunion.de>

E-Mail: [bbw@bbwtarifunion.de](mailto:bbw@bbwtarifunion.de)

24. Januar 2018

Ha/ie/4475/18

Betr.: Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679

Bezug: E-Mail vom 19.12.2017; Az.: 2-0557.8/1

Sehr geehrte Damen und Herren,

der BBW – Beamtenbund und Tarifunion (BBW) dankt für den o. g. Anhörungsentwurf und die Gelegenheit zur Stellungnahme.

Zum Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679 nehmen wir wie folgt Stellung:

Der BBW und sein Dachverband dbb beamtenbund und tarifunion begrüßen den Willen, die erforderlichen Gesetzesanpassungen, die sich aus der europäischen Rechtssetzung ergeben, vorzunehmen. Wir sind der Auffassung, dass eine zügige Umsetzung der oben genannten Richtlinie bzw. die Ausfüllung der durch die oben genannte Verordnung eingeräumten Spielräume geboten ist, um eine Harmonisierung der europarechtlichen Vorgaben mit dem deutschen Recht auch auf landesrechtlicher Ebene voran zu treiben. Hinzu kommt, dass die technische Entwicklung immer schneller voranschreitet, so dass die Fragen der Datenerhebung, -verarbeitung und -nutzung zunehmend drängender werden. Technisch ist heute vieles machbar, was noch vor einigen Jahren kaum denkbar war. Für uns geht es vordringlich um die Frage der sinnvollen Begrenzung und um die Regelung des Machbaren.

Generell war aus unserer Sicht zunächst die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zu freiem Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG

- 2 -

(im Folgenden: Datenschutz-Grundverordnung – DSGVO) sehr zu begrüßen, weil sie ein einheitlich hohes Datenschutzniveau für die gesamte Union festschreibt. Gleichzeitig hat die DSGVO aber auch etwa 70 Öffnungsbereiche, in denen durch nationale Regelungen von den Vorgaben der DSGVO abgewichen werden kann. Im Prinzip sind drei deutlich weicher geregelte Tatbestände in der DSGVO enthalten, die hinter dem bisherigen deutschen BDSG zurückbleiben, das sind die mündliche Einwilligung, die Löschregelung und der fehlende Beschäftigtendatenschutz, den sich die Protagonisten mit Kollektivvereinbarungen jeweils im Einzelnen selbst schaffen sollen, und dann noch eben diese Öffnungsklauseln, vor allem bei den Bußgeldvorgaben.

Von besonderer Bedeutung sind für uns insbesondere die Fragen im Zusammenhang mit dem Datenschutz im Beschäftigungsverhältnis.

Wir fordern grundsätzlich, dass auf die Verwendung unbestimmter Rechtsbegriffe verzichtet wird, wenn klare Definitionen und eindeutige Voraussetzungen geschaffen werden können, so dass die Voraussetzungen und Grenzen bezüglich eines Eingriffs in das Recht auf informationelle Selbstbestimmung eindeutig für jeden bestimmbar sind. Aus unserer Sicht bedarf der Schutz personenbezogener Daten einer systematischen und normenklaren Regelung, um Rechtsklarheit und Rechtssicherheit zu erreichen. Diesen Anforderungen genügt der vorliegende Entwurf nicht.

Wichtige Fragestellungen, wie beispielsweise die Verwendung von Daten aus sozialen Medien im Rahmen von Einstellungsverfahren, werden weiterhin nicht hinreichend beantwortet. Auch die Einräumung der Möglichkeit der Videoüberwachung bereits bei Vorliegen einer abstrakten Gefahr stellt aus unserer Sicht ebenfalls keine eindeutige Regelung dar.

Für den BBW als gewerkschaftliche Interessenvertretung stehen die Rechte und der Schutz der Beschäftigten im Mittelpunkt. Die Ausgestaltung des Datenschutzes und des gesetzlichen Beschäftigtendatenschutzes muss diesen Grundsätzen gerecht werden und sowohl größtmöglichen Schutz als auch größtmögliche Transparenz bieten. Die rechtliche Ausgestaltung von Regelungsnormen und Schutzvorschriften sollte aus unserer Sicht daher zumindest den Anspruch haben, auch dem betroffenen Personenkreis eine Orientierung über die getroffenen Regelungen zu bieten. Uns ist bewusst, dass man diesem Anspruch an Transparenz bereits in der methodischen Gestaltung nicht gerecht werden kann, da stets eine Zusammenschau von landesrechtlichen Regelungen mit den europarechtlichen Vorschriften notwendig ist und weiterhin das Wiederholungsverbot gilt. Dies ist im Ergebnis jedoch wenig anwenderfreundlich. Sinnvoll wäre aus unserer Sicht zumindest die Zurverfügungstellung einer ‚durchgeschriebenen‘ Version, die auf Verweisungen verzichtet und eine selbsterklärende Struktur bietet.

Der BBW weist darauf hin, dass die Umsetzung der geplanten Gesetzesänderungen voraussetzt, dass auf allen Ebenen der öffentlichen Verwaltung entsprechend qualifiziertes Personal zur Verfügung steht. Dabei sind, gerade im IT-Bereich, entsprechend der Wettbewerbssituation mit der

- 3 -

Privatwirtschaft, angemessene Einkommens- und Beschäftigungsbedingungen und Qualifizierungsangebote zu gewährleisten.

#### **Zu Art. 17 – Änderung des Landesbeamtengesetzes**

Mit der europäischen Reform des Datenschutzrechts durch die Datenschutz-Grundverordnung sind viele grundlegende Regelungen für die Mitgliedstaaten getroffen worden. Daneben enthält die DSGVO zahlreiche Regelungsaufträge und Öffnungsklauseln, die auf nationaler Ebene umgesetzt werden müssen. Insoweit wirkt sich die DSGVO auch auf die beamtenrechtlichen Regelungen zum Personalaktenrecht aus.

Nach Auffassung des BBW wäre es sinnvoll, in den Vorschriften zum Personalaktenrecht im LBG ausdrücklich darauf hinzuweisen, dass in Teilen die Regelungen in der DSGVO abschließend sind (wie z. B. in Bezug auf Art. 28 und 29 hinsichtlich der Datenverarbeitung im Auftrag).

#### **Zu § 83 - Verarbeitung**

§ 83 LBG in bisheriger Fassung bezog sich auf die „Erhebung“ von Personalaktendaten. Im Weiteren regelte § 84 LBG in bisheriger Fassung die Speicherung, Veränderung oder Nutzung von Personalaktendaten. In der DSGVO wird generell von dem Begriff der „Verarbeitung“ personenbezogener Daten ausgegangen. Dieser beinhaltet nach Art. 4 Nr. 2 DSGVO „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung“. Vor diesem Hintergrund soll § 83 LBG dahingehend neu gefasst werden, dass der Regelungsumfang der Norm vom Teilaspekt des „Erhebens“ auf die gesamte „Verarbeitung“ erweitert wird. Diese Erweiterung ist grundsätzlich nicht zu beanstanden.

Zudem wird die bisher in § 83 LBG verwendete Formulierung, dass Personalaktendaten „nur“ unter bestimmten Voraussetzungen erhoben werden dürfen, gestrichen. Wie aus der Begründung hervorgeht, erfolgt diese Streichung aus dem Grund, dass sich für bestimmte Verarbeitungssituationen eine Ermächtigung zur Datenverarbeitung direkt aus der DSGVO ergeben könne. Aus Sicht des dbb sollte sich das jedoch auch im Gesetzestext widerspiegeln und nicht nur in der Begründung genannt werden. Wir regen daher an, das Wort „nur“ beizubehalten, aber folgenden Zusatz hinzuzufügen: „,es sei denn, für bestimmte Verarbeitungssituationen ergibt sich eine Ermächtigung zur Datenverarbeitung direkt aus der Verordnung (EU) 2016/679.“

- 4 -

Zur Erleichterung der Anwendungspraxis wäre zudem wünschenswert, dass in der Gesetzesbegründung Beispiele dazu aufgeführt werden.

#### **Zu § 87 – Auskunft, Anhörung**

In Absatz 3 Satz 2 wird geregelt, dass auf Verlangen Abschriften, Kopien oder Ausdrücke, auch auszugsweise, gefertigt werden. Hier sollte aus Gründen der Klarheit hinzugefügt werden, dass den Beamtinnen und Beamten diese Abschriften, Kopien oder Ausdrücke auf Verlangen auch zu überlassen sind.

In Absatz 4 ist die Regelung vorgesehen, dass Feststellungen über den Gesundheitszustand nicht der Auskunft unterliegen, wenn zu befürchten ist, dass die betroffene Beamtin oder der betroffene Beamte bei Kenntnis des Befundes weiteren Schaden an der Gesundheit nimmt. Diese Beschränkung der Auskunftserteilung ist für uns nicht tragbar. Feststellungen über den Gesundheitszustand welcher Art auch immer dürfen den betroffenen Beamten/der betroffenen Beamtin nicht vorenthalten werden. Solche höchstpersönlichen, dem Gesundheitszustand betreffenden Informationen muss der Betroffene erhalten. Der Dienstherr darf an dieser Stelle keine Wertung vornehmen.

#### **Zu Art. 19 – Änderung des Landespersonalvertretungsgesetzes**

Wir sind der Auffassung, dass die Datenschutz-Grundverordnung eigentlich keine Auswirkungen auf die personalvertretungsrechtlichen Vorschriften hat, da die Personalvertretungen Teil der Dienststelle sind und somit im Verhältnis Dienststellenleiter - Personalrat keine Weitergabe von Daten an Dritte erfolgt. Änderungen sind somit grundsätzlich nicht erforderlich.

Vor diesem Hintergrund sind die Änderungen in Art 19 Nr. 1 und 2 aber nicht zu beanstanden. In Art. 19 Nr. 3 wird hingegen das Beteiligungsrecht durch einen Wechsel von einem Widerspruchsrecht hin zu einem Zustimmungsvorbehalt eingeschränkt.

Wir bitten Sie, unsere Anregungen aufzugreifen.

Mit freundlichen Grüßen

  
Kai Rosenberger



**Landesverband  
Baden-Württemberg**

Landesverband Baden-Württemberg  
Der Vorsitzende

Bund Deutscher Finanzrichter Landesverband Baden-Württemberg • Börsenstraße 6 • 70174 Stuttgart

An das

Datum 30.01.2018

Name Ewald Lamminger

MINISTERIUM FÜR INNERES,  
DIGITALISIERUNG UND MIGRATION  
BADEN-WÜRTTEMBERG

Aktenzeichen 2-0557.8/1\_Stellungnahme BDFR  
(Bitte bei Antwort angeben)

Per E-Mail: [Registatur2@im.bwl.de](mailto:Registatur2@im.bwl.de)

**Entwurf eines Gesetzes zur Anpassung des allgemeinen  
Datenschutzrechts und sonstiger Vorschriften an die Verordnung  
(EU) 2016/679**

Sehr geehrte Damen und Herren,

ich bedanke für die eingeräumte Möglichkeit zur Stellungnahme zu dem vorgenannten Gesetzesentwurf. Im Hinblick auf die Komplexität und den kurzen Zeitrahmen für eine Stellungnahme war eine vertiefte Auseinandersetzung und verbandsinterne Diskussion leider nicht möglich. Trotzdem ist aus Sicht der Finanzgerichtsbarkeit auf Folgendes hinzuweisen:

Nach § 2 Abs. 5 Landesdatenschutzgesetz-Entwurf (LDSG-E) gilt das Gesetz für die Gerichte nur, soweit sie in Verwaltungsangelegenheiten tätig werden.

Die EU-Datenschutzgrundverordnung (VO (EU) 2016/679, -DSGVO-) normiert jedoch in Art. 12 - 21 sog. Betroffenenrechte, die für alle „Verantwortlichen“ im Sinne des Art. 4 Nr. 7 DSGVO und mithin auch für die Gerichte unmittelbar gelten (vgl. insoweit Satz 1 des 20. Erwägungsgrundes sowie Art. 2 DSGVO).

Nach Art. 23 Abs. 1 f) DSGVO können für die Justiz insoweit Ausnahmen bestimmt werden. Nachdem hiervon im neugefassten Bundesdatenschutzgesetz (BDSG) kein

Börsenstraße 6 • 70174 Stuttgart • Telefon 0711 6685-207 • Telefax 0711 6685-199  
VVS Haltestelle: Friedrichsbau (Linien U9 und U14); S-Bahnhaltestelle Stadtmitte (Linien S1 bis S6)  
[lamminger@fgstuttgart.justiz.bwl.de](mailto:lamminger@fgstuttgart.justiz.bwl.de) • [www.bdff.de](http://www.bdff.de)  
Sprechzeiten: nach Vereinbarung

- 2 -

Gebrauch gemacht wurde, sollten im vorliegenden Gesetzesentwurf entsprechende Beschränkungen der Betroffenenrechte aufgenommen werden.

Eine entsprechende Regelungskompetenz folgt aus § 1 Abs. 2 Nr. 2 BDSG.

Sie ist auch erforderlich, da ansonsten eine Beeinträchtigung der gerichtlichen Arbeit zu befürchten ist.

Gestützt auf Art. 17 Abs. 1 d) DSGVO könnten Beteiligte die Löschung von Daten fordern oder gestützt auf Art. 18 Abs. 1 a) die Sperrung ihrer personenbezogenen Daten verlangen. Inwieweit dann eine Verwertung durch das Gericht trotzdem zulässig bliebe (vgl. Art. 17 Abs. 3 e) DSGVO), erscheint zumindest zweifelhaft.

Entsprechendes gilt bei den Informationspflichten nach Art. 14 DSGVO. Im finanzgerichtlichen Verfahren werden u.a. die Veranlagungsakten bei den Finanzbehörden angefordert. Inwieweit eine Informationspflicht gestützt auf Art. 14 Abs. 5 c) bzw. d) entfallen kann, ist unklar und damit klärungsbedürftig.

Nach der bisherigen Fassung des § 83 Landesbeamtengesetz (LBG) darf der Dienstherr unter bestimmten Voraussetzungen Personalaktendaten **erheben**. Nach der Neufassung darf er Personalaktendaten **verarbeiten**, der Regelungsinhalt wird mithin erweitert, ohne dass ein sachlicher Grund hierfür ersichtlich wäre. Sollte hiermit eine Aushöhlung der Mitbestimmungsrechte der Personalgremien intendiert sein, so wäre die Neuregelung abzulehnen. In jedem Fall ist eine Klarstellung erforderlich.

Nach Erwägungsgrund 20 der DSGVO sollen die Aufsichtsbehörden nicht für die Verarbeitung personenbezogener Daten durch Gerichte im Rahmen ihrer justiziellen Tätigkeit zuständig sein. Mit der Aufsicht über diese Datenverarbeitungsvorgänge sollten besondere Stellen im Justizsystem des Mitgliedstaats betraut werden können, die insbesondere die Einhaltung der Vorschriften dieser Verordnung sicherstellen, Richter und Staatsanwälte besser für ihre Pflichten aus dieser Verordnung sensibilisieren und Beschwerden in Bezug auf derartige Datenverarbeitungsvorgänge bearbeiten sollten. Der vorliegende Gesetzesentwurf sieht insoweit keine Regelung vor.

Mit freundlichen Grüßen



Lamminger



## Bund Deutscher Kriminalbeamter

### Landesverband Baden-Württemberg

BDK Baden-Württemberg | August-Borsig-Straße 2 | D-71032 Böblingen

Ministerium für Inneres, Digitalisierung und Migration Baden-Württemberg

nur per E-Mail  
an [poststelle@im.bwl.de](mailto:poststelle@im.bwl.de)  
cc an: [Registatur2@im.bwl.de](mailto:Registatur2@im.bwl.de)

#### Ihr Zeichen

Schreiben vom 19.12.2017,  
Az. 2-0557.8/1

**Unser Ansprechpartner**  
Steffen Mayer

**Funktion**  
Landesvorsitzender

Böblingen, 31.01.2018

### Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679

Sehr geehrte Damen und Herren,

wir danken Ihnen für die Einbindung. Wir begrüßen die Stärkung der Stellung des Landesbeauftragten für den Datenschutz und das erklärte Ziel, den Beschäftigtendatenschutz zu festigen. Gerade im Beschäftigtendatenschutz sehen wir im täglichen Dienst, dass immer noch Daten der Beschäftigten verarbeitet werden, die nicht zwingend für die konkrete Aufgabe erforderlich sind. So werden beispielsweise in einer Dienststelle für die Verfahrensberechtigung von DV-Anwendern Geburtsdatum und Geburtsort als erforderliche Felder aufgeführt und erhoben, obwohl über die Benutzerkennung (USBNK) und die Personalnummer eine zweifelsfreie systemseitige Zuordnung für die Erteilung einer DV-Berechtigung völlig ausreicht. Zweites Beispiel: In einer landesweiten Anwendung zur Administration des Dienstsports, die jüngst landesweit ausgerollt wird, wird die Amtsbezeichnung als Datum erhoben bzw. verarbeitet.

Zu Artikel 11, Änderung des Flüchtlingsaufnahmegesetzes: Wir geben zu bedenken, dass der neu eingefügte vollständige Ausschluss der Verarbeitung genetischer Daten, die Nutzung der Ergebnisse einer molekulargenetischen Analyse vollständig verhindert. Die zulässige Verarbeitung biometrischer Daten fokussiert gemäß Begründung hingegen auf die Gestalt der Fingerabdruckdaten. Die Erfahrungen des kriminalpolizeilichen Erkennungsdienstes zeigen, dass es Menschen gibt, bei denen keine entsprechenden Fingerabdrücke abgenommen werden können, weil sie durch (dauerhafte) Verletzungen oder gezielte Manipulationen verändert worden sind und

**Bund Deutscher Kriminalbeamter** | Landesverband Baden-Württemberg  
August-Borsig-Straße 2 | D-71032 Böblingen  
Telefon +49 (0)7031 605112 | E-Mail: [lv.bw@bdk.de](mailto:lv.bw@bdk.de)  
Internet: [www.bdk.de](http://www.bdk.de) | <https://www.facebook.com/bdk.bw>  
Landesvorsitzender: Steffen Mayer | Mobil: 0157 58431010

Der BDK ist Mitglied im  
■ **Conseil Européen des Syndicats de Police**  
■ **Stifterrat Deutsches Forum für Kriminalprävention**  
■ **Netzwerk Europäische Bewegung, Deutschland**  
■ **Cyber-Sicherheitsrat Deutschland e.V.**



## **Bund Deutscher Kriminalbeamter**

### **Landesverband Baden-Württemberg**

---

damit kein verlässliches Ergebnis bieten. Mindestens in solchen Fällen könnte die Molekulargenetik eine ernsthafte Alternative zur eindeutigen Identifizierung von Personen bieten (mit Ausnahme von eineiigen Zwillingen gleichen Geschlechts).

Mit freundlichen Grüßen

A handwritten signature in black ink, appearing to read 'Steffen Mayer', is written over the printed name.

Steffen Mayer  
BDK-Landesvorsitzender BW

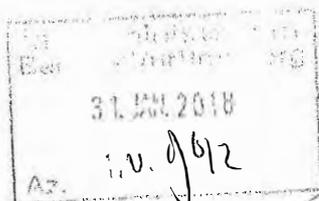


Deutsche  
Rentenversicherung  
Baden-Württemberg

Deutsche Rentenversicherung Baden-Württemberg  
76122 Karlsruhe

Die Geschäftsführung  
Gartenstr. 105, 76135 Karlsruhe

Ministerium für Inneres,  
Digitalisierung und Migration  
Postfach 10 34 65  
70029 Stuttgart



196.2

Anfahrt:  
Straßenbahnlinie 1, 5 oder  
Buslinie 55 (Haltestelle  
Weinbrennerplatz)

Ihr Zeichen	Ihre Nachricht	Unsere Nachricht	Geschäftszeichen (Bei Zuschrift bitte immer angeben)	Datum
2-0557.8/1	19.12.2017		01035000508/ST-LDSG-N	29.01.2018

**Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und sonstiger an die Verordnung (EU) 2016/679 hier: Stellungnahme zum Anhörungsverfahren**

Sehr geehrte Damen und Herren,

nach Durchsicht des Gesetzentwurfs sollten aus unserer Sicht folgende Änderungs- und Ergänzungsvorschläge im weiteren Gesetzgebungsverfahren berücksichtigt werden:

• **Artikel 17 (Änderung des Landesbeamtengesetzes)**

Die letzte Änderung des Landesbeamtengesetzes erfolgte durch *Artikel 8 des Gesetzes vom 21. November 2017 (GBl. S. 597, 605)*.  
Deshalb ist die die Gesetzesangabe im zweiten Halbsatz hier zu berichtigen

• **Hinzufügung eines neuen Artikels (Änderung des Landeskrebsregistergesetzes)**

Teilaspekte der Verarbeitung nach der Verordnung (EU) 2016/679, die bisher ausdrücklich im Gesetz genannt sind (Erhebung, Verarbeitung, Nutzung) sind jetzt vom Begriff der Verarbeitung umfasst. Deshalb sollte der § 16 des LKrebsRG entsprechend geändert werden.

Freundliche Grüße

Schwarz  
Vorsitzender der Geschäftsführung



2-0557.8/1/183

Landesbank BW  
IBAN: DE20 60050101 0002001485  
BIC: SOLADEST600

DZ Bank  
IBAN: DE26 66060000 0000055522  
BIC: GENODE6KXXX

www.deutsche-rentenversicherung-bw.de  
De-Mail: postfach@drv-bw.de-mail.de  
E-Mail: info@drv-bw.de  
Telefonzentrale: Karlsruhe 0721 825-0  
Stuttgart 0711 848-0





Deutscher Gewerkschaftsbund  
**Bezirk Baden-Württemberg**

DGB-Bezirk Baden-Württemberg | Willi-Bleicher-Str. 20 | 70174 Stuttgart  
Ministerium für Inneres, Digitalisierung und  
Migration Baden-Württemberg

Postfach 10 34 65  
70029 Stuttgart

vorab per Email: [registratur2@im.bwl.de](mailto:registratur2@im.bwl.de)

**Stellungnahme des DGB zum Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts an die Verordnung (EU) 2016/679 – Az.: 2-0557.8/1** 31. Januar 2018

Sehr geehrte Damen und Herren,  
sehr geehrter Herr

**Dominik Gaugler**  
Abteilungsleiter  
Öffentlicher Dienst / Beamte / Recht /  
Kommunalpolitik

vielen Dank für die Gelegenheit zur Stellungnahme des DGB Baden-Württemberg zum Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts an die Verordnung (EU) 2016/679.

Willi-Bleicher-Str. 20  
70174 Stuttgart

Angefügt senden wir Ihnen unsere o. g. DGB-Stellungnahme.

Mit freundlichen Grüßen

Dominik Gaugler

Anlage

**Deutscher  
Gewerkschaftsbund**

**Bezirk  
Baden-Württemberg**

**Stellungnahme des DGB Baden-Württemberg**

zum Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts an  
die Verordnung (EU) 2016/679  
Az.: 2-0557.8/1

Stuttgart im Januar 2018



**Deutscher  
Gewerkschaftsbund****Bezirk  
Baden-Württemberg****Grundsätzliches**

Vor dem Hintergrund der unmittelbaren Geltung der EU-Datenschutz-Grundverordnung zum 25. Mai 2018 ist es nachvollziehbar, dass das neue Datenschutzgesetz für das Land Baden-Württemberg weniger Regelungen enthält, als das bisher geltende Landesdatenschutzgesetz.

Aufgrund der unmittelbaren Geltung der Artikel 37 bis 39 der EU-Datenschutz-Grundverordnung enthält der vorliegende Gesetzesentwurf jedoch keine Regelungen mehr zur Bestellung von behördlichen Datenschutzbeauftragten sowie deren Stellvertreterinnen und Stellvertreter.

Die Artikel 37 bis 39 der EU-Datenschutz-Grundverordnung sind jedoch an vielen Stellen sehr allgemein gefasst. So bleibt offen, auf welcher Ebene der Verwaltung künftig behördliche Datenschutzbeauftragte zu bestellen sind. Sollten diese unbestimmten Rechtsbegriffe nicht konkretisiert werden, werden sich vermutlich die Gerichte damit beschäftigen müssen.

Das bisherige Landesdatenschutzgesetz des Landes war hier eindeutiger. Danach sind behördliche Datenschutzbeauftragte immerhin als „Kann-Vorschrift“ enthalten.

Bereits in früheren Anhörungsverfahren hat sich der DGB Baden-Württemberg für eine verbindliche Einführung eines/r behördlichen Datenschutzbeauftragten stark gemacht. Mit Blick auf die wagen Regelungen der EU-Datenschutz-Grundverordnung und der Tatsache, dass persönliche Daten und deren Schutz in der heutigen Zeit immer bedeutender werden, ist es für den DGB Baden-Württemberg notwendig, eine verbindliche und klarstellende Regelung im Landesdatenschutzgesetz aufzunehmen.

Als unterstes Minimum sollte aus Sicht des DGB Baden-Württemberg gewährleistet sein, dass auf der Ebene jeder obersten Dienstbehörde eine behördliche Datenschutzbeauftragte oder ein behördlicher Datenschutzbeauftragter und eine Stellvertretung bestellt werden.

Dazu kommt, wenn nach Artikel 37 Abs. 6 der EU-Datenschutz-Grundverordnung der bzw. die behördliche Datenschutzbeauftragte seine Aufgaben auf der Grundlage eines Dienstleistungsvertrages erfüllt, muss aus Sicht des DGB Baden-Württemberg in der Behörde trotzdem ein Ansprechpartner bzw. eine Ansprechpartnerin vorhanden sein. Dies kann u. a. dadurch gewährleistet werden, dass in diesem Fall eine Stellvertretung bestellt wird, die in einem Dienst- oder Arbeitsverhältnis zur Behörde bzw. öffentlichen Stelle steht.

**Deutscher  
Gewerkschaftsbund****Bezirk  
Baden-Württemberg**

Die Ausführungen machen deutlich, dass es notwendig ist, eine gesetzliche Verpflichtung zur Bestellung eines/r behördlichen Datenschutzbeauftragten und einer entsprechenden Stellvertretung in das Gesetz aufzunehmen. Mindestens eine der beiden Personen sollte dabei in einem Beschäftigungsverhältnis zur öffentlichen Stelle bzw. Behörde stehen.

**Zu den inhaltlichen Regelungen im Einzelnen:****Artikel 1 Landesdatenschutzgesetz****Zu § 3 des vorliegenden Entwurfs**

Die Regelungen zum technischen Datenschutz sind für den DGB Baden-Württemberg von großer Bedeutung, gerade in einer Zeit in der technische Entwicklungen immer schneller und Innovationszyklen immer kürzer werden. Sowohl die Beschäftigten als auch die Bürgerinnen und Bürger müssen darauf vertrauen können, dass Behörden und öffentliche Stellen den technischen Datenschutz und damit Datensicherheit auf einem hohen Niveau gewährleisten. Nach dem aktuellen Stand der Technik ist deswegen ein angemessenes Schutzniveau für gespeicherte Daten sicherzustellen. Deshalb wäre für den DGB hier eine ergänzende Regelung sinnvoll, die die Einhaltung technischer Mindeststandards festschreibt. Diese könnte lauten:

*Die für die Datenverarbeitung verantwortlichen Stellen sind zur Einhaltung der einschlägigen Standards, der technischen Richtlinien und der Empfehlungen des zuständigen Bundesamtes für Sicherheit in der Informationstechnologie verpflichtet.*

**Zu § 14 des vorliegenden Entwurfs**

Die Regelungen des § 14 des Entwurfs ersetzen die bisherigen Regelungen des § 36 des Landesdatenschutzgesetzes zur Datenverarbeitung bei Dienst- und Arbeitsverhältnissen. Sie gelten damit für die Beschäftigten des öffentlichen Dienstes und ergänzen die spezialgesetzlichen Regelungen des Beamtenrechtes zum Umgang mit Personalakten bzw. Personalaktendaten.

Der DGB Baden-Württemberg weist an dieser Stelle darauf hin, dass auch bei allgemeinen Regelungen zur Datenverarbeitung bei Beschäftigungsverhältnissen im öffentlichen Dienst die Regelungen des § 50 des Beamtenstatusgesetzes zu Personalaktendaten zu beachten sind.

Ausdrücklich begrüßt der DGB Baden-Württemberg daher den Verweis auf die beamtenrechtlichen Regelungen in § 14 Abs. 3 des Entwurfs. Diese gewährleisten eine

**Deutscher  
Gewerkschaftsbund****Bezirk  
Baden-Württemberg**

einheitliche Rechtsanwendung für alle Beschäftigtengruppen und ermöglichen somit eine effektive Personalverwaltung im öffentlichen Dienst.

Der § 14 Abs. 6 wirft für den DGB Baden-Württemberg die Frage auf, ob dadurch am Ende eine nicht dauerhafte und nicht systematische Überwachung bzw. Gewinnung von Daten mit Hilfe anderer technischer Einrichtungen für den Zweck der Verhaltens- und Leistungskontrolle zulässig wären.

Aus Sicht des DGB Baden-Württemberg ist es von hoher Bedeutung, dass der Ausschluss der Verhaltens- und Leistungskontrolle an dieser Stelle möglichst weitgehend formuliert und ausgestaltet wird. Inhaltlich zu ergänzen wäre außerdem eine Regelung, die Daten mit einschließt, die erst in einem automatisierten Verfahren gewonnen werden. Der DGB Baden-Württemberg schlägt daher für den Abs. 6 folgende Formulierung vor:

*(6) Daten von Beschäftigten, die im Rahmen der Durchführung technischer und organisatorischer Maßnahmen zur Datensicherheit verarbeitet oder mit Hilfe von optisch-elektronischer, sonstiger technischer Einrichtungen oder in einem automatisierten Verfahren gewonnen werden, dürfen nicht zu Zwecken der Verhaltens- und Leistungskontrolle ausgewertet werden.*

Der DGB Baden-Württemberg bittet darüber hinaus zu prüfen, ob der § 14 nach dem Vorbild des § 32 Abs. 3 des Bundesdatenschutzgesetzes um einen weiteren Absatz ergänzt werden kann, der klarstellt, dass die Beteiligungsrechte der Interessenvertretungen der Beschäftigten unberührt bleiben. Der DGB Baden-Württemberg würde eine derartige Ergänzung ausdrücklich begrüßen. Eine derartige Regelung wäre auch ein Hinweis auf die notwendige weitere Ausgestaltung des Datenschutzes durch die betriebliche Mitbestimmung z. B. im Rahmen von IT-Fachverfahren.

**Zu Artikel 17 „Änderung des Landesbeamtengesetzes“****Zu § 83 des vorliegenden Entwurfs**

Im Vergleich zur alten Formulierung fehlt im neuen § 83 Abs. 1 Satz 1 die begrenzende Formulierung „nur“. Dieses wäre aus Sicht des DGB Baden-Württemberg wieder zu ergänzen, um sicherzustellen, dass der Dienstherr personenbezogene Daten über Bewerberinnen und Bewerber, Beamtinnen und Beamte sowie ehemalige Beamtinnen und Beamte nur verarbeiten darf, soweit dies im Rahmen der aufgeführten Tätigkeiten der Personalverwaltung oder Personalwirtschaft erforderlich ist oder eine (andere) Rechtsvorschrift dies erlaubt. Der Verweis auf die Personalverwaltung und Personal-

**Deutscher  
Gewerkschaftsbund****Bezirk  
Baden-Württemberg**

wirtschaft schließt dabei unmittelbar an die Formulierung im § 50 des Beamtenstatusgesetzes des Bundes an. Dieser regelt verbindlich, dass Personalaktendaten nur für die Zwecke der Personalverwaltung oder Personalwirtschaft verwendet werden dürfen, es sei denn, die Beamtin oder der Beamte willigt in die anderweitige Verwendung ein.

Für Ausnahmefälle kann landesrechtlich eine abweichende Verwendung vorgesehen werden. Die abweichende Verwendung ist damit auf explizit landesrechtlich geregelte Ausnahmefälle beschränkt. Ausnahmefälle sind jedoch immer darzustellen und als Ausnahmen zu begründen.

Die Ergänzung des Wortes „nur“ zur Begrenzung der Datenverarbeitung in § 83 Abs. 1 Satz 1 würde damit dem geltenden Bundesrecht entsprechen.

Des Weiteren lehnt der DGB Baden-Württemberg die geplanten Regelungen zur Verarbeitung von Daten im Auftrag ab. Aufgrund der besonderen Sensibilität von Personaldaten kann es nicht im Sinne der Beschäftigten oder auch des Landes sein, dass diese Daten durch Dritte bearbeitet werden. Für den DGB Baden-Württemberg muss das Land hier seine Regelungskompetenz nutzen und verhindern, dass Verarbeitung von Personalakten möglich ist.

**Zu § 84 des vorliegenden Entwurfs**

Das Wort „ausschließlich“ bedeutet im Umkehrschluss, dass automatisierte Verarbeitung personenbezogener Daten prinzipiell bei allen Entscheidungen zulässig ist. Dem kann der DGB Baden Württemberg nicht uneingeschränkt zustimmen. Es muss unter Beteiligung des jeweils zuständigen Personalrats vorab bestimmt werden, bei welchen beamtenrechtlichen Entscheidungen automatisierte Verarbeitung personenbezogener Daten angewendet werden dürfen und bei welchen nicht.

**Zu § 87 Abs. 4 des vorliegenden Entwurfs**

Im vorliegenden Entwurf ist für den DGB Baden-Württemberg nicht geregelt, wer autorisiert ist, die dort geäußerte Befürchtung zu benennen. Ein Beamter oder eine Beamtin, der/die sich z.B. im Verlauf eines Zuruhesetzungs- oder Disziplinarverfahrens wehren möchte, wird seines Grundrechts der informationellen Selbstbestimmung beraubt. Ungeachtet der Frage, ob eine solche Einschränkung nicht etwa verfassungswidrig sein könnte, kann der DGB Baden Württemberg einer solchen generellen Einschränkung der Auskunftspflicht nicht zustimmen.

**Deutscher  
Gewerkschaftsbund****Bezirk  
Baden-Württemberg**

Abschließend bedankt sich der DGB Baden-Württemberg für die Möglichkeit der Stellungnahme zum vorliegenden Gesetzesentwurf. Für eventuell notwendige weitere Erörterungen des Gesetzesentwurfs und dieser Stellungnahme steht der DGB Baden-Württemberg gerne zur Verfügung.

---

**Von:** Heinbach, Wolf  
**Gesendet:** Dieter Dr.  
Montag, 22. Januar 2018 17:12  
**An:** (MWK);  
**Cc:**  
**Betreff:** WG: Anhörung LDSG

Sehr geehrte Damen und Herren,

zu dem überlassenen Gesetzentwurf zur Neufassung des Landesdatenschutzgesetzes möchten wir Ihnen die nachfolgenden Anmerkungen des Datenschutzbeauftragten der Dualen Hochschule Baden-Württemberg zukommen lassen. Eine vertiefte Auseinandersetzung und systematische Prüfung war aufgrund der Kurzfristigkeit leider nicht möglich.

- **§ 3** (Sicherstellung des Datenschutzes) korrespondiert mit Art. 32 DSGVO und wiederholt z.T. die dort genannten Maßnahmen zur Wahrung der Interessen der betroffenen Person. In der nicht abschließenden Aufzählung wird unter Nr. 4 "die Beteiligung der oder des Datenschutzbeauftragten der jeweiligen öffentlichen Stelle" genannt. Gem. Art. 34 Abs. 1 DSGVO ist der Datenschutzbeauftragte aber ohnehin in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen einzubinden. Die Formulierung in § 3 Abs. 1 Satz 3 Nr. 4 des Entwurfs suggeriert, dass es hier eine Wahlmöglichkeit gibt und die Einbindung schon eine besondere Schutzmaßnahme darstellt. Dies ist aber nicht der Fall, da die Einbindung in jedem Fall zu erfolgen hat. Daher sollte § 3 Abs. 1 Satz 3 Nr. 4 gestrichen werden.
- **§ 13 Abs. 2** (Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken) übernimmt die Formulierung aus § 35 Abs. 2 LDSG a.F., welche dort für alle Kategorien personenbezogener Daten gilt (und nicht nur für die besonderen gem. Art. 9 DSGVO). Begrüßt wird die (zumindest für besondere Kategorien personenbezogener Daten) übernommene Pflicht zur Pseudonymisierung. Allerdings ist die Gesetzesbegründung zu § 13 Abs. 2 ("Im Übrigen gilt gemäß § 3 eine Pflicht zur Pseudonymisierung.") nicht korrekt, da Pseudonymisierung in § 3 nur als beispielhafte Maßnahme aufgezählt wird. Daher sollte die Gesetzesbegründung in diesem Punkt überarbeitet werden.
- **§ 14 Abs. 3** ("Eine dauerhafte Überwachung von Beschäftigten mit Hilfe optisch-elektronischer oder sonstiger technischer Einrichtungen zum Zwecke der Verhaltens- und Leistungskontrolle ist unzulässig.") ist mindestens unglücklich formuliert. Eine, auch nur vorübergehende Videobeobachtung oder eine anders geartete Überwachung (möglicherweise verdeckt) greift stark in die Persönlichkeitsrechte der Beschäftigten ein. Der Wortlaut des Gesetzentwurfs könnte aber so interpretiert werden, dass die Hürden für eine nicht dauerhafte oder nicht systematische Überwachung gar nicht besonders hoch sind. Auch die zugehörige Gesetzesbegründung, die praktisch nur den Wortlaut des Absatzes wiederholt, ist dabei wenig hilfreich. Es sollte klar gestellt sein, dass eine Überwachung von Beschäftigten die absolute Ausnahme sein sollte und überhaupt nur unter engen Voraussetzungen zulässig ist.
- **§ 17** (Videoüberwachung öffentlich zugänglicher Räume) lässt – wie auch in der Gesetzesbegründung ausführlich – im Gegensatz zu § 20a LDSG a.F. eine Videoüberwachung bereits bei einer abstrakten Gefahr zu. Bisher bestand dagegen die Voraussetzung, dass Tatsachen die Annahme rechtfertigen, dass eine Gefährdung vorliegt. Ebenfalls ist eine Differenzierung zwischen der reinen Beobachtung und der Aufzeichnung wie in § 20a LDSG a.F., die dem

Verantwortlichen auch Anhaltspunkte für die Prüfung der Zulässigkeit und Verhältnismäßigkeit gegeben hat, leider nicht mehr vorgesehen.

Mit freundlichen Grüßen

Dr. Wolf Dieter Heinbach  
Kanzler

Duale Hochschule Baden-Württemberg  
Baden-Wuerttemberg Cooperative State University  
**Präsidium**  
Friedrichstraße 14  
70174 Stuttgart



---

Von: (MWK)  
Gesendet: Dienstag, 9. Januar 2018 11:41  
An: poststelle <[poststelle@dhbw.de](mailto:poststelle@dhbw.de)>  
Betreff: Anhörung LDSG

Sehr geehrte Damen und Herren,

in der Anlage erhalten Sie den Gesetzentwurf mit zwei Anlagen (Entwurf und Begründung) mit der Bitte um Stellungnahme.

Mit freundlichen Grüßen

[[cid:image001.png@01D3893D.67A19750](#)]

Ministerium für Wissenschaft, Forschung  
und Kunst Baden-Württemberg  
Abteilung 2  
Königstr. 46  
70173 Stuttgart

Internet: [www.mwk.baden-wuerttemberg.de](http://www.mwk.baden-wuerttemberg.de)<<http://www.mwk.baden-wuerttemberg.de>>

**ERZDIÖZESE FREIBURG**  
Erzbischöfliches Ordinariat  
Schoferstr. 2  
79098 Freiburg

**EVANGELISCHE LANDESKIRCHE IN BADEN**  
Evangelischer Oberkirchenrat  
Blumenstraße 1 – 7  
76133 Karlsruhe

**DIÖZESE ROTTENBURG – STUTTGART**  
Bischöfliches Ordinariat  
Eugen-Bolz-Platz 1  
72108 Rottenburg

**EVANGELISCHE LANDESKIRCHE IN WÜRTEMBERG**  
Evangelischer Oberkirchenrat  
Gänsheidestraße 4  
70184 Stuttgart

---

Rottenburg, 30. Januar 2018

Ministerium für Inneres, Digitalisierung und Migration  
Baden-Württemberg

Postfach 10 34 65  
70029 Stuttgart

Per e-mail: [poststelle@im.bwl.de](mailto:poststelle@im.bwl.de)  
[Registratur2@im.bwl.de](mailto:Registratur2@im.bwl.de)

**Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts  
und sonstiger Vorschriften an die Verordnung (EU) 2016/679  
Anhörungsverfahren  
Ihr Schreiben vom 19.12.2017; Az.: 2-0557.8/1**

Sehr geehrte Frau  
sehr geehrte Damen und Herren,

zunächst dürfen wir uns im Namen der Evangelischen Landeskirche in Baden, der Evangelischen Landeskirche in Württemberg, der Erzdiözese Freiburg und der Diözese Rottenburg-Stuttgart bei Ihnen recht herzlich bedanken für Ihr freundliches Schreiben vom 19.12.2017, Az.: 2-0557.8/1, nebst den beigefügten Unterlagen, und

für die Anhörung der Kirchen im Verfahren zum Erlass eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679. Wir kommen der Bitte um Stellungnahme gerne nach.

Die Kirchen begrüßen das Gesetzesvorhaben und sehen insbesondere die Notwendigkeit, das Datenschutzrecht des Landes Baden-Württemberg an die unmittelbar geltenden Vorschriften der Verordnung (EU) 2016/679, der Datenschutz- Grundverordnung der Europäischen Union, und an das geänderte Bundesdatenschutzgesetz anzupassen. Sie bitten freilich darum, in zweifacher Hinsicht noch Ergänzungen zum bestehenden Gesetzentwurf vorzunehmen:

**1. Regelung zur Übermittlung personenbezogener Daten an Stellen der öffentlich-rechtlichen Religionsgesellschaften:**

In der geltenden Fassung des Landesdatenschutzgesetzes (LDSG) enthält § 17 unter der Überschrift Übermittlung an Stellen der öffentlich-rechtlichen Religionsgesellschaften folgende Regelung: „Für die Übermittlung personenbezogener Daten an Stellen der öffentlich-rechtlichen Religionsgesellschaften gilt § 16 Abs. 1 bis 3 entsprechend, sofern für diese Stellen ausreichende Datenschutzregelungen gelten. Die Feststellung hierüber trifft das Innenministerium.“ Im vorliegenden Entwurf zur Anpassung des allgemeinen Datenschutzrechts fehlt bislang eine entsprechende Vorschrift. Zwar regelt § 42 Bundesmeldegesetz (BMG) in Verbindung mit § 6 Baden-württembergisches Ausführungsgesetz zum Bundesmeldegesetz (BW AGBMG) eingehend die Datenübermittlungen an öffentlich-rechtliche Religionsgesellschaften, doch betrifft diese Vorschrift allein die Meldebehörden.

Personenbezogene Daten können aber etwa auch in öffentlichen Krankenhäusern, bei Notfalleinsätzen der Rettungskräfte, in Justizvollzugsanstalten und in anderen Fällen vorhanden und gespeichert sein und zugleich ein dringendes, durch das Grundrecht der Glaubens- und Religionsfreiheit (Art. 4 Abs. 1 und 2 GG) geschütztes Bedürfnis nach Einsatz eines Seelsorgers/einer Seelsorgerin in einer existenzbedrohenden Situation bestehen. Die seelsorgerliche Tätigkeit der Kirchen, die eine Weitergabe personenbezogener Daten an sie voraussetzt, ist hier nicht nur durch die Verfassung (Art. 4 Abs. 1 und 2 GG, 137 Abs. 3 S. 1 WRV/140 GG), sondern auch durch Art. 16 Vertrag des Landes Baden-Württemberg mit der Evangelischen Landeskirche in Baden und mit der Evangelischen Landeskirche in Württemberg (EvKiVBW) vom 17. Oktober 2007 (GBl. 2008, S. 1) geschützt, der im Wege paritätischer Gleichbehandlung auch den katholischen Diözesen zugute kommt. Auch bei seelsorgerlichen Maßnahmen bei der Polizei oder bei der Feuerwehr selbst kann ein dringendes Bedürfnis nach Weitergabe personenbezogener Daten an die Kirchen und deren Seelsorger/innen bestehen, das ebenfalls durch die Glaubensfreiheit, angesichts der persönlichen Situation, in der sich Angehörige der

Rettungskräfte befinden können, aber auch noch durch weitere Grundrechte geschützt sein kann. Daher bestimmt Art. 27 Abs. 4 EvKIVBW allgemein: „Die Behörden übermitteln den Kirchen die zur Erfüllung ihrer Aufgaben erforderlichen Daten. Die Kirchen schützen diese Daten nach den Bestimmungen des kirchlichen Datenschutzrechts.“

Selbst wenn sich Bedenken gegen eine Weitergabe an die öffentlich-rechtlich organisierten Religionsgemeinschaften unmittelbar auf die EU-Datenschutz-Grundverordnung (EU-DSGVO) gründen würden, so ist doch darauf hinzuweisen, dass nach deren Art. 91 die religiösen Vereinigungen und Gemeinschaften, die dessen Voraussetzungen erfüllen (was bei den großen Kirchen in Baden-Württemberg der Fall ist), dort eine Sonderstellung genießen, und dass nach Art. 17 des Vertrages über die Arbeitsweise der Europäischen Union diese den Status, den Kirchen und religiöse Vereinigungen oder Gemeinschaften in den Mitgliedstaaten nach deren Rechtsvorschriften genießen, achtet und ihn nicht beeinträchtigt. Damit sind die Vorschriften der EU-DSGVO jedenfalls im Lichte des Art. 17 AEUV zugunsten kirchlicher Betätigungsfreiheit auszulegen. Im übrigen schützt auch Art. 10 i. V. m. Art. 12 der Charta der Grundrechte der Europäischen Union das Wirken der Kirchen entsprechend ihrem religiösen Auftrag. Da nach Art. 6 des Vertrags über die Europäische Union die Charta der Grundrechte und die Verträge über die Europäische Union und deren Arbeitsweise rechtlich gleichrangig sind, kann auch dies nicht ohne Auswirkungen auf die EU-DSGVO bleiben.

Angesichts dessen erscheint im novellierten Landesdatenschutzgesetz eine Regelung zur Übermittlung personenbezogener Daten an Stellen der öffentlich-rechtlichen Religionsgesellschaften geboten. Die Kirchen bitten daher um die Aufnahme einer entsprechenden Vorschrift in den Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts an geeigneter Stelle.

**2. Regelung zur Vollstreckung von Bußgeldbescheiden der kirchlichen Datenschutzaufsicht:**

Gemäß Art. 91 Abs. 1 der EU-DSGVO haben die Kirchen die Möglichkeit, ihren eigenen Datenschutz beizubehalten, sofern dieser mit den Vorgaben der EU-DSGVO in Einklang gebracht worden ist. Sie müssen die Einhaltung der Datenschutzbestimmungen durch eine eigene, unabhängige Datenschutzaufsicht sicherstellen, die die in Kapitel VI der EU-DSGVO aufgestellten Voraussetzungen erfüllt. So hat für den Bereich der evangelischen Kirche die Synode der Evangelischen Kirche in Deutschland am 15.11.2017 ein neues Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (EKD-Datenschutzgesetz DSG EKD) beschlossen, das am 24. Mai 2018 in Kraft treten wird. Für den Bereich der katholischen Kirche hat die Vollversammlung des Verbandes der Diözesen Deutschlands am 20.11.2017 ein neues Gesetz

über den Datenschutz (KDG) beschlossen, das allerdings zu seiner Wirksamkeit in den einzelnen Diözesen noch der Inkraftsetzung durch den jeweiligen Diözesanbischof bedarf. Die Umsetzung wird in den beiden (Erz-)Diözesen des Landes Baden-Württemberg, der Erzdiözese Freiburg und der Diözese Rottenburg-Stuttgart – ebenfalls spätestens bis zum 24. Mai 2018 – erfolgt sein.

Zur Herstellung einer vollständigen Gleichwertigkeit des kirchlichen mit dem staatlichen Datenschutz wird durch § 45 DSG EKD bzw. § 51 (katholisches) KDG insbesondere auch die Verhängung von Geldbußen durch die jeweils zuständige Datenschutzaufsicht eingeführt und mit § 51 Abs. VII KDG eine Regelung zur Vollstreckbarkeit aufgenommen. Die Kirchen haben aufgrund ihres Körperschaftsstatus jedoch nur das Recht, Bußgeldbescheide zu erlassen, können diese jedoch – wegen des staatlichen Gewaltmonopols – nicht selbst vollstrecken; dies ist nur möglich, wenn ihnen staatliche Stellen hierzu Vollstreckungshilfe gewähren.

Zwar können Geldbußen der kirchlichen Datenschutzaufsicht – allerdings sehr zeitaufwändig und umständlich – auf dem Zivilrechtsweg mittels einer Zahlungsklage und einer nachfolgenden Zwangsvollstreckung durchgesetzt werden. Im Interesse eines effektiven und gleichwertigen Datenschutzes von Staat und Kirchen erscheint es daher wünschenswert, im neuen LDSG von Baden-Württemberg eine Vorschrift aufzunehmen, die der kirchlichen Datenschutzaufsicht auf Antrag die Möglichkeit gibt, die von ihr verhängten Geldbußen unmittelbar im Verwaltungszwangsverfahren durch staatliche Behörden im Wege der Amts- und Vollstreckungshilfe beizutreiben zu lassen. Will eine Kirche aufgrund ihres religiösen Selbstverständnisses oder ihres Kirchenrechts diesen Weg nicht wählen, so bleibt ihr die Möglichkeit unbenommen, die Bußgeldforderungen auf dem Zivilrechtsweg durchzusetzen.

Vergleichbare Regelungen existieren aus demselben Grund bereits im Kirchensteuerrecht (vgl. § 15 KiStG BW), bei der Vollstreckung kirchlicher Gebühren (Art. 27 Abs. 3 EvKiVBW), im Disziplinarrecht (vgl. § 51 Abs. 2 Württ. Kirchengesetz), sowie im Friedhofsgebührenrecht mehrerer Bundesländer (vgl. bspw. § 4 Abs. 3 Bestattungsgesetz NRW). Mit der Einführung einer solchen Regelung auch für Bußgeldbescheide der kirchlichen Datenschutzaufsicht würde somit lediglich ein bereits bekanntes Regelungskonzept für ein weiteres Rechtsgebiet übernommen. Nach dem Kenntnisstand der Kirchen besteht auch in anderen Bundesländern, z. B. im Saarland und in Nordrhein-Westfalen Offenheit für dieses Anliegen der Kirchen.

Eine entsprechende Bestimmung im LDSG von Baden-Württemberg könnte demnach in etwa folgendermaßen aussehen: „Wendet eine Kirche oder eine

religiöse Vereinigung oder Gemeinschaft umfassende Regeln zum Datenschutz im Sinne des Art. 91 der Verordnung (EU) 2016/679 an, so kann auf Antrag der zuständigen Oberkirchenbehörde das Ministerium für Inneres, Digitalisierung und Migration die Vollstreckung von Bußgeldern, die auf der Grundlage dieser Regeln von der zuständigen kirchlichen Stelle verhängt wurden, den unteren Verwaltungsbehörden übertragen."

Die Kirchen wären sehr dankbar, wenn seitens des Landes Baden-Württemberg Bereitschaft bestünde, die beiden von ihnen angeregten Ergänzungen im Rahmen der Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679 in das novellierte Landesdatenschutzgesetz aufzunehmen.

Die Kirchen bedanken sich nochmals ausdrücklich für die Möglichkeit zur Stellungnahme im Rahmen der beabsichtigten Rechtsänderungen und für Ihr Interesse an dieser. Für Rückfragen stehen wir selbstverständlich gerne zur Verfügung und verbleiben

mit freundlichen Grüßen



Dr. Clemens Stroppel  
Generalvikar



## Baden-Württemberg

MINISTERIUM FÜR INNERES, DIGITALISIERUNG UND MIGRATION  
HAUPTPERSONALRAT

Innenministerium • Pf. 10 34 65 • 70029 Stuttgart

Abteilung 2  
im Hause

Datum 29. Januar 2018

Name Tilly Bair

Aktenzeichen HPR-zu 0557.8/1028  
(Bitte bei Antwort angeben)

—  Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679, Schreiben vom 19.12.2017, Az.: 2-0557.8/1

—  
Sehr geehrter Herr  
sehr geehrte Frau

der Hauptpersonalrat (HPR) hat die o.g. Vorlage in seiner Sitzung am 10. Januar 2018 beraten und die nachfolgende Stellungnahme beschlossen.

Für den Hauptpersonalrat ist es nicht nachvollziehbar, warum im Rahmen der Anpassung des Landesdatenschutzgesetzes – LDSG der Beschäftigtendatenschutz nicht mit aufgenommen werden soll. Zumal in der alten Fassung des Landesdatenschutzgesetzes – LDSG z.B. in den §§ 21- 24 Regelungen zum Beschäftigtendatenschutz enthalten sind.

Aus Sicht des HPR ist eine gesetzliche Regelung für den Beschäftigtendatenschutz wichtig, richtig und sinnvoll.

Dieser Punkt ist dem HPR auch deshalb wichtig, weil im aktuellen Leitfaden des Datenschutzbeauftragten der Beschäftigtendatenschutz keine Erwähnung findet.

- 2 -

Zur Erleichterung der Lesbarkeit von Gesetzesänderungen dürfen wir Sie bitten, zukünftig eine Synopse mit der Gegenüberstellung alte Regelung / neue Regelung als Vorlage zu verwenden. Dies erleichtert die Lesbarkeit der Dokumente.

Mit freundlichen Grüßen

gez.  
Tilly Bair  
Vorsitzende



## Baden-Württemberg

HAUPTPERSONALRAT FÜR GRUND-, HAUPT-, WERKREAL-, REAL- UND GEMEINSCHAFTSSCHULEN SOWIE AN  
SONDERPÄDAGOGISCHEN BILDUNGS- UND BERATUNGSZENTREN  
BEIM MINISTERIUM FÜR KULTUS, JUGEND UND SPORT

Hauptpersonalrat GHWRGS beim Kultusministerium  
Baden-Württemberg • Postfach 10 34 42 • 70029 Stuttgart

Ministerium für Inneres  
Digitalisierung und Migration  
Baden-Württemberg  
Postfach 10 34 65  
70029 Stuttgart

Stuttgart 23.01.2018

Name Alfred König  
Gebäude Thouretstr. 2  
Aktenzeichen A-1424/EDV/LDSG/Kö  
(Bitte bei Antwort angeben)

ARGE-HPR-Vors.

Postfach 103465  
70029 Stuttgart

### Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts an die Verordnung (EU) 2016/679

Schreiben vom 19. Dezember 2017, 2-0557.8/1

Sehr geehrter Herr  
sehr geehrte Frau  
sehr geehrte Frau

Der Hauptpersonalrat GHWRGS gibt zum oben angeführten Entwurf folgende Stellungnahme ab:

#### **Zu § 5 Absatz 1 Ziffer 1**

**Der Hauptpersonalrat GHWRGS schlägt vor, die Formulierung „oder einer Gefahr“ zu ersetzen durch „oder einer unmittelbar drohenden Gefahr“.**

Diese eingeschränkte Formulierung ist aus der Sicht des Hauptpersonalrats GHWRGS unabdingbar um die Schwelle für eine mögliche Datenverarbeitung zu anderen Zwecken

- 2 -

im Sinne der Grundprinzipien nach Artikel 5 der EU Datenschutzgrundverordnung zu erhöhen.

#### **Zu § 6**

**Der Hauptpersonalrat GHWRGS ist der Auffassung, dass grundsätzlich die übermittelnde öffentliche Stelle die Zulässigkeit der Übermittlung prüfen muss.**

Es muss bspw. aus der Sicht des Hauptpersonalrats GHWRGS die übermittelnde öffentliche Stelle prüfen, ob bei der Übermittlung von Bewerbungsdaten das Einverständnis nach § 14 Absatz 2 Landesdatenschutzgesetz (Entwurf) vorliegt. Es ist abenteuerlich anzunehmen, dass die anfordernde Stelle dieses Einverständnis einholt.

#### **Zu § 7**

**Der Begriff „örtlich zuständige öffentliche Stelle“ ist an keiner Stelle definiert.**

Was ist unter diesem Begriff zu verstehen? Handelt es sich hier um Verantwortliche, oder was ist mit diesem Begriff gemeint? Dieser Begriff sollte definiert werden.

#### **Zu § 14**

**Es sollte aufgenommen werden, dass Daten von Bewerberinnen und Bewerbern, bei denen ein Beschäftigungsverhältnis nicht begründet wurde, spätestens nach Ablauf eines Jahres zu löschen sind, es sei denn, dass die betroffene Person eingewilligt hat oder die Daten wegen eines anhängigen Rechtsstreites erforderlich sind (vergleiche derzeitiges Landesdatenschutzgesetz).**

Dem Hauptpersonalrat GHWRGS ist aufgefallen, dass in § 14 des Entwurfs für Bewerbungen keine Löschvorschriften mehr enthalten sind.

#### **Zu § 14 Absatz 6 des Entwurfs**

**Der Hauptpersonalrat GHWRGS beantragt die Streichung des Begriffs „dauerhafte“ oder zumindest der deutlichen zeitlichen Begrenzung.**

Die Eingriffsintensität in das Grundrecht auf informationelle Selbstbestimmung durch die Verwendung von optisch-elektronischen Verfahren ist äußerst groß und schon deshalb

- 3 -

darf auch aus der Sicht des Hauptpersonalrats GHWRGS damit keine Leistungs- und Verhaltenskontrolle erfolgen. Im Übrigen sei angemerkt, dass auf Seite 70 des Koalitionsvertrags festgehalten ist, dass der Beschäftigtendatenschutz verbessert werden soll. Nach diesem Entwurf wäre eine temporäre Überwachung zulässig, die nach dem derzeit geltenden Landesdatenschutzgesetz nicht zulässig wäre. In sofern handelt es sich hierbei eindeutig um eine Verschlechterung des Beschäftigtendatenschutzes. Im Übrigen ist unbestimmt, wann es sich um eine dauerhafte und wann es sich um eine temporäre Überwachung handelt.

**Zu § 17 des Entwurfs**

**Der bisherige § 20 a des alten Landesdatenschutzgesetzes hat viel präziser formuliert, wann eine Videoüberwachung zulässig war. Die Regelungen in § 17 Absatz 1 sind letztendlich nicht konkret bestimmt.**

Sinnvoller wäre aus der Sicht des Hauptpersonalrats GHWRGS eine Regelung, wenn durch Tatsachen die Annahme gerechtfertigt wäre, dass der Schutz von Leben, Gesundheit oder Freiheit von Personen oder der Schutz von öffentlichen Einrichtungen, Verkehrsmitteln, Gebäuden, Kulturgütern etc. gefährdet ist.

**Zu Artikel 17, § 87 Absatz 3**

**Der Hauptpersonalrat GHWRGS beantragt die Aufnahme des Wortes "kostenfrei" vor dem Wort Abschriften**

Die Möglichkeit, dass von Beschäftigten für Auszüge aus ihren Personalaktendaten Gebühren verlangt werden könnten, muss ausgeschlossen werden.

**Zu Artikel 17, § 87 Absatz 4**

**Der Hauptpersonalrat GHWRGS beantragt die Streichung der Ziffer 1.**

Aus der Sicht des Hauptpersonalrats GHWRGS kann das Auskunftsrecht eines betroffenen Patienten über seinen Gesundheitszustand nicht beschnitten werden. Dies gilt auch für im Rahmen eines Dienst- bzw. Arbeitsverhältnisses erstellte medizinische Gutachten. Im Übrigen liegt es mit Sicherheit nicht in der Entscheidung einer personalverwaltenden Stelle festzustellen, wann zu befürchten ist, dass die betroffene Beamtin oder

- 4 -

der betroffene Beamte bei Kenntnis des Befundes "weiteren Schaden an der Gesundheit nimmt".

Der Hauptpersonalrat GHWRGS bittet um die Berücksichtigung seiner Vorschläge.

Mit freundlichen Grüßen

.

Alfred König

Vorsitzender

**HAUPTSCHWERBEHINDERTENVERTRETUNG DER POLIZEI  
BEIM MINISTERIUM FÜR INNERES, DIGITALISIERUNG  
UND MIGRATION BADEN-WÜRTTEMBERG**

Landeskriminalamt • Postfach 500 729 • 70337 Stuttgart  
E-Mail: [hsbv@polizei.bwl.de](mailto:hsbv@polizei.bwl.de)  
FAX: 0711/5401-2075

Ministerium für Inneres, Digitalisierung und  
Migration Baden-Württemberg  
Abteilung 2  
Willy-Brandt-Straße 41  
70173 Stuttgart

Datum 18.01.2018  
Name Karpf, Michael  
Aktenzeichen 5114-01/18  
(Bitte bei Antwort angeben)

Per Mail an: [Registatur2@im.bwl.de](mailto:Registatur2@im.bwl.de)

---

 **STELLUNGNAHME**

Ihre E-Mail mit Anlagen vom 22.12.2017, Az.: 2-0557.8/1  
Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und  
sonstiger Vorschriften an die Verordnung (EU) 2016/679

Sehr geehrte Damen und Herren,

die Hauptschwerbehindertenvertretung der Polizei dankt für die Übersendung des o.g.  
Gesetzesentwurfs vom 14.12.2017 zur Anpassung des Datenschutzrechts an die EU-  
DSGVO mit der Möglichkeit zur Stellungnahme. Folgende Anmerkung zur Anpassung des  
Personalaktenrechts im Landesbeamtengesetz (Artikel 17) wird vorgetragen:

**Artikel 17 Nr. 6** regelt u.a. die Neufassung von § 87 LBG. Gemäß Absatz 4 Nr. 1 sollen  
Feststellungen über den Gesundheitszustand nicht der Auskunft unterliegen, wenn „zu  
befürchten ist, dass die betroffene Beamtin oder der betroffene Beamte bei Kenntnis des  
Befunds weiteren Schaden an der Gesundheit nimmt“.

Eine solche Einschränkung des Informationsinteresses mag grundsätzlich ihre Berechti-  
gung haben. Allerdings ist die einschränkende Bedingung „wenn zu befürchten ist“ derart  
abstrakt formuliert, dass bei der Feststellung der Voraussetzungen durch die personal-  
verwaltende Stelle sehr subjektive Aspekte den Ausschlag geben könnten. Dies würde der  
Intention der Regelung nach einer schonenden Interessensabwägung nicht gerecht wer-  
den. In der Gesetzesbegründung wird zutreffend herausgestellt, dass ausschließende  
Gründe von hohem Gewicht sein und im Sinne der Fürsorgepflicht des Dienstherrn dem  
konkreten Gesundheitsschutz dienen müssen. Diesem Aspekt Rechnung tragend, wird  
empfohlen, anstelle „wenn zu befürchten ist“ als einschränkende Bedingung „wenn durch  
Tatsachen begründete Besorgnis besteht“ zu formulieren.

Mit freundlichen Grüßen

gez. Dr. Michael Karpf  
Hauptvertrauensperson



Hochschulen für Angewandte Wissenschaften Baden-Württemberg e.V.  
HAW BW e.V. · Hospitalstraße 8 · 70174 Stuttgart

Ministerium für Inneres, Digitalisierung und  
Migration Baden-Württemberg  
Postfach 10 34 65  
70029 Stuttgart

#### Der Vorsitzende

Unser Zeichen: 3010/EB  
Datum: 30. Januar 2018

*nachrichtlich:*

*Ministerium für Wissenschaft, Forschung und Kunst Baden-Württemberg*

#### **Anhörung zum Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679; AZ: 2-0557.8/1**

gemeinsame Stellungnahme für die staatlichen Hochschulen für Angewandte Wissenschaften im Bereich des MWK

Sehr geehrte Damen und Herren,

vielen Dank für die Einladung zur Abgabe einer Stellungnahme zum Entwurf des Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679, die der HAW BW e.V. als zentrale Interessenvertretung der 3 Hochschulen für Angewandte Wissenschaften in kirchlicher Trägerschaft und der 21 staatlichen Hochschulen im Geschäftsbereich des MWK gerne nutzt.

Die Hochschulen für Angewandte Wissenschaften begrüßen die Intention des Landesgesetzgebers, im Rahmen der durch das Europarecht vorgesehenen Spielräume angemessene Erweiterungen zu Gunsten der Forschung im Datenschutzrecht zu implementieren. Sie nehmen ebenso wahr, dass der Gesetzgeber an einigen Stellen die Möglichkeit zur Abweichung von Vorgaben der EU-DSGVO genutzt hat, um weiteren Bürokratieaufbau in Behörden aufgrund des Datenschutzes zu bremsen. Gleichwohl bitten die Hochschulen den Gesetzgeber darum, zu analysieren, ob die EU-DSGVO weitere Spielräume zur Vereinfachung und Entbürokratisierung des Datenschutzrechts bietet, und diese zu nutzen. Zudem bitten sie den Gesetzgeber schon jetzt vorsorglich darum, im Verlauf des Gesetzgebungsverfahrens keine zusätzlichen Verschärfungen und Bürokratisierungen zu verankern.

Die Hochschulen weisen darauf hin, dass sie bislang mit Ausnahme von zwei zentralen E13-Stellen im Jahr 2016, die zudem zusätzlich auch die Informationssicherheit abdecken sollen, keinerlei Ressourcen vom Land erhalten haben, um die massiven Änderungen und den durch die EU-DSGVO geforderten Systemwechsel zu bewältigen. Datenschutz und IT-Sicherheit gehen schon heute zu Lasten der knappen Ausstattung der Hochschulen für ihre Kernaufgaben in Lehre, Forschung und Studium. Mangels entsprechenden Personalstellen sind die Hochschulen gezwungen, Professoren von ihren Kernaufgaben

HAW BW e.V.  
Hochschulen für  
Angewandte Wissenschaften  
Baden-Württemberg e.V.

hochschulen-bw.de

Kontakt  
Hospitalstraße 8  
70174 Stuttgart

Fon 0711 995281-61  
Fax 0711 995281-66  
info@haw-bw.de

Vorstand  
Prof. Dr. Dr. h.c. Bastian Kaiser (Vorsitzender)  
Prof. Dr.-Ing. Dr. h.c. Winfried Lieber  
Prof. Dr. Gerhard Schneider  
Prof. Dr. Hendrik Brumme

Geschäftsführer  
Benjamin Peschke M.A.

Bankverbindung  
IBAN DE02 6005 0101 0004 5880 23  
BIC SOLADEST600  
BW-Bank Stuttgart

Steuernummer 99015/31755  
Vereinsregister 721177  
Amtsgericht Stuttgart

teilweise abzuziehen und sie fachfremd damit zu betrauen. Jede neue zusätzliche Aufgabe und jeder neue Prozess, der implementiert werden muss, führt zu einer Verschlechterung.

Vor diesem Hintergrund regen die HAW fachlich-juristisch an, auf Ebene der Landesgesetzgebung folgende Vereinfachungen und Klarstellungen zu prüfen und ggf. umzusetzen:

• **§ 9 LDSG-E [Beschränkung des Auskunftsrechts]**

Die Hochschulen begrüßen, dass der Gesetzgeber in Absatz 2 ausdrücklich aufgenommen hat, dass öffentliche Stellen, die eine große Menge von Daten verarbeiten, von Antragstellern verlangen können, dass sie ihr Auskunftsbegehren präzisieren, sowie, dass es ermöglicht wird, die Auskunft zu verweigern, wenn diese einen unzumutbaren Aufwand auslösen würde. Wünschenswert wäre, dass der Gesetzgeber die unbestimmten Rechtsbegriffe ‚große Menge von Daten‘ und ‚unzumutbar‘ in der Gesetzesbegründung erläutern würde, sodass die Rechtspraxis ausreichende Anhaltspunkte für die Auslegung der Begriffe hat.

Überdies wird angeregt, zu prüfen, ob eine gebührenrechtliche Grundlage im Landesrecht gebraucht wird, um in Fällen, in denen Antragsteller wiederholte Auskunftersuchen stellen, Gebühren auf Verwaltungskostenbasis zu erheben, so wie dies von Art. 15 Abs. 3 EU-DSGVO vorgesehen ist.

• **§ 13 LDSG-E [Privilegierung für die Wissenschaft]**

Die Hochschulen begrüßen sehr, dass der Gesetzgeber von der Möglichkeit, die Wissenschaft über Art. 5 EU-DSGVO hinaus zu privilegieren, Gebrauch machen wird. Um die Privilegierung noch deutlicher auszugestalten und gleichzeitig Auslegungsproblemen vorzubeugen, werden folgende Änderungen in § 13 LDSG-E angeregt:

*1. Keine Eingrenzung des § 13 auf „wissenschaftliche oder historische Forschungszwecke“*

Überraschenderweise privilegiert – was möglicherweise auf eine schlechte Übersetzung der EU-DSGVO zurückzuführen ist – das LDSG-E nur „wissenschaftliche oder historische Forschungszwecke“. Es ist unklar, ob der Gesetzgeber damit etwas bezweckt, nämlich eine Differenzierung zwischen „wissenschaftlicher Forschung und nicht-wissenschaftlicher Forschung“, und was er in diesem Fall unter „nicht-wissenschaftlicher Forschung“ versteht. Im allgemeinen Sprach- und Rechtsgebrauch ist Forschung eine Ausprägung von Wissenschaft, neben der Lehre (vgl. Art. 5 Abs. 3 S. 1 GG). Es wird daher angeregt, in § 13 stets ‚Forschungszwecke‘ in Bezug zu nehmen. Diese sind per se wissenschaftlich – je nach Disziplin auch historisch.

*2. Klare Trennung von Verarbeitung einerseits und Veröffentlichung andererseits*

Zur Vorbeugung von Missverständnissen erscheint eine klare Trennung der Inhalte von § 13 Abs. 1 und 2 einerseits (Verarbeitung) und Abs. 3 andererseits (Veröffentlichung) angezeigt. Denn es werden ganz unterschiedliche Fragen geregelt: in § 13 Abs. 1 und 2 geht es um die Verarbeitung besonderer Kategorien personenbezogener Daten zu Forschungszwecken und zu statistischen Zwecken, während § 13 Abs. 3 die Veröffentlichung von (allgemein) personenbezogenen Daten zur Darstellung von Forschungsergebnissen ohne Einwilligung regelt. Hierzu sollten die Regelungen in unterschiedlichen Paragraphen verankert werden, die wie folgt bezeichnet sind:

§ ... Verarbeitung personenbezogener Daten zu Forschungszwecken und zu statistischen Zwecken

§ ... Veröffentlichung personenbezogener Daten zur Darstellung von Forschungsergebnissen

*3. Aufnahme einer forschungsspezifischen Generalklausel*

Zur Begründung von Rechtssicherheit in Fällen, in denen die subsidiäre Vorschrift in § 4 nicht ausreicht, ist die Aufnahme einer forschungsspezifischen Generalklausel in § 13 dringend erforderlich. Es gibt Forschungsprojekte, in denen eine größere Menge von personenbezogenen Daten verarbeitet wird. Hierzu sollte § 13 einen neuen Absatz 1 erhalten, der vergleichbar der Regelung im bayrischen Gesetzesentwurf lautet: „Für Zwecke der Forschung dürfen im erforderlichen Umfang personenbezogene Daten erhoben und

verarbeitet werden.“ Die bislang im Entwurf vorgesehenen Absätze 1 und 2, die sich ausschließlich auf besondere Kategorien personenbezogener Daten beziehen und für deren Verarbeitung sehr strenge Voraussetzungen aufstellen, würden so zu Absätzen 2 und 3.

#### 4. Verarbeitung von „besonderen Kategorien personenbezogener Daten“

Der Gesetzesentwurf schränkt in § 13 Absätze 1 und 2 die Verarbeitung von „besonderen Kategorien personenbezogener Daten“ zu Forschungszwecken dahingehend ein, dass dies nur zulässig ist, wenn die Interessen der öffentlichen Stelle die schutzwürdigen Belange **erheblich** überwiegen. Eine solche Beschränkung ist weder nach den Vorgaben der EU-DSGVO erforderlich, noch haben andere deutsche Gesetzgeber solche Einschränkungen implementiert. Um einerseits Wettbewerbsnachteile für die Forschung der baden-württembergischen Hochschulen zu vermeiden, und andererseits die bundesländerübergreifenden Forschungsprojekte nicht zu erschweren durch unterschiedliche rechtliche Voraussetzungen, wird darum gebeten, dass Wort „erheblich“ aus § 13 Abs. 1 LDSG-E zu streichen.

#### 5. Praktikable Lösung für Fälle, in denen die Anonymisierung nur mit unverhältnismäßig hohem Aufwand möglich ist

Der Gesetzesentwurf sieht vor, dass besondere Kategorien personenbezogener Daten zu anonymisieren sind, sobald dies nach dem Forschungs- oder Statistikzweck möglich ist. Es wird angeregt, zu ermöglichen, dass alternative Lösungen des Datenschutzes eröffnet werden, wo eine Anonymisierung nur mit unverhältnismäßig großem Aufwand möglich wäre (z. B. verschlüsselte Aufbewahrung unter Verschluss). Beispielsweise in Forschungsprojekten zur Sicherheit im Straßenverkehr, die mit videogestützten Methoden durchgeführt werden, ist die Anonymisierung nur mit einem äußerst großen Aufwand möglich, da ggf. viele Stunden Videomaterial „verpixelt“ werden müssen, auch wenn diese nur einem sehr begrenzten Personenkreis zugänglich gemacht werden.

#### • Ausweitung der wissenschaftlichen Publikationsmöglichkeiten

Die derzeit unter § 13 Abs. 3 des Entwurfs vorgesehene Regelung für Forschung betreibende öffentliche Stellen, personenbezogene Daten ohne Einwilligung zu veröffentlichen, ist zu eng formuliert. Es gibt neben zeitgeschichtlichen Forschungsergebnissen auch andere Forschungsergebnisse, bei denen unerlässlich ist, personenbezogene Daten zu veröffentlichen, obwohl keine Einwilligung dafür vorliegt. Es wird daher angeregt, die Vorschrift unter Berücksichtigung der vielfältigen Bedürfnisse der Wissenschaft wie folgt zu formulieren:

<p>Gesetzesentwurf IM:          „Die wissenschaftliche Forschung betreibenden öffentlichen Stellen dürfen personenbezogene Daten außer bei Einwilligung nur veröffentlichen, soweit dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist.“</p>	<p>Vorschlag HAW:          „Die Forschung betreibenden öffentlichen Stellen dürfen personenbezogene Daten außer bei Einwilligung nur veröffentlichen, soweit dies für die Darstellung von Forschungsergebnissen unerlässlich ist.“</p>
--	--

#### • § 14 Abs. 4 [Datenverarbeitung bei Straftatverdacht]

Es wird begrüßt, dass der Gesetzesentwurf nunmehr eine ausdrückliche Regelung dafür enthält, nach Interessenabwägung personenbezogene Daten von Beschäftigten, die im Verdacht stehen, eine Straftat im Beschäftigungsverhältnis begangen zu haben, zu verarbeiten. Es wird jedoch angeregt, zu prüfen, ob es nicht korrekter wäre, statt von „der betroffenen Person“ zu formulieren „eine der betroffenen Personen“, da sich der Verdacht in vielen Fällen nicht gegen einen bestimmten Beschäftigten richten wird, sondern gegen mehrere Beschäftigte in einem bestimmten Bereich.

**• § 14 Abs. 6 [Dauerhafte Überwachung von Beschäftigten mit technischen Einrichtungen]**

§ 14 Abs. 6 trägt in der vorgeschlagenen Form nicht zu einer für die Praxis hilfreichen Klarstellung und Grenzziehung bei. Es wird daher angeregt, die Vorschrift entweder so zu überarbeiten, dass sie für die Arbeit der Behörden und Personalvertretungen klare Leitlinien gibt, oder sie zu streichen. Wünschenswert wäre eine Aussage des Gesetzgebers, dass elektronische Systeme zur effizienten Organisation der Arbeit (z.B. Ticketing-Systeme) eingesetzt werden dürfen, wobei dabei anfallende personenbezogene Arbeitnehmerdaten einer strengen Zweckbindung unterliegen sollten.

**• § 14 Abs. 8 [Zuverlässigkeitsüberprüfung]**

Es wird darum gebeten, die neue Regelung zur Zuverlässigkeitsüberprüfung bei Personen, die in sicherheitsrelevante Bereiche gelangen wollen, zu entbürokratisieren, indem das Erfordernis der Einwilligung gestrichen wird, zumal eine „Einwilligung“ aufgrund der Drucksituation häufig gar nicht rechtssicher erteilt werden kann.

**• Wünschenswerte Erweiterungen und Ergänzungen des Gesetzesentwurfs**

- Klarstellung, dass der Grundsatz der Datenportabilität in Art. 20 EU-DSGVO im hoheitlichen Bereich der Hochschulen, insbesondere bei Studium, Lehre und Prüfungen, nicht gilt, da die Hochschulen hier in Ausübung öffentlicher Gewalt handeln.
- Aufnahme des Datengeheimnisses, das bislang ausdrücklich im LDSG geregelt war, was den Vorteil hatte, dass aufwändige individuelle Verpflichtungen der Beschäftigten auf das Datengeheimnis aufgrund der gesetzlichen Bestimmungen nicht erforderlich waren.
- Konkretisierung der Rechtsstellung des behördlichen Datenschutzbeauftragten, z. B. durch Konkretisierung des Aufgabenbereichs und durch Verankerung eines Benachteiligungsverbots.
- Überprüfung, ob es weiterhin ermöglicht werden kann, dass eine übergeordnete Fachaufsichtsbehörde für die nachgeordneten Behörden eine Auftragsdatenverarbeitungsvereinbarung mit einer zuverlässigen dritten Stelle abschließen kann (vgl. § 7 Abs. 2 S. 5 LDSG); in manchen Fällen ist dies eine effiziente Lösung. Außerdem sollte geprüft werden, ob es nicht wie bisher ermöglicht werden kann, Erleichterungen vorzusehen, sofern eine öffentliche Stelle für eine andere öffentliche Stelle Auftragsdatenverarbeitungsleistungen erbringt (vgl. § 7 Abs. 3 LDSG).

Bei Rückfragen stehen die Hochschulen für Angewandte Wissenschaften Ihnen gerne zur Verfügung.

Freundliche Grüße



Professor Dr. Dr. h.c. Bastian Kaiser



Ingenieurkammer Baden-Württemberg

**Daniel Sander**  
HauptgeschäftsführerIngenieurkammer Baden-Württemberg  
Körperschaft des öffentlichen RechtsZellerstraße 26, 70180 Stuttgart  
www.ingbw.de

Ingenieurkammer BW, Postfach 102412, 70020 Stuttgart

Ministerium für Inneres, Digitalisierung  
und Migration Baden-Württemberg  
Postfach 10 34 65 •  
70029 Stuttgart**per Mail** versendet an:  
Registatur2@im.bwl.de

Stuttgart, 31. Januar 2018

**Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679**Ihr Schreiben vom 19. Dezember 2017  
AZ: 2-0557.8/1

Sehr geehrter Herr

zunächst möchten wir uns für die Anhörung und damit verbundene Möglichkeit der Stellungnahme zum Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016-679 bedanken.

Im Folgenden möchten wir zu dem geplanten Entwurf Stellung nehmen:

## 1. § 4 LDSG („Zulässigkeit der Verarbeitung personenbezogener Daten“)

Gemäß § 4 LDSG gilt: „Die Verarbeitung personenbezogener Daten ist unbeschadet sonstiger Bestimmungen zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der öffentlichen Stelle liegenden Aufgabe oder in Ausübung öffentlicher Gewalt, die der öffentlichen Stelle übertragen wurde, erforderlich ist.“ Hierunter hoffen wir fällt beispielsweise die Tätigkeit unseres Schlichtungsausschusses, aber ebenso die als Kammer-service angebotene juristische Rechtsberatung. Eventuell lässt sich dies in den Anmerkungen zum Gesetz noch exakter ausführen.

## 2. § 11 LDSG („Beschränkung der Benachrichtigungspflicht“)

In § 11 LDSG werden einige Fallvariationen bei welcher eine Beschränkung der Benachrichtigungspflicht möglich ist, dargestellt.

Wir würden ergänzend empfehlen, § 11 LDSG dahingehend zu erweitern, dass auch aus Gründen der Unverhältnismäßigkeit (sei es in Bezug auf den damit verbundenen Aufwand, als auch in Bezug auf die Priorität der Angelegenheit) die öffentliche Stelle von einer Benachrichtigung der betroffenen Person absehen kann.

Seite 1 von 2

Präsidium:  
Prof. Dr.-Ing. Stephan Engelsmann (Präsident)  
Dr.-Ing. Klaus Wittemann (1. Vizepräsident)  
Dipl.-Ing. (FH) Helmut Zenker (2. Vizepräsident)  
Dipl.-Ing. Guido Hils (Schatzmeister)Beisitzer im Vorstand:  
Dr.-Ing. Dr. techn. Andreas Hutarew  
Dipl.-Ing. Lilly Kunz-Wedler  
Prof. Dr.-Ing. Klaus-Peter Meßmer  
Dipl.-Ing. Andreas NußbaumHauptgeschäftsführer: Daniel Sander M.A.  
Bankverbindung: BW Bank Stuttgart  
SWIFT-BIC: SOLADEST600  
IBAN: DE54600501017871515813



Seite 2 von 2 zum Schreiben vom 31. Januar 2018

Ingenieurkammer Baden-Württemberg

### 3. Einschränkungen des Art. 21 EU DSGVO („Widerspruchsrecht“)

Wir regen an, dass in LDSG ebenfalls eine Regelung noch aufgeführt wird, die für die Institutionen, die unter das LDSG fallen, Ausnahmen zu Artikel 21 EU DSGVO vorsehen. Auch hier geht es darum, dass zu überprüfen ist, ob die vom LDSG umfassten Institutionen ihre Tätigkeiten ordnungsgemäß ausüben können, wenn sie vollständig den Pflichten aus Artikel 21 EU DSGVO ausgesetzt sind.

Aus unserer Sicht ist es notwendig, dass es ähnliche Ausnahmen im Sinne des § 4, 5 LDSG auch für das Widerspruchsrecht gibt.

### 4. Fehlende Ausnahmeregelung zu Art. 18 EU DSGVO („Recht auf Einschränkung der Verarbeitung“).

Art. 18 Abs. 1 i. V. m. Abs. 2 EU DSGVO gibt der betroffenen Person das Recht auf Einschränkung der Verarbeitung ihrer persönlichen Daten.

Im vorliegenden Entwurf des LDSG findet sich aus unserer Sicht keine Regelung, die den betroffenen Institutionen die Möglichkeit einräumt, Ausnahmen für die Anwendung des Art. 18 EU DSGVO vorzunehmen.

Wir regen aus diesem Grund an, dass in einem etwaigen neuen § 10a LDSG Beschränkungen auf das Recht auf Einschränkung der Verarbeitung vorgenommen werden. Der Wortlaut könnte sich an den §§ 4, 5 LDSG orientieren.

Abschließend möchten wir betonen, dass wir es äußerst begrüßen, dass der Landesgesetzgeber von der Möglichkeit der Verwendung der Öffnungsklauseln Gebrauch macht. Insbesondere die Regelung des § 27 LDSG begrüßen wir sehr und halten diese für äußerst gelungen.

Mit freundlichen Grüßen

Daniel Sander M.A.



Präsidium:  
Prof. Dr.-Ing. Stephan Engelsmann (Präsident)  
Dr.-Ing. Klaus Wittemann (1. Vizepräsident)  
Dipl.-Ing. (FH) Helmut Zenker (2. Vizepräsident)  
Dipl.-Ing. Guido Hills (Schatzmeister)

Beisitzer im Vorstand:  
Dr.-Ing. Dr. techn. Andreas Hutarew  
Dipl.-Ing. Lilly Kunz-Wädler  
Prof. Dr.-Ing. Klaus-Peter Meßmer  
Dipl.-Ing. Andreas Nußbaum

Hauptgeschäftsführer: Daniel Sander M.A.  
Bankverbindung: BW Bank Stuttgart  
SWIFT-BIC: SOLADEST000  
IBAN: DE54600501017871515813



Karlsruher Institut für Technologie

KIT | Präsidium | Postfach 6980 | 76049 Karlsruhe

Ministerium für Wissenschaft, Forschung  
und Kunst Baden-Württemberg (MWK)  
Königstraße 46  
70173 Stuttgart

Per E-Mail:

**Vizepräsidentin für  
Personal und Recht**  
Christine von Vangerow

Kaiserstraße 12  
76131 Karlsruhe

Datum: 25.01.2018



## **Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679**

Sehr geehrte Frau  
sehr geehrter Frau  
sehr geehrte Damen und Herren,

das Karlsruher Institut für Technologie (KIT) nimmt zum Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679 (LDSG-E) wie folgt Stellung:

### **1) § 14 Datenverarbeitung bei Dienst- und Arbeitsverhältnissen, Zuverlässigkeitsüberprüfung**

- a) Verarbeitung der Beschäftigtendaten zum Zwecke der Prüfrechte von Drittmittelgebern

Die wissenschaftlichen Einrichtungen werden zu einem nicht unerheblichen Teil durch Drittmittel finanziert. Bereits zum Zeitpunkt der Beantragung von Drittmitteln fragen Drittmittelgeber umfangreiche Informationen bei Antragstellern über die Beschäftigten (Lebensläufe, Qualifikationen u.ä.) ab. Für Nachweise über die Mittelverwendung räumen sich Drittmittelgeber umfangreiche Prüfrechte der Arbeitsverträge, Personalkosten und An- und Abwesenheiten während der Durchführung sowie nach Abschluss der Projekte ein.

Karlsruher Institut für Technologie (KIT)  
Kaiserstraße 12  
76131 Karlsruhe  
USI-IDNr: DE266749428

Präsident: Prof. Dr.-Ing. Holger Hanselka  
Vizepräsidenten: Prof. Dr. Thomas Hirth,  
Prof. Dr. Oliver Kraft, Christine von Vangerow,  
Prof. Dr. Alexander Wanner

LBBW/BW Bank  
IBAN: DE44 6005 0101 7495 5001 49  
BIC/SWIFT: SOLADEST600

LBBW/BW Bank  
IBAN: DE18 6005 0101 7495 5012 96  
BIC/SWIFT: SOLADEST600

2

Die Drittmittelgeber berufen sich auf unterschiedliche Vorschriften, die ihnen nach ihrer Auffassung ein Prüfrecht einräumen, wie z. B. § 44 LHO Baden-Württemberg. Allerdings verdrängen die haushaltsrechtlichen Vorschriften die datenschutzrechtlichen Vorschriften nicht, da sie nicht explizit den Schutz personenbezogener Daten regeln. Außerdem können diese lediglich eine Erhebungs-, jedoch nicht eine Übermittlungsgrundlage darstellen.

In der jüngsten Vergangenheit mehrten sich Anfragen sowohl nationaler als auch europäischer Drittmittelgeber, die die Übermittlung von Arbeitsverträgen zum Gegenstand haben. Vor-Ort-Kontrollen werden von den Drittmittelgebern regelmäßig nicht für ausreichend angesehen.

Der Arbeitgeber hat die Rechte der Beschäftigten zu schützen. Eine wissenschaftliche Einrichtung, die auf Drittmittel angewiesen ist, kann die zunehmend sich ändernden Anforderungen der Drittmittelgeber nicht ignorieren.

Grundsätzlich besteht für Drittmittelgeber eine Anforderlichkeit, die ordnungsgemäße Abrechnung der geförderten Projekte prüfen zu können, da diese im Rahmen ihrer ihnen zugewiesenen Aufgaben handeln.<sup>1</sup> Demnach muss auch die wissenschaftliche Einrichtung grundsätzlich in der Lage sein, die Beschäftigtendaten (auch Personalaktendaten) an Bewilligungsbehörden übermitteln zu dürfen, sofern diese für die konkrete Prüfung erforderlich sind.

Das LDSG-E verweist für die Verarbeitung der Personalaktendaten auf § 50 des Beamtenstatusgesetzes und die §§ 83 bis 88 des Landesbeamtengesetzes Baden-Württemberg. Danach ist eine Übermittlung der von den Drittmittelgebern oft geforderten Unterlagen (wie z. B. der Arbeitsverträge) schwer und nur unter besonderen Voraussetzungen begründbar.

Vor dem Hintergrund, dass diese Problematik mögliche finanzielle Konsequenzen für Forschungseinrichtungen nach sich zieht - Drittmittelgeber könnten bei Nichtübermittlung der geforderten Unterlagen Rückforderungsansprüche gegen die Zuwendungsempfänger geltend machen - ist eine eindeutige Rechtsgrundlage dringend von Nöten, die sich ausdrücklich auf die Beschäftigtendaten bezieht und die Verarbeitung von Personalaktendaten mitabdeckt. Dies erfordern sowohl die Rechtssicherheit als auch die Rechtsklarheit.

<sup>1</sup> So auch der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, s. ZENDAS, Übermittlung personenbezogener Daten an Bewilligungsbehörden des Bundes im Rahmen einer Projektförderung, abrufbar unter <https://www.zendas.de/download.html?file=ee3d830308390cf8cb437004ac618aa9>, zuletzt abgerufen am 12. Januar 2018. Das Schreiben kann bei Bedarf zur Verfügung gestellt werden.

3

Die Einwilligungserklärung als alternative Rechtsgrundlage für das Übermitteln personenbezogener Beschäftigendaten eignet sich nach der vom KIT vertretenen Auffassung für diesen Zweck nur bedingt, da diese unter dem Vorbehalt des jederzeitigen Widerrufs durch den Beschäftigten steht. Das Prüfrecht der Zuwendungsgeber und damit mögliche Rückforderungen gegen die Zuwendungsempfänger kann in der Praxis jedoch nicht von der freiwilligen und widerruflichen Einwilligungserklärung der Beschäftigten abhängen.

Nach Einschätzung des KIT dürfte dieser Regelungsbedarf nicht ausschließlich für Forschungseinrichtungen, sondern mutmaßlich für alle Zuwendungsgeber und -empfänger relevant sein, unabhängig davon, ob es sich um ein gesetzliches oder vertragliches Prüfungsrecht handelt. Wissenschaftlichen Einrichtungen müssen auch Möglichkeiten an die Hand gegeben werden, vertragliche Verpflichtungen erfüllen zu können. Über diese Möglichkeiten verfügen grundsätzlich die wissenschaftlichen Einrichtungen, die privatrechtlich organisiert sind (Art. 6 Abs. b) DS-GVO). Es kann aber gerade nicht darauf ankommen, welche Rechtsform eine wissenschaftliche Einrichtung besitzt, um die Prüfanforderungen von Drittmittelgebern erfüllen zu können.

Es wird daher empfohlen einen neuen § 14 Abs. 3 LDSG-E einzuführen:

3) *Personenbezogene Daten von Beschäftigten **einschließlich der Personalaktendaten** dürfen verarbeitet werden, soweit diese für Zwecke der Ausübung eines gesetzlichen oder vertraglich vorgesehenen Prüfungsrechts erforderlich sind.*

b) § 14 Abs. 3: Verweis auf § 50 des Beamtenstatusgesetzes und der §§ 83 bis 88 des Landesbeamtengesetzes

Gemäß § 14 Abs. 3 LDSG-E sollen für die Verarbeitung der Personalaktendaten von Arbeitnehmerinnen und Arbeitnehmern sowie Auszubildenden in einem privatrechtlichen Ausbildungsverhältnis die für die Beamtinnen und Beamten geltenden Vorschriften des § 50 des Beamtenstatusgesetzes und der §§ 83 bis 88 des Landesbeamtengesetzes entsprechende Anwendung finden.

Die Beamtengesetze finden ihre verfassungsrechtliche Grundlage in Art. 33 Abs. 5 GG. Das dort verankerte Gebot der Fortentwicklung des Berufsbeamtentums gilt nicht für die Arbeitnehmerinnen und Arbeitnehmer im öffentlichen Dienst.<sup>3</sup>

<sup>2</sup> Der Passus „einschließlich Personalaktendaten“ wäre zu streichen, sofern der Gesetzgeber der Empfehlung des KIT unter Ziff. 1b) folgt und den derzeitigen § 14 Abs. 3 LDSG-E nicht in die endgültige Fassung des Gesetzes übernimmt.

<sup>3</sup> Klenzler/Stehele, Beamtenrecht Baden-Württemberg, 2. Auflage, Kapitel 3, Rn 24.

4

Der Beamte befindet sich in einer besonderen Beziehung zum Staat, seine Grundrechte unterliegen weitergehenden Begrenzungen. Das strenge Personalaktenrecht im Beamtenrecht trägt dem „besonderen Gewaltverhältnis“ zwischen dem Beamten und dem Staat Rechnung. Dies kann daher auf die Beschäftigten im öffentlichen Dienst nicht ohne Einschränkungen übertragen werden.

Dafür spricht, dass weder das derzeit gültige Bundesdatenschutzgesetz (BDSG) noch das neue BDSG, das am 25. Mai 2018 in Kraft tritt, einen entsprechenden Verweis auf die Anwendung der beamtenrechtlichen Vorschriften für die Beschäftigten der öffentlichen Stellen enthält.

Die Anwendung des Beamtenrechts auf die Beschäftigten im öffentlichen Dienst führt bereits nach der bestehenden Rechtslage in der Praxis vermehrt zu sachfremden Ergebnissen. Dies belegen bereits die Ausführungen unter Ziff. 1 a). Des Weiteren sind auch die Regelungen in § 86 Abs. 2 Nr. 1-4 LBG BW nicht ohne weiteres auf das Verhältnis zu Angestellten übertragbar. Die Regelungen, die vor dem Hintergrund etwaiger Versorgungsansprüche der Beamten die Aufbewahrung der Unterlagen regeln, passen nicht auf das Beschäftigtenverhältnis. Auch die Variante des § 86 Abs. 2 Nr. 1 LBG BW, die gerade den Fall des Ausscheidens ohne Versorgungsansprüche regelt, passt nicht. Dies führt dazu, dass gerade eine so wichtige Regelung wie der Fristbeginn für die Aufbewahrung von Personalakten der Auslegung des Rechtsanwenders überlassen wird. Die entsprechende Anwendung dieser Regelung führt allerdings nicht zu einem eindeutigen Ergebnis, was nicht im Sinne des Gesetzgebers sein kann.

Die Gesetzesbegründung zur Vorgängerregelung des § 36 Abs. 2 LDSG besagt:

„In Bezug auf Beamte enthält die Vorschrift einen Verweis auf die maßgeblichen Vorschriften des Landesbeamtengesetzes. Hinsichtlich der Verarbeitung von Daten der Angestellten und Arbeiter sowie der Auszubildenden erscheint es angemessen, die Vorschriften des Landesbeamtengesetzes entsprechend anzuwenden; ...“<sup>4</sup>.

Am KIT sind laut dem Jahresbericht 2016 ca. 9 300 Beschäftigte und 547 Beamte inklusive der Professoren und Professorinnen tätig. Dies bedeutet, dass ein Gesetz auf über 8 000 Betroffene angewendet wird, welches in direkter Anwendung ausschließlich für ca. 500 Personen gilt und welches weder von seiner Zielrichtung noch vom Wortlaut auf diese Betroffenen passt.

<sup>4</sup> LT-Drs. 12/4899, S. 48 für § 30 a Abs. 2 LDSG. § 30 a Abs. 2 LDSG stellte die vom 01. September 2000 bis zum 31. Dezember 2010 geltende Vorgängerregelung des § 36 Abs. 2 LDSG dar. Diese Regelung ist bis auf den durch Art. 22 des Dienstrechtsreformgesetzes geänderten Verweis auf § 50 BeamtStG und §§ 83 bis 88 LBG wortlautgleich mit § 36 Abs. 2 LDSG.

5

Insoweit muss in Bezug auf das KIT und seine Sonderrolle unter den Universitäten in Baden-Württemberg der oben dargestellten Gesetzesbegründung widersprochen werden. Eine entsprechende Anwendung der beamtenrechtlichen Vorschriften auf die Angestellten und Arbeiter ist - zumindest für das KIT- gerade nicht angemessen.

Das KIT empfiehlt daher, § 14 Abs. 3 LDSG-E zu streichen.

## 2) § 17 Videoüberwachung öffentlich zugänglicher Räume

Die Gesetzesbegründung zum § 17 LDSG-E (s. 29) stellt klar, dass die Videoüberwachung zur Wahrung des Hausrechts und berechtigter Interessen sich zukünftig „allein nach Artikel 6 Absatz 1 Buchstabe f“ der DS-GVO richtet und daher „nicht mehr erwähnt“ wird.

Danach wären für die oben genannten Anwendungsfälle (Wahrung des Hausrechts und berechtigter Interessen) nicht die Anforderungen des § 17 Abs. 2 bis Abs. 6 LDSG-E zu beachten. Dies würde allerdings den Datenschutz, insbesondere im Verhältnis zum derzeit gültigen Landesdatenschutzgesetz in Baden-Württemberg, erheblich schwächen. Gerade die Kennzeichnungspflicht dient dem Schutz des Persönlichkeitsrechts der Betroffenen und darf nicht wegfallen, wenn es um die Wahrung des Hausrechts und der berechtigten Interessen der öffentlichen Stelle geht.

Um etwaige Missverständnisse zu vermeiden, empfiehlt das KIT daher eine entsprechende Klarstellung in der Gesetzesbegründung, dass die Absätze 2 bis 6 des § 17 LDSG-E auch auf die Anwendungsfälle der Wahrung des Hausrechts sowie berechtigter Interessen der öffentlichen Stelle Anwendung finden.

Mit freundlichen Grüßen



Christine von Vangerow

---

**Von:** Wolfgang Kreißig  
**Gesendet:** Mittwoch, 31. Januar 2018 18:27  
**An:** Registratur 2 (IM)  
**Cc:**  
**Betreff:** Stellungnahme der Landesanstalt für Kommunikation zu dem Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679 - Aktenzeichen: 2-0557.8/1  
**Anlagen:** Gesetzesentwurf Stand 30.10.2017.pdf

**Stellungnahme der Landesanstalt für Kommunikation zu dem Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679**

**Aktenzeichen: 2-0557.8/1**

Sehr geehrte Damen und Herren,

der in der Anlage beigefügte Entwurf eines Gesetzes zum 21. Rundfunkänderungs-staatsvertrag und zur Anpassung des Medien-Datenschutzrechts an die Verordnung (EU) 2016/679 (Datenschutzgrundverordnung, DS-GVO) sieht u.a. neu die Zuständigkeit des Vorsitzenden des Vorstands der LFK für die Aufsicht bei der Datenverarbeitung privater Rundfunkveranstalter zu journalistischen Zwecken (§ 50 Abs. 3 LMedienG-E) vor. Das Ziel dieses Gesetzes ist es, die medienspezifischen datenschutzrechtlichen Bestimmungen im Landesmediengesetz und im Landespressegesetz an die Vorgaben der DS-GVO anzupassen, um dem in Artikel 85 DS-GVO für die Mitgliedsstaaten vorgesehenen Regelungsauftrag nachzukommen. Dieser lässt für die Datenverarbeitung zu journalistischen, wissenschaftlichen, künstlerischen oder literarischen Zwecken Abweichungen bzw. Ausnahmen von der DS-GVO zu, um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang bringen zu können (sog. Medienprivileg).

Der Gesetzgeber hat daneben eine positive Rundfunkordnung zu schaffen, in der die Vielfalt der bestehenden Meinungen im Rundfunk möglichst breit und umfassend vermittelt werden. Dies erfordert auch geeignete organisatorische Vorkehrungen, um den Rundfunk nicht einseitig dem Staat oder einer gesellschaftlichen Gruppe auszuliefern (stRspr, etwa BVerfGE 57, 295, 320 ff.). Die kommunikationsverfassungs-rechtlichen Anforderungen der Rundfunkfreiheit (Art. 5 Abs. 1 S. 2 GG) verlangen eine unabhängige Medienaufsicht, die staatsfern organisiert ist und nicht in verfassungswidriger Weise in die Freiheit der Veranstalter einzugreifen vermag. Insoweit übt die LFK als unabhängige und staatsferne Anstalt des öffentlichen Rechts die Aufsicht über die privaten Rundfunkveranstalter aus.

Durch die Neuregelung des Medien-Datenschutzrechts im Entwurf des LMedienG wird diese Funktion auf die Aufsicht über die Einhaltung datenschutzrechtlicher Bestimmungen bei der Datenverarbeitung zu journalistischen Zwecken ausgedehnt. Diese Aufsicht soll künftig von dem Vorsitzenden des LFK-Vorstandes wahrgenommen werden. Die Ausgestaltung seines Amtes entspricht dem Unabhängigkeitsniveau der DS-GVO. Daneben wird zur weiteren Sicherung seiner Unabhängigkeit für die Ausübung der Aufsicht im datenschutzrechtlichen Bereich eine Dienst- und Rechtsaufsicht ausgeschlossen (§ 50 Abs. 3 S. 5 LMedienG-E).

Der Anwendungsbereich des Landesdatenschutzgesetzes (LDSG) gilt wie bisher für alle öffentlichen Stellen des Landes (§ 2 Abs. 1 LDSG-E). Zuständige Aufsichtsbehörde ist grundsätzlich der Landesbeauftragte für den Datenschutz (LfD), § 24 Abs. 1 LDSG-E. Eine sektorale Aufsicht wird etwa – wie bislang – für den SWR auf Grund seiner Staatsferne geregelt (§ 26 Abs. 1 LDSG). Die allgemeine Aufsicht des LfD über die LFK kann nach diesseitigem Rechtsverständnis nicht gelten, soweit der staatsferne Vorsitzende des Vorstandes die Datenschutzaufsicht im journalistischen Bereich wahrnimmt. Denn eine unbeschränkte

Aufsicht des LfD über die LFK hätte mittelbar auch eine Aufsicht über die journalistische Datenverarbeitung der Rundfunkveranstalter zur Folge, zumal diese den Kernbereich der Rundfunkfreiheit berührt. Zu Recht wird auch der Bereich der sog. „Mischdatenverarbeitung“, die einen medienspezifischen Bezug aufweist, dem staatsfernen Vorsitzenden des Vorstandes übertragen (S. 20 des Entwurfs eines Gesetzes zum 21. Rundfunkänderungsstaatsvertrag und zur Anpassung des Medien-Datenschutzrechts an die Verordnung (EU) 2016/679).

Wir regen daher an, in das neue LDSG bzw. in dessen Begründung – etwa zu § 24 Abs. 1 LDSG-E - aus Gründen der Klarheit des Gesetzes aufzunehmen, dass **die Zuständigkeit des Landesbeauftragten für den Datenschutz zur Aufsicht über den Datenschutz bei der LFK nicht gegeben ist, soweit der Vorsitzenden des Vorstands der Landesanstalt für Kommunikation seinerseits die Aufsicht nach § 50 Abs. 3 LMedienG wahrnimmt.**

Mit freundlichen Grüßen

Wolfgang Kreißig

**Dr. Wolfgang Kreißig**  
Präsident

-----

Landesanstalt für Kommunikation Baden-Württemberg (LFK)  
Postanschrift: [Postfach 10 29 27, 70025 Stuttgart](mailto:Postfach 10 29 27, 70025 Stuttgart)  
Hausanschrift: [Reinsburgstr. 27, 70178 Stuttgart](mailto:Reinsburgstr. 27, 70178 Stuttgart)  
Internet: <http://www.lfk.de>



**Baden-Württemberg**  
**LANDESARCHIV**  
FACHPROGRAMME UND BILDUNGSARBEIT

Az.: 0551.0/8

Datum: 31. Januar 2018

** Gesetz zur Anpassung des allgemeinen Datenschutzrechts und sonstiger  
Vorschriften an die Verordnung (EU) 2016/679 Baden-Württemberg  
hier: Stellungnahme des Landesarchivs Baden-Württemberg**

1. Verarbeitung besonderer Kategorien von Daten zu im öffentlichen Interesse liegenden Archivzwecken

Der Gesetzentwurf sieht bisher keine Rechtsgrundlage für die Verarbeitung von besonderen Kategorien von Daten für im öffentlichen Interesse liegende Archivzwecke vor. Nach Artikel 9 Absatz 1 Datenschutzgrundverordnung (EU-DSGVO) ist die Verarbeitung besonderer Kategorien von Daten untersagt. Die Mitgliedstaaten können von diesem Verarbeitungsverbot aber nach Artikel 9 Absatz 2 Buchstabe j EU-DSGVO insbesondere für im öffentlichen Interesse liegende Archivzwecke Ausnahmen regeln.

Ohne eine solche Regelung können die öffentlichen Archive in Baden-Württemberg besondere Kategorien von Daten nicht verarbeiten. Dies ist aber erforderlich, weil für unterschiedliche Forschungsrichtungen – z.B. zur Diskriminierung von Minderheiten, für die Medizinforschung – sowie für die Politikplanung solche Daten archiviert werden müssen. Die Daten werden auch benötigt für Belange Betroffener wie z.B. derzeit für Entschädigungsberechtigungen ehemaliger Heimkinder aus psychiatrischen Einrichtungen.

Aus diesem Grund ist die Schaffung einer Rechtsgrundlage für die Verarbeitung besonderer Kategorien von Daten zu im öffentlichen Interesse liegende Archivzwecke erforderlich und entsprechend im Gesetzentwurf aufzunehmen.

- 2 -

## 2. Ausnahmen von den Betroffenenrechten

Damit Archive auch unter der Geltung der EU-DSGVO im bisherigem Umfang arbeitsfähig bleiben, wurde in Art. 89 Abs. 3 EU-DSGVO ein „Archivprivileg“ verankert. Nach Artikel 89 Abs. 3 EU-DSGVO können die Mitgliedstaaten für im öffentlichen Interesse liegende Archivzwecke Ausnahmen von Betroffenenrechten nach Artikel 15, 16, 18, 19, 20 und 21 DSGVO vorsehen.

Im Gesetzentwurf wird in § 13 nur der Forschungsbereich derogiert. Die Derogation des Archivbereichs ist nicht vorgesehen. Die Aufnahme von Ausnahmen von den Betroffenenrechten für im öffentlichen Interesse liegende Archivzwecke ist allerdings erforderlich. Damit wird in Archiven

- a) die Übernahme dauerhaft gesichert und
- b) vermieden, dass bei der Verarbeitung von personenbezogenen Informationen zusätzliche Aufwände nach Art. 15, 16, 18-21 EU-DSGVO anfallen.

Der Bund hat hierzu eine vergleichbare Regelung im neuen Bundesdatenschutzgesetz in § 28 Absatz 2 bis 4 getroffen. Diese könnte unter systematischen Gesichtspunkten für eine Regelung im Landesdatenschutzgesetz Vorbild sein; allerdings ist bei der Derogation für Archivzwecke, wie in Art. 89 DSGVO vorgesehen, die Einbeziehung des gesamten Art. 18 sowie des Art. 19 DSGVO vorzunehmen.

## 3. „Löschungssurrogat“ – Archivierung ersetzt Löschung

Damit die o.g. Daten für die genannten Zwecke genutzt werden können, muss eine Abgabe an die Archive möglich sein. Dafür bedarf es einer gesetzlichen Ermächtigung, auch diejenigen Daten zu archivieren, die Löschvorschriften unterliegen, des sog. *Löschungssurrogats*, nach dem die Archivierung eine vorgeschriebene Löschung ersetzt. Dieses bisher national bzw. in der Bundesrepublik auch auf Länderebene verankerte Prinzip wurde in der EU-DSGVO Art. 17 Abs. 3 aufgenommen. Sobald archivische Belange geltend gemacht werden können, findet das *Recht auf Vergessen-werden* seine Grenzen. Mit der EU-DSGVO wird der Vorrang archivischer Zwecke vor der Löschung ausdrücklich und grundsätzlich anerkannt.

Dieser Vorrang der Archivierung vor der Löschung setzt nach EU-DSGVO Art. 17 Abs. 3 d) „im öffentlichen Interesse liegende Archivzwecke“ voraus. In Verbindung mit der Anbieterspflicht in § 3 Abs. 1 Satz 1 und 2 Landesarchivgesetz BW für nicht mehr benötigte Daten und dem § 10 (Beschränkung des Rechts auf Löschung) Abs. 1 des novellierten Datenschutzgesetzes

*Die Bestimmungen des Landesarchivgesetzes zur Anbietungspflicht sowie sonstige gesetzliche oder satzungsmäßige Dokumentations- und Aufbewahrungspflichten bleiben unberührt.*

besteht künftig das Löschungssurrogat für folgende Daten (EU-DSGVO Art. 17 Abs. 1)

- a) Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.*
- b) Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.*
- c) Die betroffene Person legt gemäß Artikel 21 Absatz 1 Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder die betroffene Person legt gemäß Artikel 21 Absatz 2 Widerspruch gegen die Verarbeitung ein.*
- d) Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.*
- e) Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.*
- f) Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Artikel 8 Absatz 1 erhoben.*

Damit wird die bisherige Regelung in § 23 Abs. 3 LDSG mit dem Anbietungsvorrang vor der Löschung (Ersetzung der Löschung durch Archivierung = „Löschungssurrogat“) bei

1. Daten, die einer allgemeine Löschverpflichtung unterliegen und
2. Daten, die unzulässig gespeicherten wurden

vollständig ersetzt.

Unklar ist, ob mit dieser Aufzählung auch Daten einbezogen sind, die nach landesgesetzlichen Spezialgesetzen einer Löschverpflichtung unterliegen und bisher ebenfalls vom Löschungssurrogat nach § 23 Abs. 3 LDSG erfasst waren. Wenn diese Frage positiv entschieden wird, würde das Löschungssurrogat für diese Daten ebenfalls aufgrund von Art. 17 EU-DSGVO gelten.

Sofern diese Daten nicht einbezogen wären, wird zur Beibehaltung des geltenden Zustands eine separate Regelung benötigt. Eine Möglichkeit bestünde darin, eine Auffangregelung im Landesarchivgesetz im Zusammenhang mit der korrespondierenden Regelung zur Anbietungspflicht zu schaffen.

- 4 -

Es könnte in das o.g. Gesetz ein separater Artikel als Nr. 20 „Änderung des Landesarchivgesetzes“ eingeschoben und darin der § 3 (1) Satz 1 LArchG wie folgt erweitert werden.

*Die Behörden, Gerichte und sonstigen Stellen des Landes bieten alle Unterlagen, die sie zur Erfüllung ihrer Aufgaben nicht mehr benötigen, dem Landesarchiv an, sofern die Anbietungspflicht nicht abweichend geregelt ist. Unabhängig davon sind alle Unterlagen jedoch spätestens 30 Jahre nach ihrer Entstehung ...*

Die Formulierung *sofern die Anbietungspflicht nicht abweichend geregelt ist* stellt eine schlanke Version der Anbietungspflicht bei zu löschenden Daten dar. Ähnlich hatte der Bundesrat – auf Initiative Baden-Württembergs – bei der Beratung dieses Sachverhalts für das Bundesarchivgesetz formuliert: „Anzubieten sind auch Daten, die nach gesetzlichen Vorschriften vernichtet oder gelöscht werden müssen, es sei denn, es ist nach diesen gesetzlichen Vorschriften ausgeschlossen, sie den zuständigen öffentlichen Archiven anzubieten.“

Bei dem Vorschlag wird weiter davon ausgegangen, dass die Formulierung *„alle Unterlagen, die sie zur Erfüllung ihrer Aufgaben nicht mehr benötigen“* in § 3 (1) Satz 1 LArchG umfassend zu verstehen ist; selbst wenn diese im Archivrecht seit langem bewährte Formulierung Ähnlichkeiten mit DSGVO Art. 17 Abs. 1 Buchstabe a) aufweist, sind damit auch sämtliche Fälle einbezogen, die in der DSGVO unter Art. 17 Abs. 1 Buchstabe b) bis f) genannt werden, sowie weitere bisher nicht aufgeführte, aber vorstellbare Fälle. Damit wird eine enumerative Aufzählung vermieden, die bei Gesetzesänderungen stets nachzuführen wäre.

### **Vorschlag**

Es wird daher vorgeschlagen,

1. den Gesetzentwurf um eine Rechtsgrundlage für die Verarbeitung besonderer Kategorien von Daten zu im öffentlichen Interesse liegenden Archivzwecken und
2. um Ausnahmen von den Betroffenenrechten, soweit dies nach Artikel 89 Abs. 3 EU-DSGVO möglich ist, zu ergänzen.
3. Es sollen weiterhin Archivierungsmöglichkeiten für Unterlagen bestehen, die Löschverpflichtungen nach landesgesetzlichen Regelungen unterliegen. Sofern es nötig ist, sollte dafür das Landesarchivgesetz ergänzt werden, um den geltenden Rechtszustand beizubehalten.

31.1.2018, Dr. Clemens Rehm



# Baden-Württemberg

LANDESARCHIV  
ARCHIVISCHER GRUNDSATZ

## AKTENNOTIZ

Az.: 0551.0/8

Datum: 7.2.2018

### **Derogation nach EU-DSGVO Art. 89 für Archivzwecke. Umsetzung in Landesgesetzen**

Bei der Umsetzung der Derogationsmöglichkeiten für Archivzwecke, die in der EU-DSGVO durch Art. 89 gegeben sind, zeichnen sich in den Bundesländern unterschiedliche Wege ab.

Ein inzwischen häufig gegangener Weg ist die Verankerung der Derogation im jeweiligen Landesdatenschutzgesetz. In diesen Fällen wird auf die im Bund verabschiedete neue Form des § 28 BDSG Bezug genommen bzw. diese direkt übernommen, wie es in Hessen geschehen ist (vgl. Anlage Datenschutz-Anpassungs- und -Umsetzungsgesetz, Drucksache 18/11325).

Die für Archivzwecke mögliche Derogation wird im § 28 Abs. 4 BDSG für Art. 18 Absatz 1 Buchstabe c) und für Art. 19 EU-DSGVO **nicht** umgesetzt. Damit wird die Arbeit der Archive erheblich belastet.

Bei der weiteren Umsetzung der EU-DSGVO in Landesgesetzen ist darauf zu achten, dass für Archivzwecke die Derogation von Art. 18 umfassend stattfindet und Art. 19 einbezogen wird.

Damit befindet sich der Gesetzgeber auf der Linie, die seinerzeit die Länder bei der Verabschiedung der EU-DSGVO bezogen haben, als sie die Derogationsmöglichkeit von Art. 18 und Art. 19 für Archivzwecke unterstützt haben.

- 2 -

**Zu Art. 18 Absatz 1 Buchstabe c)**

Eine betroffene Person kann vom Datenhaltenden die Einschränkung der Verarbeitung ihrer Daten verlangen, wenn sie diese Daten zur Geltendmachung von Ansprüchen benötigt – und zwar auch in den Fällen, in denen der Datenhaltende diese Daten nicht mehr benötigt.

Dieser Fall tritt in Archiven regelmäßig auf, wenn Unterlagen als archivwürdig übernommen wurden und dann z.B. bei der Erschließung nach archivfachlichen Grundsätzen fein- oder nachkassiert wird, weil sich bei der Autopsie der Stücke die Archivwürdigkeit nicht bestätigt hat.

Der Konfliktfall liegt dann wie folgt: Ein Betroffener wendet sich mit seinem Ansuchen an die aktenproduzierende Stelle, die entsprechend der Ablieferungsliste an das zuständige Archiv weiterverweist. Sofern dort nach- bzw. feinkassiert worden ist, ist der Betroffene in seinen Rechten eingeschränkt. Eine solche Situation ließe sich nur vermeiden, wenn vor jeder Nach- bzw. Feinkassation alle in den Unterlagen genannten Personen und ggf. deren Nachfahren vor der Vernichtung gefragt würden, ob nach Art. 18 Punkt 1 c) Einsprüche erhoben würden. Da dies für Archive nicht leistbar ist, wurde die Derogationsmöglichkeit geschaffen.

**Zu Art. 19**

Alle Personen, denen ihre Daten offengelegt wurden, müssen nach Art. 19 über Berichtigung, Löschung oder Einschränkung der Verarbeitung ihrer Daten informiert werden. Da die Archive bei der Übernahme von Daten nicht mitgeteilt bekommen, wem welche Daten in der ursprünglich datenführenden Stelle zugänglich gemacht wurden, können sie diese Aufgabe nicht erfüllen.

Im Art. 19 wird diese Auskunftspflicht unter bestimmten Bedingungen aufgehoben. Diese Einschränkung wird mit den Worten „es sei denn“ eingeleitet und kennzeichnet sie damit als Ausnahmetatbestand. Dieser Ausnahmetatbestand ist aber in Archiven der Regelzustand; daher wurde die Derogationsmöglichkeit geschaffen.

Dr. Clemens Rehm  
7. Februar 2018

Anlage

## § 28 BDSG

*Datenverarbeitung zu im öffentlichen Interesse liegenden Archivzwecken*

*(1) Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 zulässig, wenn sie für im öffentlichen Interesse liegende Archivzwecke erforderlich ist. Der Verantwortliche sieht angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person gemäß § 22 Absatz 2 Satz 2 vor.*

*(2) Das Recht auf Auskunft der betroffenen Person gemäß Artikel 15 der Verordnung (EU) 2016/679 besteht nicht, wenn das Archivgut nicht durch den Namen der Person erschlossen ist oder keine Angaben gemacht werden, die das Auffinden des betreffenden Archivguts mit vertretbarem Verwaltungsaufwand ermöglichen.*

*(3) Das Recht auf Berichtigung der betroffenen Person gemäß Artikel 16 der Verordnung (EU) 2016/679 besteht nicht, wenn die personenbezogenen Daten zu Archivzwecken im öffentlichen Interesse verarbeitet werden. Bestreitet die betroffene Person die Richtigkeit der personenbezogenen Daten, ist ihr die Möglichkeit einer Gegendarstellung einzuräumen. Das zuständige Archiv ist verpflichtet, die Gegendarstellung den Unterlagen hinzuzufügen.*

*(4) Die in Artikel 18 Absatz 1 Buchstabe a, b und d, den Artikeln 20 und 21 der Verordnung (EU) 2016/679 vorgesehenen Rechte bestehen nicht, soweit diese Rechte voraussichtlich die Verwirklichung der im öffentlichen Interesse liegenden Archivzwecke unmöglich machen oder ernsthaft beeinträchtigen und die Ausnahmen für die Erfüllung dieser Zwecke erforderlich sind.*



## Baden-Württemberg

DER LANDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ UND DIE INFORMATIONSFREIHEIT

LfDI Baden-Württemberg · Postfach 10 29 32 · 70025 Stuttgart

### Vorab per E-Mail

Innenministerium  
Baden-Württemberg  
Postfach 10 34 65  
70029 Stuttgart

Datum 30. Januar 2018

Name Herr Broo

Aktenzeichen D 2200/1

(Bitte bei Antwort angeben)

 Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679  
Ihr Schreiben vom 19. Dezember 2017, Az.: 2-0557.8/1

Sehr geehrte Damen und Herren,

für die Gelegenheit, im Rahmen der Anhörung zu o. g. Gesetzentwurf Stellung zu nehmen, danken wir.

### Zu Artikel 1 des Gesetzentwurfs (Landesdatenschutzgesetz)

1. Der Gesetzentwurf beschränkt sich auf Bestimmungen zur Anpassung der Anwendung der Vorschriften der Datenschutz-Grundverordnung (DS-GVO). Die Umsetzung der Richtlinie (EU) 2016/680 (nachf.: RL 2016/680) bleibt einem gesonderten Gesetz vorbehalten. Hierzu soll dem Vernehmen nach ein Polizeidatenschutzgesetz geschaffen werden. Da nicht davon auszugehen ist, dass dieses Gesetz auch Regelungen über die Datenverarbeitung der **Gerichte der Strafgerichtsbarkeit** enthalten wird, ist offen, an welcher Stelle zur Gewährleistung der richterlichen Unabhängigkeit für die Gerichte der Strafgerichtsbarkeit eine dem § 2 Absatz 5 des Entwurfs vergleichbare Regelung geschaffen werden soll (Erwägungsgrund [EG] 80 RL 2016/680). Denkbar wäre insoweit - allerdings unter Inkaufnahme eines Bruchs in der Systematik -, in § 2 Absatz 1 Satz 3 Nummer 3 des Entwurfs die Wörter „mit Ausnahme des Absatzes 5,“ anzufügen.

- 2 -

Dabei wird davon ausgegangen, dass den „zuständigen Behörden“ im Sinne der RL 2016/680 auch die Strafgerichte zuzuordnen sind (vgl. EG 11 Satz 2, EG 80 Satz 1 RL 2016/680 „Gerichte und andere Justizbehörden“).

Die Datenverarbeitung durch die Staatsanwaltschaften wird zwar im Wesentlichen in der Strafprozessordnung durch den Bundesgesetzgeber geregelt. Für die Datenverarbeitung außerhalb des eigentlichen Bereiches der Strafverfolgung gehen wir davon aus, dass diese in den sachlichen Anwendungsbereich der DS-GVO fällt. Der Entwurf enthält diesbezüglich aber keine Regelung. Insbesondere findet § 2 Absatz 4 des Entwurfs keine Anwendung, da die Vorschrift ausdrücklich davon ausgeht, dass die Datenverarbeitung **nicht** in den sachlichen Anwendungsbereich der DS-GVO fällt.

2. Da sich die Bußgeldandrohungen der DS-GVO nicht gegen die handelnde Person, sondern (nur) gegen Verantwortliche richten, ist fraglich, ob künftig (noch) Geldbußen gegen Behördenmitarbeiter verhängt werden können, wenn diese unter Überschreitung ihrer Kompetenzen aus privaten Gründen personenbezogene Daten verarbeiten. Dies wäre nur dann möglich, wenn der Mitarbeiter, weil er die Daten für eigene Zwecke verwendet, selbst als Verantwortlicher im Sinne des Artikels 4 Nummer 7 DS-GVO anzusehen wäre. Um solche Sanktionslücken zu vermeiden, sollte das Landesdatenschutzgesetz nach wie vor das Datengeheimnis entspr. dem bisherigen § 6 LDSG regeln und den Verstoß hiergegen mit einem Bußgeld bewehren (vgl. Artikel 11 und 23 des Entwurfs eines bayerischen Datenschutzgesetzes).
3. Der Landesbeauftragte für den Datenschutz übt (auch) gegenüber öffentlichen Stellen die Befugnisse insbesondere nach Artikel 58 Absatz 2 DS-GVO aus (§ 24 Absatz 2 des Entwurfs). Dies wird künftig dazu führen, dass Anweisungen, Anordnungen, Verbote und sonstige Maßnahmen auch gegenüber Behörden durch Verwaltungsakt getroffen werden. Kommt eine Behörde einer solchen Verwaltungsentscheidung nicht nach, muss dem Landesbeauftragten ermöglicht werden, seine Verfügung durchzusetzen. Während Artikel 58 Absatz 5 DS-GVO unmittelbar die Befugnis einräumt, direkt oder indirekt ein gerichtliches Verfahren einzuleiten, fehlt es an einer Rechtsgrundlage für die Anwendung von Mitteln des Verwaltungszwangs. § 22 des Landesverwaltungsvollstreckungsgesetzes schließt eine Vollstreckung gegen Behörden ohne spezielle gesetzliche Grundlage ausdrücklich aus. Das Fehlen einer solchen Befugnis der Aufsichtsbehörde, ihre Entscheidungen auch zwangsweise durchsetzen zu können, würde diesen in der Praxis in weitem Maße ihre praktische Wirksamkeit nehmen. Der Gesetzge-

- 3 -

ber ist aber verpflichtet dafür zu sorgen, dass für die Um- und Durchsetzung der Befugnisse der Aufsichtsbehörde wirksame Mittel zur Verfügung stehen. Nach Artikel 288 Absatz 3 des Vertrags über die Arbeitsweise der Europäischen Union in Verbindung mit Artikel 4 Absatz 3 des Vertrages über die Europäische Union sind die Mitgliedstaaten im Rahmen der ihnen belassenen Freiheit verpflichtet, diejenigen Formen und Mittel zu wählen, die für die Gewährleistung der praktischen Wirksamkeit der europäischen Rechtsakte gemäß ihrer Zielsetzung am geeignetsten sind (EuGH, Urteil vom 04. Juli 2006 - C-212/04 -, juris, m.w.N.). Dies erfordert eine Regelung, welche den Landesbeauftragten berechtigt, auch gegenüber Behörden die Zwangsmittel des Landesverwaltungsvollstreckungsgesetzes anzuwenden.

4. Die Sinnhaftigkeit des § 2 Absatz 3 Satz 2 des Entwurfs erschließt sich nicht. Der Vorrang des Landesdatenschutzgesetzes beschränkt sich auf Bestimmungen des Landesverwaltungsverfahrensgesetzes (LVwVfG), welche die Datenverarbeitung im Rahmen der Sachverhaltsermittlung betreffen. Was dies konkret bedeutet, bleibt offen. Auch der Hinweis auf den Hauptanwendungsfall, die Datenerhebung gemäß § 4 des Entwurfs, ist wenig erhellend; diese Bestimmung enthält wenig mehr als den Grundsatz der Erforderlichkeit. Neben den die Sachverhaltsermittlung betreffenden Vorschriften der §§ 24 und 26 LVwVfG gibt es im Landesverwaltungsverfahrensgesetz weitere Vorschriften, welche die Verarbeitung personenbezogener Daten betreffen (§ 74 Absatz 1 Satz 2, Absatz 3, Absatz 4 i.V.m. § 39, § 69 Absatz 2 Satz 1 LVwVfG), die in der Verwaltungspraxis immer wieder zu Problemen führen (vgl. BVerfG, Kammerbeschluss vom 24. Juli 1990 - 1 BvR 1244/87-, juris). Der Gesetzentwurf enthält sich insoweit einer Aussage, was gelten soll.
5. Zu § 3 des Entwurfs: Als „Konkretisierung“ (siehe Begründung) der in Artikel 32 Absatz 1 DS-GVO genannten Maßnahmen können allenfalls die Nummern 2 bis 5 sowie 10 gelten. Sowohl der Einleitungssatz wie auch die Nummern 1 und 6 bis 9 wiederholen wörtlich Artikel 32 Absatz 1 DS-GVO. Hierin sehen wir einen Verstoß gegen das Wiederholungsverbot (hierzu: EuGH, Urteil vom 7. Februar 1973 - 39/72 -, juris). Auch mit Blick auf EG 8 DS-GVO erscheint die Wiederholung nicht erforderlich.
6. § 4 des Entwurfs bringt seinem Wortlaut nach den Vorbehalt des Gesetzes nicht zum Ausdruck. Da die Landesverfassung selbst kein dem allgemeinen Persönlichkeitsrecht des Grundgesetzes entsprechendes Persönlichkeitsrecht normiert

- 4 -

ist, ergibt sich der Gesetzesvorbehalt in diesem Zusammenhang direkt aus dem Rechtsstaats- und dem Demokratieprinzip. Um klarzustellen, dass die Allzuständigkeit der Gemeinden aus Artikel 28 Absatz 2 Satz 1 GG keine öffentliche Aufgabe im Sinne von § 4 des Entwurfes begründet, sollten nur Aufgaben, „die der öffentlichen Stelle durch oder aufgrund eines Gesetzes“ übertragen wurden“, von der Regelung des § 4 des Entwurfes umfasst sein.

7. Im Unterschied zum bisherigen § 15 Absatz 2 Nummer 5 LDSG verlangt § 5 Absatz 1 Nummer 1 des Entwurfs nicht mehr eine „unmittelbar drohende“ Gefahr als Voraussetzung für eine Zweckänderung. Eine solche erhebliche Ausweitung der Zweckänderungsbefugnisse widerspricht dem Grundsatz der Datenminimierung (Artikel 5 Absatz 1 Buchstabe c, Artikel 6 Absatz 4 DS-GVO; „notwendige und verhältnismäßige Maßnahme“). Der Gesetzentwurf lässt jedenfalls nicht erkennen, inwieweit der Rückschritt gegenüber dem bisherigen Datenschutzniveau in diesem Punkt berechtigt sein könnte.

In § 5 Absatz 1 Nummer 3 des Entwurfs sollten in Anpassung an den Wortlaut der Nummern 1 und 2 die Wörter „geboten erschein“ durch die Wörter „erforderlich ist“ ersetzt werden.

Daneben erscheint der Nachsatz „soweit die Verarbeitung notwendig und verhältnismäßig ist“ überflüssig. „Notwendig und verhältnismäßig“ sind die Kriterien, die als Maßstab an die Regelung von Zweckdurchbrechungen als solche anzulegen sind. Dieselben Kriterien erneut für die Einzelfallprüfung vorzusehen, erscheint insbesondere in Anbetracht dessen, dass solche Einzelfallmaßnahmen tatbestandlich die Erforderlichkeit voraussetzen, nicht sachgerecht. Zumal es schwer nachvollziehbar ist, nach welchen Gesichtspunkten (kumulativ) die Notwendigkeit einer Verarbeitung zu beurteilen sein soll, deren Erforderlichkeit bereits festgestellt wurde.

Die Begründung zu § 5 Absatz 2 des Entwurfs bezieht sich offensichtlich noch auf eine ältere Entwurfassung. Tatsächlich geht es hier um Weiterverarbeitungen, die allerdings mit den ursprünglichen Zwecken vereinbar sind (EG 50 Satz 3 DS-GVO). Das Unterbleiben einer Information der betroffenen Person in den Fällen des § 5 Absatz 1 Nummer 4 des Entwurfs (Überprüfung von Angaben; § 5 Absatz 3) findet keine Rechtsgrundlage in Artikel 23 Absatz 1 DS-GVO. Es dürfte auch grundsätzlich auszuschließen sein, dass die Information des Betroffenen über eine solche Überprüfung den Verarbeitungszweck gefährden kann.

8. Nach Artikel 5 Absatz 2 DS-GVO liegt die Beweislast für die Rechtmäßigkeit einer Datenverarbeitung beim Verantwortlichen (Pötters, in: Gola, DS-GVO, Artikel

- 5 -

5 Rdnr. 34). Angesichts dessen ist es zweifelhaft, ob die Verantwortung für die Rechtmäßigkeit einer Datenübermittlung, wie dies - entsprechend der bisherigen Rechtslage - in § 6 Absatz 1 Satz 2 des Entwurfs vorgesehen ist, auf die empfangende Stelle abgewälzt werden kann.

§ 6 Absatz 2 des Entwurfs überträgt die Regelung des Absatzes 1 auf die Fälle, in denen ein automatisiertes Abrufverfahren eingerichtet ist. Diesbezüglich bestehen die bereits dargestellten Bedenken. Hinzu kommt, dass anders als bisher in § 8 LDSG der Entwurf keine spezifische Bestimmung über die automatisierte Abrufverfahren enthält. Eine solche hätte hier nahegelegen, da § 6 Absatz 2 des Entwurfs auf solche Verfahren Bezug nimmt, ohne dass im Gesetz oder in der DS-GVO näher bestimmt ist, unter welchen Voraussetzungen diese eingerichtet werden dürfen.

9. § 7 Absatz 1 Satz 5 des Entwurfs verpflichtet zur Wahrung eines gesetzlich bisher nicht geregelten Datengeheimnisses. Insofern verweisen wir auf die Ausführungen unter Nummer 2.
10. Für die in § 9 Absatz 1 Satz 2 des Entwurfs vorgesehene Einschränkung des Auskunftsrechts sehen wir keine Berechtigung. Beschränkungen sind nach Artikel 23 Absatz 1 DS-GVO nur zulässig, wenn sie den dort näher aufgeführten Interessen dienen. Zwecke der Datensicherung oder Datenschutzkontrolle sind dort nicht enthalten.  
Auch für die in § 9 Absatz 2 des Entwurfs vorgesehene Einschränkung des Auskunftsrechts sehen wir in dieser Form keine Berechtigung. Eine solche Einschränkung setzt voraus, dass die öffentliche Stelle der betroffenen Person Hinweise gibt, die es dieser ermöglichen, die Angaben nach § 9 Absatz 2 Satz 1 des Entwurfs zu machen, etwa indem die öffentliche Stelle die jeweils für eine Auskunft bedeutsamen Arten der Informationen, die sie verarbeitet, oder der Verarbeitungsvorgänge, die bei ihr stattfinden, benennt.
11. § 10 Absatz 2 des Entwurfs schließt eine Pflicht zur Löschung im mutmaßlichen Interesse der betroffenen Person aus. Dazu ist zu sagen, dass dies nur solange gelten kann, bis feststeht, ob die betroffene Person tatsächlich ein Interesse an der weiteren Speicherung hat. Es kann nicht sein, dass die verantwortliche Stelle letztlich über den Kopf der betroffenen Person über die weitere Speicherung entscheidet, deren Dauer ebenfalls im Ermessen der verantwortlichen Stelle liegen würde. Erforderlich ist deshalb, dass eine Benachrichtigung der betroffenen Per-

- 6 -

son vorgeschrieben wird, damit diese darüber entscheiden kann, ob und ggf. wie lange die Daten weiterhin gespeichert werden sollen.

12. Es wird angeregt, § 11 Absatz 1 Nummer 3 des Entwurfs zu streichen. Die IT-Sicherheit kann einen Verzicht auf die Benachrichtigung nicht normenklar begründen. Hier besteht die konkrete Gefahr einer Überdehnung dieser Ausnahmenvorschrift in der Praxis. Zudem ist die eigenständige Regelung in Nummer 3 auch deshalb nicht erforderlich, weil Nummer 1 (Gefährdung der öffentlichen Sicherheit und des Wohls des Bundes und der Länder etc.) eine Gefährdung der Sicherheit informationstechnischer Systeme mit abdecken würde.
13. § 12 Absatz 2 Nummer 2 des Entwurfs lässt eine Zweckänderung zu, wenn „die Voraussetzungen des § 5 Absatz 1 Nummern 1 oder 2 vorliegen und die zur Verschwiegenheit verpflichtete Stelle eingewilligt hat“. Aufgrund welcher Umstände und Erwägungen es genügen soll, dass die Verarbeitung „zur Abwehr“ bereits (irgend) „einer Gefahr für die öffentliche Sicherheit erforderlich ist“ (§ 5 Absatz 1 Nummer 1 LDSG-E), und was mit „eingewilligt“ gemeint ist, erschließt sich auch mit Blick auf die Begründung (in der von „zugestimmt“ die Rede ist) nicht.
14. Dass § 13 Absatz 3 des Entwurfs auf Artikel 89 Absatz 1 DS-GVO beruht und die Rechte und Freiheiten der betroffenen Person, deren personenbezogene Daten danach veröffentlicht werden dürfen, „garantiert“, erschließt sich uns nicht. Vielmehr dürfte § 13 Absatz 3 des Entwurfs in diese Rechte und Freiheiten eingreifen, zumal die derzeitige Voraussetzung des § 35 Absatz 3 LDSG, wonach überwiegende schutzwürdige Interessen des Betroffenen nicht entgegenstehen dürfen, entfallen soll.
15. In § 14 Absatz 1 des Entwurfs sollte folgender neuer Satz 2 eingefügt werden:  
„Die Verarbeitung ist auch zulässig, wenn sie zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Dienst- oder Betriebsvereinbarung ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist.“ Hierdurch wird die Weitergabe personenbezogener Daten an Interessenvertretungen wie den Personalrat oder die Schwerbehindertenvertretung legitimiert.  
Angeregt wird, aus Gründen der besseren Verständlichkeit den bisherigen Satz 2 als neuen Absatz 2 zu fassen. Jedenfalls sollten nach den Wörtern „öffentlichen Stellen“ die Wörter „oder der betroffenen Person“ eingefügt werden (entsprechend dem Wortlaut des Artikel 9 Absatz 2 Buchstabe b DS-GVO). Schließlich

- 7 -

sollte klargestellt werden, ob die Verarbeitung besonderer Kategorien personenbezogener Daten auch auf der Grundlage von Kollektivvereinbarungen möglich sein soll oder nicht und ob die Verarbeitung besonderer Kategorien personenbezogener Daten auch auf der Grundlage einer Einwilligung des Beschäftigten erfolgen kann; wird hierzu nichts gesagt, ist die Einwilligung möglich (vgl. Artikel 9 Absatz 1 Buchstabe a DS-GVO).

In § 14 Absatz 2 des Entwurfs sollten vor dem bisherigen Satz folgende neuen Sätze eingefügt werden: „Erfolgt die Verarbeitung personenbezogener Daten von Beschäftigten auf der Grundlage einer Einwilligung, sind für die Beurteilung der Freiwilligkeit der Einwilligung insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen. Freiwilligkeit kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Der Arbeitgeber hat die beschäftigte Person über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht nach Artikel 7 Absatz 3 der Verordnung (EU) 2016/679 in Textform aufzuklären. Die Bedingungen an die Einwilligung gelten auch für die Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten; die Einwilligung muss sich dabei ausdrücklich auf diese Daten beziehen.“ Grund hierfür ist, dass nach Erwägungsgrund [EG] 155 DS-GVO Bedingungen an die Einwilligung gestellt werden können. Eine solche Bedingung wäre die Schriftform. Diese ist in Artikel 7 DS-GVO nicht vorgesehen. Durch das Schriftformerfordernis wird dem Schutz der Beschäftigten Rechnung getragen. Artikel 88 Absatz 2 DS-GVO fordert, dass die nationalen Bestimmungen zum Beschäftigtendatenschutz angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person vorsehen. Durch die Aufnahme des Schriftformerfordernisses wird Artikels 88 Absatz 2 DS-GVO Rechnung getragen. Die Bedingungen für die Einwilligung sollten zum Schutz der Beschäftigten auch für die Verarbeitung besonderer Kategorien personenbezogener Daten auf Grundlage einer Einwilligung gelten.

In § 14 Absatz 4 des Entwurfs sollten nach dem Wort „wenn“ die Wörter „zu dokumentierende“ eingefügt werden. Dies ist erforderlich, um eine Kontrolle durch die Aufsichtsbehörde zu ermöglichen. Da die Verantwortlichen bereits wegen der Rechenschaftspflicht aus Artikel 5 Absatz 2 DS-GVO zur Dokumentation verpflichtet sind, würde die Klarstellung zu mehr Rechtssicherheit für die Verantwort-

lichen führen. Des Weiteren sollte geprüft werden, ob auch schwerwiegende Pflichtverletzungen von der Regelung mit umfasst sein sollten. Die Rechtsprechung sieht auch schwerwiegende Pflichtverletzungen von § 32 Absatz 1 Satz 2 BDSG umfasst. Da in vielen Fällen keine Straftat, sondern nur eine schwerwiegende Pflichtverletzung des Dienstverhältnisses vorliegt, erscheint diese Ergänzung praxisgerecht.

In § 14 Absatz 5 des Entwurfs sollten die Zwecke, die zu einer Verarbeitung biometrischer Daten von Beschäftigten mit deren Einwilligung berechtigen, näher umschrieben werden. In der bisherigen Fassung fehlt es an der Bestimmtheit. In Betracht kämen zum Beispiel Autorisierungs- oder Authentifikationszwecke. Bezüglich der zweiten Alternative ergibt sich weder aus der Vorschrift noch aus der Begründung, ob das dringende dienstliche Bedürfnis auch bei der Einwilligung oder nur bei der Grundlage einer Dienst- oder Betriebsvereinbarung gegeben sein muss. Zudem sollten Fälle genannt werden, wann von einem dringenden dienstlichen Bedürfnis ausgegangen werden kann. Hierzu findet sich auch nichts in der Begründung.

§ 14 Absatz 6 sollte ersatzlos gestrichen werden. Die Zwecke der Verhaltens- und Leistungskontrolle sind bereits von Absatz 1 umfasst und müssen den Grundsatz der Erforderlichkeit wahren. Eine Verhaltens- und Leistungskontrolle ist nur stichprobenartig oder anlassbezogen möglich. Bei einem Straftatverdacht richtet sich die Verarbeitung personenbezogener Daten nach Absatz 4. Eine dauerhafte Verhaltens- und Leistungskontrolle kommt einer Totalkontrolle gleich und ist damit stets unverhältnismäßig und damit unzulässig. Sollte der Absatz beibehalten werden, ist Folgendes zu beachten: Zur Erreichung der Zwecke der Verhaltens- und Leistungskontrolle ist in der Regel eine Überwachung mit Hilfe optisch-elektronischer Einrichtungen nicht erforderlich und damit unzulässig. Dieser Passus ist zu streichen. Aus der Vorschrift muss sich dann aber ergeben, dass die optisch- elektronische Einrichtung von den sonstigen technischen Einrichtungen ausgenommen ist. Andernfalls würde die optisch-elektronische Einrichtung unter die sonstigen technischen Einrichtungen fallen. In der Vorschrift selbst sollte klar definiert sein, wann von einer dauerhaften Überwachung auszugehen ist. Davon ist in der Regel bei einer Dauer von 24 Stunden ohne Unterbrechung oder an mehr als vier Tagen auszugehen. Sofern der Absatz nicht gestrichen wird, sollte zum besseren Verständnis der Hinweis auf Absatz 1 der Vorschrift mitaufgenommen werden, da eine Verarbeitung nur dann zulässig ist, wenn der Grundsatz der Erforderlichkeit gewahrt ist.

Es sollte folgender neuer Absatz 7 eingefügt werden: „(7) Die Absätze 1 bis 6 sind auch anzuwenden, wenn personenbezogene Daten, einschließlich besonde-

rer Kategorien personenbezogener Daten, von Beschäftigten verarbeitet werden, ohne dass sie in einem Dateisystem gespeichert sind oder gespeichert werden sollen.“ Anders als bisher gilt das LDSG-neu nur noch für automatisierte Verarbeitungen oder nicht-automatisierte Verarbeitung in einem Dateisystem. Somit fällt ein wichtiger Teil im Bereich des Beschäftigtendatenschutzes heraus, wenn dieser Absatz nicht aufgenommen wird. Nachfragen beim ehemaligen Dienstherrn erfolgen oft telefonisch. Nur durch die Aufnahme des Absatzes können Beschäftigte umfassend in ihrem Recht auf informationelle Selbstbestimmung geschützt werden. So würden Beschäftigte beispielsweise während des Bewerbungsgesprächs schutzlos gestellt werden, wenn ihnen unzulässige Fragen gestellt werden (Stichwort Fragerecht des Arbeitgebers/Dienstherrn). Um die bisherige Rechtslage aufrecht zu erhalten, ist eine Aufnahme des Absatzes dringend erforderlich.

Die Regelung über die Zuverlässigkeitsüberprüfung des § 14 Absatz 8 erscheint im Kontext der Regelung über die Datenverarbeitung im Rahmen von Beschäftigungsverhältnissen systemfremd. Im Übrigen halten wir sie insoweit für problematisch, als der Begriff des „sicherheitsrelevanten Bereiches“ zu unbestimmt ist. Letztlich bleibt es jeder öffentlichen Stelle überlassen, wie sie solche Bereiche definiert. Damit sind dem Anwendungsbereich der Vorschrift keine klaren Grenzen gesetzt. Weiterhin fehlt es auch nur ansatzweise an einer Festlegung, welche Daten im Rahmen einer solchen Überprüfung verarbeitet werden sollen. Die Begrenzung durch den Verweis auf den Erforderlichkeitsgrundsatz in Absatz 1 reicht hierfür nicht aus. Wann jemand als unzuverlässig angesehen wird und welche Daten in diesem Zusammenhang verarbeitet werden sollen, unterläge dem freien Ermessen der einzelnen Behörde. Geht es etwa um die Verhinderung von Terroranschlägen, bedarf es zur Feststellung der Zuverlässigkeit weit weniger und weit weniger sensible Daten als zur Verhinderung von Diebstählen oder Ausspähungen. Schließlich stellt sich die Frage, welchen Mehrwert eine Regelung gegenüber der bisherigen Rechtslage hat, die kumulativ zur Datenverarbeitung eine Einwilligung der Betroffenen erfordert, ansonsten aber keine weiteren Inhalte aufweist. Als Beispiel dafür, wie eine Regelung für die Zuverlässigkeitsüberprüfung aussehen könnte (deren Notwendigkeit im Übrigen nicht bestritten, sondern vom Landesbeauftragten vielmehr seit Jahren gefordert wird) kann auf § 13a des hessischen Gesetzes über die öffentliche Sicherheit und Ordnung verwiesen werden.

16. § 15 Absatz 1 des Entwurfs soll das Verarbeiten personenbezogener Daten zur Entscheidung über öffentliche Auszeichnungen und Ehrungen (so die Begründung) auf „eine rechtliche Grundlage unabhängig von der Einwilligung“ stellen und festlegen, dass die öffentlichen Stellen insofern nicht zur Informations- und Auskunftserteilung gemäß Artikel 13 bis 15 DS-GVO verpflichtet sind. Da es nach der Begründung unter anderem um „besonders sensible Bereiche“, „die persönliche Integrität der auszuzeichnenden Person“ und „eine möglichst umfassende Heranziehung entscheidungsrelevanter Daten“ geht, steht im Raum, dass die betroffene Person auch hinsichtlich ihres Privatlebens „durchleuchtet“ werden soll (etwa hinsichtlich Vorstrafen, Auffälligkeiten, Aufenthaltsorten, Kontaktpersonen und Vorlieben). Für einen solchen erheblichen Grundrechtseingriff sehen wir jedenfalls in § 15 Absatz 1 des Entwurfs mit Blick auf die Begründung keine Eingriffsnorm, zumal der Wortlaut des § 15 Absatz 1 Halbsatz 1 des Entwurfs keine Erforderlichkeit anspricht. Nach der Begründung sind die Umstände, die zu einer positiven oder negativen Entscheidung führen, oft sehr sensibel und berühren die Integrität der beteiligten Personen. Warum gerade das den weiteren erheblichen Grundrechtseingriff stützen soll, dass beispielsweise den betroffenen Personen kein Auskunftsrecht zustehen soll und über öffentliche Auszeichnungen und Ehrungen im Rahmen eines „Geheimverfahrens“ entschieden werden soll, erschließt sich uns nicht. Vielmehr wäre das Gegenteil geboten.
17. In Anbetracht des Risikos einer gegen Artikel 21 der Charta der Grundrechte der Europäischen Union verstoßenden Verarbeitung von Daten ist die Verarbeitung sensibler Daten im Sinne des Artikel 9 Absatz 1 DS-GVO besonderen Restriktionen unterworfen. Um dem gerecht zu werden, bedarf es einer speziellen Regelung, sofern solche Daten entgegen ihrem ursprünglichen Erhebungszweck verarbeitet werden sollen. Es wird vorgeschlagen, dem § 16 des Entwurfs folgenden neuen Satz 2 anzufügen (vgl. insoweit § 24 Absatz 2 BDSG vom 30. Juni 2017, BGBl. I S. 2097):  
„Die Verarbeitung besonderer Kategorien personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem sie erhoben wurden, ist zulässig, wenn die Voraussetzungen des Satzes 1 und ein Ausnahmetatbestand nach Artikel 9 Absatz 2 der Verordnung (EU) 2016/679 vorliegen.“
18. Mit § 17 des Entwurfs soll die Videoüberwachung öffentlich zugänglicher Räume neu geregelt und somit die bisherige Regelung des § 20a LDSG ersetzt werden. Hierzu Folgendes:

- a. Sowohl nach dem Wortlaut des Entwurfs als auch der Begründung richtet sich die Videoüberwachung zur Wahrung des Hausrechts sowie zur Wahrung berechtigter Interessen zukünftig allein nach Artikel 6 Absatz 1 Unterabsatz 1 **Buchstabe f** DS-GVO. Dem liegt ein enges Verständnis des Artikel 6 Absatz 1 Unterabsatz 1 **Buchstabe e** DS-GVO zugrunde, wonach die Verarbeitung **unmittelbar** zur Erfüllung einer öffentlichen Aufgabe erforderlich sein muss. Dient sie dagegen nur **mittelbar** der Wahrnehmung einer öffentlichen Aufgabe (etwa der Wahrung des Hausrechts oder dem Eigentumsschutz), beurteilt sich die Rechtmäßigkeit einer Datenverarbeitung stattdessen allein nach Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe f DS-GVO.

Ein solches enges Verständnis des Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe e DS-GVO und - folgerichtig - der damit korrespondierenden Öffnungsklausel führt dann aber zu einem äußerst begrenzten Anwendungsbereich des (neuen) § 17, da es in der Praxis kaum Fälle geben wird, in denen die Behörde eine Videoüberwachung unmittelbar zur Wahrnehmung ihrer Aufgaben einsetzen wird.

Wir halten diese Auffassung für vertretbar, allerdings sollte dann im Normtext (vgl. zur Unbestimmtheit der Tatbestandsmerkmale auch die weiteren Ausführungen) und auch in der Begründung genauer dargelegt werden, welche Fälle letztlich noch unter das Landesdatenschutzgesetz fallen. In jedem Fall aber muss der dritte Absatz im allgemeinen Teil der Begründung zu § 17 (*„Anwendungsfälle dieser Norm werden weiterhin der Personen- und Objektschutz, also der Schutz von Personen, die sich in öffentlichen Objekten oder in deren Nähe aufhalten, sowie der Schutz der Objekte selbst sein, soweit sie die Funktionsfähigkeit der öffentlichen Stellen gewährleisten und damit mittelbar auch deren Aufgabenerfüllung dienen. Als öffentliche Objekte können Kulturgüter, öffentliche Einrichtungen, Dienstgebäude oder öffentliche Verkehrsmittel angesehen werden.“*) gestrichen werden. Denn dort werden gerade die Sachverhalte als von § 17 erfasst bezeichnet, die lediglich mittelbar der öffentlichen Aufgabenwahrnehmung dienen und daher nach Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe f DS-GVO zu beurteilen sind (Personen- und Objektschutz ist nichts anderes als Wahrung des Hausrechts und Eigentumsschutz).

Will man dagegen auch solche Anwendungsfälle erfassen, die nur mittelbar der Aufgabenerfüllung dienen, muss dies zwingend und eindeutig in § 17 geregelt werden (ähnlich wie aktuell in § 20a LDSG). Ein Verweis auf Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe f DS-GVO wäre dann aber hinfällig. In-

- 12 -

wieweit dies von der Öffnungsklausel des Artikel 6 Absatz 3 DS-GVO letztlich gedeckt wäre, ist allerdings fraglich.

- b. § 17 Absatz 1 des Entwurfs macht die Zulässigkeit der Videoüberwachung allein davon abhängig, dass sie der Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe dient und im Rahmen einer Abwägung schutzwürdige Interessen der betroffenen Personen nicht überwiegen. Diese Regelung verstößt eklatant gegen Grundsätze des Datenschutzes.

Schon bisher ist es so, dass eine allgemeine Regelung wie § 13 LDSG keine tragfähige Grundlage für Videoüberwachungsmaßnahmen darstellt (so:

BVerfG, Stattgebender Kammerbeschluss vom 23. Februar 2007 – 1 BvR

2368/06 –, juris). § 17 des Entwurfs, der inhaltlich nichts anderes regelt als

bisher § 13 LDSG, wäre somit schon verfassungsrechtlich unzulässig. Nach-

dem durch die DS-GVO nun Maßstab für die Zulässigkeit von Eingriffen in

das Datenschutzgrundrecht die Artikel 7 und 8 EU-GRCharta sind, haben

sich die Anforderungen gegenüber bisher eher erhöht. Die einschlägige

Rechtsprechung des Europäischen Gerichtshofs macht dies sehr deutlich.

Nach dessen ständiger Rechtsprechung verlangt der Schutz dieser Grund-

rechte, dass sich die Ausnahmen vom Schutz personenbezogener Daten

und dessen Einschränkungen auf das **absolut Notwendige** beschränken

müssen (EuGH, Urteil vom 08.04.2014, C-293/12, Celex-Nr. 62012CJ0293).

Sind Eingriffe in die in Artikel 7 und 8 der Charta verankerten Grundrechte

vorgesehen, bedarf es klarer und präziser Regeln zu deren Tragweite. Sol-

che klaren und präzisen Regeln fehlen hier schon hinsichtlich der Sachver-

halte, die zu einer Videoüberwachung überhaupt berechtigen sollen. § 17

geht insoweit nicht über die Generalklausel des § 4 des Entwurfs hinaus und

bleibt sogar deutlich dahinter zurück, indem nicht einmal die Erforderlichkeit

für die Aufgabenerfüllung verlangt wird. § 17 Absatz 1 bedarf somit dringend

einer Konkretisierung, vergleichbar etwa dem bisherigen 20a LDSG

(vgl. auch Artikel 24 des Entwurfs eines Bayerischen Datenschutzgesetzes,

§ 4 des Entwurfs eines Hessischen Gesetzes zur Anpassung des Hessi-

schen Datenschutzrechts an die DS-GVO).

Künftig sollen keine tatsächlichen Anhaltspunkte für eine Gefährdung mehr

verlangt werden. Ohne Anhaltspunkte dafür, dass eine Gefährdungslage be-

steht, kann jedoch die Erforderlichkeit einer Videoüberwachung kaum festge-

stellt werden. Spricht nichts für eine Gefahr, gibt es auch kein die Video-

überwachung legitimierendes (öffentliches) Interesse. Wenn in der Begrün-

dung zum Ausdruck gebracht wird, eine Gefahr könne vorliegen, ohne dass

es dafür tatsächliche Anhaltspunkte gebe, und dies führe zur Bejahung der

- Erforderlichkeit (die im Übrigen nach dem Wortlaut des § 17 Absatz 1 ebenfalls nicht vorausgesetzt wird), erscheint dies unsinnig. Auch wird verkannt, dass nach bisherigem Recht die Rechtsprechung durchweg solche Anhaltspunkte gefordert hat, um überhaupt dazu zu kommen, die Zulässigkeit einer Videoüberwachung in Erwägung zu ziehen.
- c. § 17 Absatz 4 des Entwurfs beschränkt die Informationspflichten in unzulässiger Weise. Diesbezüglich gelten zunächst die Artikel 13 und 14 DS-GVO unmittelbar. Zwar dürfen diese Pflichten auf der Grundlage des Artikels 23 DS-GVO zu den dort genannten Zwecken eingeschränkt werden; § 8 des Entwurfs enthält solche Einschränkungen. In welchem Verhältnis § 17 Absatz 2 zu § 8 steht und welche der in Artikel 23 Absatz 1 DS-GVO genannten Zwecke die Einschränkung sicherstellen soll, bleibt offen. § 17 Absatz 2 des Entwurfs verstößt nach unserer Auffassung gravierend gegen die DS-GVO.
- d. Der Wortlaut des § 17 Absatz 1 des Entwurfs umfasst beispielsweise auch das Aufnehmen und weitere Verarbeiten stehender und bewegter Bilder auch im Rahmen von Forschungsvorhaben oder während Theateraufführungen und beschränkt die Vorschrift nicht auf den in der Überschrift genannten Bereich „öffentlich zugänglicher Räume“. Insoweit wäre noch die Reichweite des § 17 des Entwurfs beziehungsweise dessen Verhältnis etwa zu bestimmten Verarbeitungszwecken wie Forschung oder zu künstlerischen und literarischen Zwecken (§ 18 des Entwurfs) zu klären.
19. Die Regelung zu § 18 des Entwurfs ist nach unserer Auffassung nicht mit der Datenschutz-Grundverordnung vereinbar. Für den Bereich des Rundfunks hat sich die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder in ihrer Entschließung vom 9. November 2017 zu den Bestimmungen im Entwurf eines Rundfunkänderungsstaatsvertrags, denen § 18 des Entwurfs nachempfunden ist, deutlich ablehnend geäußert (<https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2013/02/Umsetzung-der-DSGVO-im-Medienrecht.pdf#>).
- Bedenken bestehen zum einen am generellen Ausschluss aller in Artikel 85 Absatz 2 DS-GVO nicht als abweichungsfest vorausgesetzten Kapitel der Grundverordnung durch § 18 Absatz 1 Satz 1 des Entwurfs. Artikel 85 Absatz 2 DS-GVO konkretisiert gegenüber Absatz 1 die Anforderungen, die die Mitgliedstaaten beim Erlass von nationalen Regelungen berücksichtigen müssen. Wenn nach dem Wortlaut der Bestimmung die Mitgliedstaaten Abweichungen und Ausnahmen von den näher bezeichneten Kapiteln vornehmen dürfen, „wenn dies er-

forderlich ist“, um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen, kommt darin ein deutliches Regel-Ausnahmen-Verhältnis zum Ausdruck, wonach die Vorgaben der DS-GVO grundsätzlich auf die Verarbeitung personenbezogener Daten auch zu künstlerischen oder literarischen Zwecken anzuwenden sind. Ein pauschaler Ausschluss der Anwendung sämtlicher Vorgaben der DS-GVO wäre damit europarechtswidrig.

Zum anderen wird mit § 18 Absatz 1 Satz 2 des Entwurfs von einer Regelung in Kapitel VIII DS-GVO abgewichen. Dieses Kapitel steht jedoch nicht zur Disposition des Gesetzgebers. Hierbei ist zu bedenken, dass eine Haftung des Landes in Betracht kommt, soweit es den in Kapitel VIII enthaltenen Anspruch aus Artikel 82 Absatz 1 DS-GVO ausschließt. Nach dieser Vorschrift hat jede Person, der wegen eines Verstoßes gegen die DS-GVO ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter. Zwar dürften die Gerichte verpflichtet sein, die Vorschriften, in denen die Anwendung von Kapitel VIII ausgeschlossen wird, wegen des Vorrangs der DS-GVO unangewendet zu lassen. Soweit aber die Gerichte wegen § 18 des Entwurfs den Anspruch aus Art. 82 Absatz 1 DS-GVO nicht anwenden sollten, kommt in Betracht, dass die Betroffenen stattdessen das Land aus dem Gesichtspunkt eines offenkundigen und erheblichen Verstoßes gegen Unionsrecht bei der Rechtssetzung in Anspruch nehmen können (vgl. Ruffert in: Callies/Ruffert, EUV / AEUV, 4. Aufl. 2011, Art. 340 AEUV Rn. 36 ff. und 58 ff.).

Schließlich führt der vollständige Ausschluss des Artikel VI DS-GVO dazu, dass über die Befugnisse des Landesbeauftragten gegenüber öffentlichen Stellen, die sich auf § 18 berufen, Unklarheiten bestehen. Wenn in § 24 Absatz 2 des Entwurfs auf die Aufgaben und Befugnisse der Artikel 57 und 58 DS-GVO verwiesen wird, gleichzeitig in § 18 Absatz 1 Satz 1 des Entwurfs aber die Geltung dieses Kapitels vollständig ausgeschlossen wird, liegt hierin ein Widerspruch, der nur in der Weise gelöst werden kann, dass die Aufgaben und Befugnisse des Landesbeauftragten auch im künstlerischen und literarischen Bereich eindeutig geregelt werden. Letztlich kann es nicht sein, dass in diesen Bereichen faktisch keinerlei Datenschutzaufsicht stattfindet.

Insgesamt fordern wir, den § 18 komplett zu streichen oder jedenfalls europarechtskonform auszugestalten.

Der Wortlaut des § 18 Absatz 2 des Entwurfs unterscheidet sich vom Wortlaut des § 18a Absatz 3 des Entwurfs. Auf welchen Umständen und Erwägungen das beruht, erschließt sich uns derzeit nicht. Noch weitergehend unterscheidet sich

der Wortlaut des § 18 Absatz 2 vom Wortlaut des § 18a Absatz 4. Nach § 18a Absatz 4 Satz 1 ist - nach Maßgabe des § 18a Absatz 4 Satz 2 - das Auskunftsrecht der betroffenen Person nicht ausgeschlossen. Insoweit entnehmen wir dem Entwurf nicht, auf welche Konstellationen diese Vorschriften sich jeweils beziehen und auf welchen Umständen und Erwägungen der Grundrechtseingriff durch den insoweit uneingeschränkten Ausschluss des Auskunftsrechts der betroffenen Person durch § 18 Absatz 1 Satz 1 und Absatz 2 hinsichtlich welcher Konstellation jeweils beruhen soll.

Im Übrigen weisen wir auf Artikel 85 Absatz 3 DS-GVO hin, wonach jeder Mitgliedstaat der Kommission die Rechtsvorschriften mitzuteilen hat, die er aufgrund von Absatz 2 erlassen hat. Spätestens damit dürfte ein erhebliches Risiko eines Vertragsverletzungsverfahrens bestehen, wenn diese Regelung unverändert in Kraft treten sollte.

20. Es wird gebeten, entsprechend der bisherigen Regelung in § 26 Absatz 4 Satz 4 LDSG in § 19 Absatz 2 des Entwurfs folgenden neuen Satz 3 anzufügen: „Ihre Einbeziehung in den allgemeinen Personalaustausch der Landesverwaltung wird von der Landesregierung gewährleistet.“ Nur so kann gewährleistet werden, dass innerhalb der gesamten Landesverwaltung der für die sachgerechte Erledigung der Aufgaben unverzichtbare Wissens- und Erfahrungsaustausch fortbesteht. Weiter wird gebeten zu prüfen, ob es gemäß der Hinweise des Finanzministeriums zum TV-L (zu § 2 Nummer 1.1) einer förmlichen Übertragung der Unterschriftsbefugnis der oder des Landesbeauftragten für den Datenschutz bedarf.
21. In § 22 Absatz 4 des Entwurfs fehlt es an einer ausdrücklichen Aufnahme des Versorgungsanspruchs des Landesbeauftragten für den Datenschutz. Insoweit ist der Gesetzentwurf zwingend zu ergänzen.
22. Artikel 54 Absatz 2 DS-GVO verpflichtet die Mitgliedstaaten, sowohl die Verschwiegenheit des Mitglieds der Aufsichtsbehörde als auch die der Bediensteten der Aufsichtsbehörde zu regeln. Dies erfordert eine Anpassung des § 23 Absatz 3 des Entwurfs. Es wird vorgeschlagen, in § 23 Absatz 3 Satz 3 nach dem Wort „er“ die Wörter „oder ihre oder seine Beschäftigten“ einzufügen. Des Weiteren wird vorgeschlagen, nach Satz 4 folgenden neuen Satz anzufügen: „Die Sätze 1, 2 und 4 gelten entsprechend für die Beschäftigten der oder des Landesbeauftragten für den Datenschutz nach Beendigung ihrer Tätigkeit bei der Dienststelle der oder des Landesbeauftragten für den Datenschutz.“

- 16 -

23. § 24 Absatz 4 des Entwurfs regelt die Wahrnehmung der Befugnisse nach Artikel 58 Absatz 2 DS-GVO durch den Landesbeauftragten. Hiernach wird der Landesbeauftragte für den Datenschutz, wenn er Verstöße gegen datenschutzrechtliche Vorschriften oder sonstige Mängel bei der Verarbeitung oder Nutzung personenbezogener Daten feststellt, verpflichtet, dies der Rechts- oder Fachaufsichtsbehörde mitzuteilen und dieser vor Ausübung der Befugnisse des Artikel 58 Absatz 2 Buchstaben b bis g und j der DS-GVO Gelegenheit zur Stellungnahme zu geben. Die geplante Regelung kehrt die bislang geltende Rechtslage (§ 30 Absatz 2 LDSG) in ihr Gegenteil. Insbesondere gilt dies im Falle einer Beanstandung, welche zukünftig Artikel 58 Absatz 2 Buchstabe b DS-GVO unterfällt. Nach § 30 Absatz 2 LDSG gilt bislang, dass nur bei Beanstandungen gegenüber bestimmten, in Satz 1 Nummer 2 näher bezeichneten öffentlichen Stellen **gleichzeitig** die zuständige Rechts- oder Fachaufsichtsbehörde zu informieren ist. Deren Stellungnahme musste nicht abgewartet werden. Der Entwurf sieht hingegen vor, dass im Regelfall die Rechts- oder Fachaufsicht zeitlich vorgezogen vor der Ausübung der Befugnisse zu informieren ist und deren Stellungnahme vor Erlass einer Maßnahme abzuwarten ist.

Es ist nicht erkennbar, warum von der bewährten Vorgehensweise unter dem geltenden LDSG abgewichen werden soll. § 24 Absatz 4 des Entwurfs ist unvereinbar mit den dem Landesdatenschutzbeauftragten durch Artikel 58 DS-GVO zugewiesenen Befugnissen. Der Zwang zur Einbeziehung der Aufsichtsbehörde, bevor überhaupt die Befugnisse nach Art. 58 DS-GVO ausgeübt werden können, führt zu einer klaren - zumindest zeitweisen - Beschneidung dessen Befugnisse. Das vorgesehene Verfahren führt zudem auch zu erheblichen zeitlichen Verzögerungen und erschwert dem Landesbeauftragten, seiner Pflicht nachzukommen, wirksame Sanktionen zu verhängen. Insofern halten wir die Entwurfsregelung des § 24 Absatz 4 für europarechtswidrig. Soweit überhaupt die Notwendigkeit einer dem § 24 Absatz 4 entsprechenden Regelung gesehen wird, sollte unbedingt an der bisherigen Systematik festgehalten werden.

24. Bezüglich § 27 des Entwurfs wird auf die Ausführungen oben zu Nummer 2 verwiesen.
25. Die sprachliche Fassung des § 29 Absatz 1 des Entwurfs ist insoweit nicht zutreffend, als für die Verarbeitung personenbezogener Daten durch die Polizei primär das Polizeigesetz (PolG) gilt. Nach § 48 PolG findet das Landesdatenschutzgesetz nur ergänzend Anwendung. Systemtisch und inhaltlich richtiger wäre es, an-

- 17 -

statt des § 29 Absatz 1 den § 48 PolG etwa wie folgt zu fassen: „Soweit dieses Gesetz keine besonderen Regelungen enthält, findet bis zur Umsetzung der Richtlinie (EU) 2016/680 das Landesdatenschutzgesetz in der Fassung vom 18. September 2000 (GBl. S. 248), zuletzt geändert durch Artikel 2 des Gesetzes vom 17. Dezember 2015 (GBl. S. 1191, 1198) Anwendung.“ Entsprechendes gilt für das Landesverfassungsschutzgesetz (§ 5 Absatz 1 Satz 2 LVSG).

#### **Zu Artikel 7 (Änderung der Verordnung der Landesregierung über Zuständigkeiten nach dem Gesetz über Ordnungswidrigkeiten - OWiZuVO)**

§ 4 Absatz 2 Nummer 5 OWiZuVO soll beibehalten werden. Nach § 59 Absatz 1 des Rundfunkstaatsvertrags überwacht der Landesbeauftragte für seinen Bereich die Einhaltung der Datenschutzbestimmungen des Telemediengesetzes. Nach Artikel 58 Absatz 2 Buchstabe g DS-GVO ist der Landesbeauftragte als Aufsichtsbehörde im Sinne der DS-GVO für die Verhängung von Geldbußen zuständig. Dies spricht dafür, auch § 4 Absatz 2 Nummer 5 OWiZuVO aufzuheben. Des Weiteren sieht Artikel 8 Absatz 3 des Gesetzes zur Änderung des Landesdatenschutzgesetzes und anderer Rechtsvorschriften vom 7. Februar 2011 (GBl. S. 43, 46) vor, dass für die Verfolgung und Ahndung von Ordnungswidrigkeiten nach dem Landesdatenschutzgesetz das Regierungspräsidium Karlsruhe ist. Auch diese Bestimmung ist aufzuheben.

#### **Zu Artikel 13 (Änderung der Meldeverordnung)**

Durch die bloße Ersetzung des Verweises auf § 9 LDSG durch § 3 LDSG-neu in § 20 Absatz 2 Satz 2 MVO kann der unzutreffende Eindruck entstehen, die vorrangigen Bestimmungen insbesondere der Artikel 24 und 32 DS-GVO wären nicht zu beachten. § 3 LDSG-neu ergänzt die genannten Regelungen allerdings nur. Dies könnte vermieden werden, indem der Satz um den Hinweis auf die DS-GVO ergänzt wird: „...entsprechend der Verordnung (EU) 2016/679 sowie § 3 des Landesdatenschutzgesetzes ...“.

#### **Zu Artikel 15 (Änderung des Abschiebehaftvollzugsgesetzes Baden-Württemberg)**

1. Nach § 3 Absatz 4 Satz 1 ist bei der Unterbringung auf die religiöse und ethnische Zugehörigkeit zu achten. Bisher war in Satz 2 geregelt, dass hierfür auch Daten, die den sensiblen Daten im Sinne des § 33 LDSG zuzurechnen sind, im Rahmen der Erforderlichkeit verarbeitet werden dürfen. Künftig soll dies nur noch mit aus-

drücklicher Einwilligung der Betroffenen möglich sein. § 3 Absatz 4 Satz 2 AHaft-VollzG BW verweist damit unausgesprochen auf Artikel 9 Absatz 2 Buchstabe a DS-GVO. Diese Vorschrift setzt allerdings voraus, dass die Verarbeitungszwecke, die Gegenstand der Einwilligung sind, festgelegt werden. Hieran fehlt es bislang. Insofern bedarf es einer Ergänzung.

2. Gegen die Regelung über die Videoüberwachung besonders gesicherter Räume in § 10 Absatz 4 bestehen keine grundsätzlichen Bedenken. Satz 5 dagegen dürfte mit seiner maximalen Speicherdauer von einer Woche unverhältnismäßig sein. Dabei ist zu beachten, dass die Überwachung etwa medizinischer Bettenstationen regelmäßig mit der Erhebung sensibler Daten verbunden sein wird. Dies bedingt, dass die Speicherfristen auf das unbedingt Notwendige begrenzt werden muss. 48 Stunden als Maximalspeicherfrist dürften hier für den Regelfall ausreichen. Formal fällt auf, dass Sätze 5 und 6 jeweils mit Bezug auf Satz 2 einmal von „gespeicherten“, zum anderen von „erhobenen“ Daten sprechen. Hier wird ein einheitlicher Sprachgebrauch angeregt.
3. Die allgemeine Videoüberwachungsregelung des neuen § 10a dürfte vom Grundsatz durch die Öffnungsklausel des Artikel 6 Absatz 3 und 4 DS-GVO gedeckt sein. Es geht hier um Gefahrenabwehr und Strafverfolgungsvorsorge. Dass in solchen Einrichtungen Gefahren für die öffentliche Sicherheit und Ordnung nicht auszuschließen, ja möglicherweise sogar wahrscheinlich sind (abstrakte Gefahrenlage), kann angenommen werden. Ob damit allerdings eine Vollüberwachung zulässig ist, ist zweifelhaft. Dem dürfte der Erforderlichkeitsgrundsatz entgegenstehen. Insofern ist bei der konkreten Umsetzung darauf zu achten, dass insbesondere bei der Überwachung des Gebäudeinneren bestimmte Bereiche ausgenommen werden (z. B. Sozialräume, Toiletten, Duschen). Besondere Zurückhaltung ist bei der Beobachtung der unmittelbaren Umgebung geboten. Keinesfalls dürfen dabei Privatanwesen in der Nachbarschaft erfasst werden. Auch die Beobachtung des öffentlichen Raums ist auf einen eng begrenzten Bereich außerhalb des Einrichtungsgeländes zu beschränken.

#### **Zu Artikel 17 (Änderung des Landesbeamtengesetzes)**

1. In § 83 Absatz 1 Satz 1 des Entwurfs sollten nach dem Wort „Rechtsvorschrift“ die Wörter „oder eine Dienst- oder Betriebsvereinbarung“ eingefügt werden. Da Artikel 88 Absatz 1 DS-GVO auch eine Verarbeitung personenbezogener Beschäftigtendaten auf Grundlage von Dienstvereinbarung erlaubt und § 14

- 19 -

LDSG-neu auch die Dienstvereinbarungen mitumfasst, sollten auch hier mitbestimmungsrechtliche Vereinbarungen als Grundlage für eine Datenverarbeitung aufgenommen werden.

Folgender neuer Satz sollte angefügt werden: „Der Auftraggeber muss zudem die Einhaltung der beamtenrechtlichen Vorschriften kontrollieren. Die Auftragserteilung bedarf der vorherigen Zustimmung der obersten Dienstbehörde. Zu diesem Zweck hat der Auftragsgeber der obersten Dienstbehörde die Unterlagen nach den Artikeln 28 und 29 der Verordnung (EU) 2016/679 zuzuleiten.“ Aus der Begründung geht hervor, dass Satz 2 deklaratorischer Natur sei und abweichende Regelungen mangels Öffnungsklausel nicht möglich seien. Artikel 88 Absatz 1 DS-GVO erlaubt jedoch, dass spezifischere Vorschriften zu Zwecken des Beschäftigungsverhältnisses getroffen werden können. Zum Schutz der Beschäftigten sollten daher besondere und angemessene Maßnahmen getroffen werden. Da die DS-GVO den Auftraggeber nur zur Einhaltung der datenschutzrechtlichen Vorschriften verpflichtet, sollte der eingefügte Satz „Der Auftraggeber muss zudem die Einhaltung der beamtenrechtlichen Vorschriften kontrollieren.“ zwingend aufgenommen werden. Ferner sollte die Auftragsverarbeitung nicht ohne die vorherige Zustimmung der obersten Dienstbehörde erfolgen. Zudem sollte geprüft werden, ob auch nicht-öffentliche Stellen als Auftragnehmer in Betracht kommen sollen. Sofern dies der Fall sein soll, sollten weitere besondere und angemessene Maßnahmen im Sinne von Artikel 88 Absatz 2 DS-GVO getroffen werden. Nicht-öffentliche Stellen sollten nur beauftragt werden dürfen, wenn beim Auftraggeber sonst Störungen im Geschäftsablauf auftreten können oder der Auftragnehmer die übertragenen Aufgaben erheblich kostengünstiger erledigen kann und die beim Auftragnehmer mit der Datenverarbeitung beauftragten Beschäftigten besonders auf den Schutz der Personalaktendaten verpflichtet sind.

In § 83 Absatz 2 Satz 1 des Entwurfs sind die Wörter „gespeichert, verändert oder verwendet“ durch das Wort „verarbeitet“ zu ersetzen. Die DS-GVO geht von einem umfassenden Verarbeitungsbegriff aus (Artikel 4 Nummer 2 DS-GVO). Des Weiteren weisen wir darauf hin, dass auch die Übermittlung eine Form der Verarbeitung darstellt. § 85 LBG muss daher ebenfalls entsprechend angepasst werden. Bei der Übermittlung ging es nach dem LDSG bislang vielmehr darum, dass ein Dritter im Sinne des LDSG die Personalaktendaten erhalten hat. Die DS-GVO misst dem Begriff des Übermittels diese Bedeutung jedoch nicht zu. Daher ist eine Anpassung zwingend geboten. Hierbei ist zwischen „Empfängern“ i. S. d. Artikel 4 Nummer 9 und „Dritten“ i. S. d. Artikel 4 Nummer 10 DS-GVO zu unterscheiden.

- 20 -

Auch in § 83 Absatz 2 Satz 2 sowie in Absatz 3 des Entwurfs ist jeweils der einheitliche Verarbeitungsbegriff zu verwenden.

2. § 85 des Entwurfs ist insgesamt an den einheitlichen Verarbeitungsbegriff anzupassen.
3. Zu § 86 des Entwurfs: Die Rechte und Pflichten betreffend die Löschung nach Artikel 17 DS-GVO können nur unter den Voraussetzungen des Artikels 23 DS-GVO beschränkt werden. Artikel 17 DS-GVO selbst enthält keine Öffnungsklausel, wie in der Begründung zum Entwurf angenommen. Die Anforderungen, die Artikel 23 DS-GVO an eine wirksame Beschränkung der Betroffenenrechte (hier Recht auf Löschung) stellt, sind unseres Erachtens nicht erfüllt. Aus der Vorschrift gehen insbesondere nicht die in Artikel 23 Absatz 2 DS-GVO dargestellten spezifischen Zwecke hervor.
4. § 87 Absatz 4 Nummer 1 des Entwurfs sollte gestrichen werden. Artikel 23 Absatz 1 Buchstabe i 1. Alternative DS-GVO ist eng auszulegen. Die Beschäftigten können selbst am besten einschätzen, ob und inwieweit es in ihrem Interesse liegt, von ihren Betroffenenrechten Gebrauch zu machen. Die Beschränkungsmöglichkeit bietet daher keine Grundlage dafür, in bevormundender Weise Informationen zurückzuhalten, welche den Beschäftigten vermeintlich übermäßig belasten würden (vgl. Bäcker in Kühling/Buchner, DS-GVO Kommentar, § 23 Rn. 30). Gerade Feststellungen zum Gesundheitszustand sind für die Beschäftigten von Bedeutung, wenn auf deren Grundlage beamtenrechtliche Entscheidungen getroffen werden sollen.  
Entgegen der Begründung des Gesetzesentwurfs zu § 87 Absatz 4 Nummer 2 des Entwurfs ist die Einschränkung sehr wohl an Artikel 23 DS-GVO zu messen. Hier kommt Artikel 23 Absatz 1 Buchstabe i 2. Alternative DS-GVO in Betracht.

**Es wird gebeten, nach Artikel 19 folgende neuen Artikel einzufügen:**

„Artikel 20

Änderung des Landesbesoldungsgesetzes Baden-Württemberg

In der Anlage 2 (Landesbesoldungsordnung B) des Landesbesoldungsgesetzes Baden-Württemberg vom 9. November 2010 (GBl. S. 793, 826), das zuletzt durch Artikel 1 des Gesetzes vom 18. Juli 2017 (GBl. S. 334) geändert worden ist, wird in der Besoldungsgruppe B 3 bei der Amtsbezeichnung „Leitender Ministerialrat<sup>\*\*5)</sup> bei dem

- 21 -

Funktionszusatz nach der Zeile mit den Wörtern „als ständiger Vertreter eines Abteilungsleiters“ eine neue Zeile mit den Wörtern „als Leitender Beamter der Dienststelle des Landesbeauftragten für den Datenschutz“ eingefügt.“

Mit der Einrichtung der oder des Landesbeauftragten für den Datenschutz als oberste Landesbehörde erhält auch das Amt der Leitenden Beamtin oder des Leitenden Beamten der Dienststelle der oder des Landesbeauftragten für den Datenschutz einen deutlichen Aufgaben- und Bedeutungszuwachs, der eine besoldungsrechtliche Bewertung entsprechend B 3 rechtfertigt (§ 20 LBesGBW). Die Wertigkeit dieser Funktion ergibt sich auch aus dem Vergleich mit der bisherigen besoldungsrechtlichen Einstufung des ständigen Vertreters eines Abteilungsleiters bei einer obersten Landesbehörde in die Besoldungsgruppe B 3. Die Leitende Beamtin oder der Leitende Beamte ist die ständige Vertreterin oder der ständige Vertreter der oder des Landesbeauftragten für den Datenschutz als Leiter einer obersten Landesbehörde.

#### „Artikel 21 Überleitungsregelung

Der Beamte, der am Tag vor dem Inkrafttreten dieses Gesetzes die Funktion des Leitenden Beamten der Dienststelle des Landesbeauftragten für den Datenschutz als Ministerialrat in Besoldungsgruppe B 2 inne hat, wird vom Beginn des Kalendermonats an, in dem dieses Gesetz in Kraft tritt, in das Amt des Leitenden Ministerialrats mit dem Funktionszusatz als leitender Beamter der Dienststelle des Landesbeauftragten für den Datenschutz in Besoldungsgruppe B 3 übergeleitet.“

Das Amt der leitenden Beamtin oder des leitenden Beamten der oder des Landesbeauftragten für den Datenschutz soll wegen des Aufgabenzuwachses künftig in einem Amt nach Besoldungsgruppe B 3 ausgewiesen werden. Artikel 21 stellt die Überleitung des Beamten sicher, der am Tag vor dem Inkrafttreten dieses Gesetzes die Funktion des leitenden Beamten der Dienststelle des Landesbeauftragten für den Datenschutz in einem nach Besoldungsgruppe B 2 ausgewiesenen Amt wahrnimmt.

Mit freundlichen Grüßen  
In Vertretung

Volker Broo  
Leitender Beamter

## Stellungnahme



Vorsitzender: Dr. Carsten T. Rees  
Geschäftsstelle: Silberburgstr. 158  
70178 Stuttgart

E-Mail: [info@leb-bw.de](mailto:info@leb-bw.de)  
[www.leb-bw.de](http://www.leb-bw.de)

### **Stellungnahme des Landeselternbeirates Baden-Württemberg zur Neufassung des Landesdatenschutzgesetzes**

In seiner Sitzung am 17.01.2018 hat sich der LEB mit der Neufassung des Landesdatenschutzgesetzes befasst. Dabei hat sich der LEB auf die für Schulen relevanten Teile des neuen Gesetzes beschränkt.

#### **Der Landeselternbeirat stimmt der Vorlage zu.**

Die Umsetzung der im Landesdatenschutzgesetz formulierten Änderungen an den Schulen wird in einer gesonderten Verordnung des KM konkretisiert und umgesetzt werden. Hier sieht der Landeselternbeirat folgende Herausforderungen:

Die Datenverarbeitung an Schulen als öffentliche Stelle unterliegt zukünftig einer deutlich höheren Dokumentationspflicht; die normierte Meldung bei Unregelmäßigkeiten in der Datenverarbeitung hat innerhalb von 72 Stunden sehr schnell zu erfolgen; Verstöße sind mit drakonischen Strafen belegt.

Dies erfordert eine deutliche Professionalisierung im Umgang mit der IT und der Datenverarbeitung an Schulen und erfordert viel mehr Arbeitsstunden. Dieser Mehraufwand geht einher mit der Notwendigkeit der Weiterbildung aller Lehrer zum Thema, ganz besonders der an den Schulen dazu Beauftragten.

Die zukünftigen Regelungen müssen aus Sicht des LEB folgenden Eckpunkten gerecht werden:

- eine Überforderung der Schulen, insbesondere der kleinen Schulen, ist zu vermeiden
- die notwendige Mehrarbeit darf nicht zu Lasten der zugeteilten Lehrerwochenstunden gehen
- für die Schulen muss umfangreiche Rechtssicherheit bestehen
- der Mehraufwand für die Schulträger ist auszugleichen (Konnexität)

## Stellungnahme



- die Umsetzung muss handhabbar und lebbar sein, damit Schulen in ihren Gestaltungsmöglichkeiten nicht eingeschränkt werden, nur weil sie Sorge haben, evtl. gegen Datenschutzbestimmungen zu verstoßen

In allzu vielen Schulen ist die IT-Infrastruktur in Selbsthilfe entstanden und die Wartung und Betreuung durch Lehrer in selbst-ausbeuterischer Weise geleistet worden. Dies kann und darf vor dem Hintergrund der deutlich verschärften Anforderungen durch die EU-Datenschutzverordnung und das Landesdatenschutzgesetz nicht beibehalten werden.

Schließen möchten wir mit einem Dank an das Kultusministerium: Bei der Beratung des neuen Gesetzes hat der LEB vertrauensvoll mit den Juristen des Kultusministeriums zusammengearbeitet, weil bei dem erheblichen Umfang des Gesetzes ein detailliertes Durchdringen durch Nichtjuristen kaum möglich ist.

Für den 18. Landeselternbeirat

A handwritten signature in blue ink, appearing to read 'Dr. Rees', is written over a faint, larger blue signature.

Dr. Carsten T. Rees  
Vorsitzender

Freiburg, den 25.01.2018

## Landesinnungsverband des Schornsteinfegerhandwerks Baden-Württemberg



LIV Baden-Württemberg • Königstr. 94 • 89077 Ulm

Ministerium für Inneres, Digitalisierung  
und Migration Baden-Württemberg  
Abteilung 2 Verfassung, Kommunal- und  
Sparkassenwesen, Recht  
Willy-Brandt-Straße 41  
70173 Stuttgart

Ihre Zeichen

Ihre Nachricht vom

Unser Zeichen  
IM/ei.pe

Datum  
31.01.2018

### Stellungnahme zum Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzes und sonstiger Vorschriften an die Verordnung (EU) 2016/679

Sehr geehrte Frau  
sehr geehrter Herr

vielen Dank für die Gelegenheit, zu dem Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzes und sonstiger Vorschriften an die Verordnung (EU) 2016/679 Stellung zu nehmen.

Der Landesinnungsverband des Schornsteinfegerhandwerks Baden-Württemberg ist der zuständige Berufsverband für die Betriebe des Schornsteinfegerhandwerks und der Zusammenschluss der vier baden-württembergischen Innungen des Schornsteinfegerhandwerks, in denen derzeit 898 Mitglieder organisiert sind. Von diesen Mitgliedern verwalten 888 einen Kehrbezirk.

Die Anpassung des Datenschutzrechts in Baden-Württemberg an die Verordnung (EU) 2016/679 begrüßen wir und verknüpfen damit die Hoffnung, dass zukünftig innerhalb der einzelnen Bundesländer ein einheitliches Datenschutzniveau bestehen wird. Die Datenschutzgrundverordnung (DSGVO) regelt ab dem 25. Mai 2018 unmittelbar für alle die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten. Die DSGVO hat Öffnungsklauseln für den nationalen Gesetzgeber. Der Bund hat hierfür für bestimmte öffentliche und nicht öffentliche Stellen letztes Jahr durch die Neufassung des Bundesdatenschutzgesetzes (BDSG n.F.) Gebrauch gemacht. Letztendlich verbleibt für den Landesgesetzgeber daher nur ein enger Regelungsbereich für die Landesbehörden und die Kommunen, der mit dem vorliegenden Entwurf auch wahrgenommen wurde.

Die Umsetzung in Landesrecht erfolgt aus unserer Sicht im eröffneten Rahmen und wird von uns, mit Ausnahme der Anregungen zu einzelnen Regelungen, im Großen und Ganzen befürwortet.

...



**Anschrift**  
Königstraße 94  
89077 Ulm

**Kommunikation**  
Telefon 0731 93688-0  
Telefax 0731 93688-20  
Info@livulm.de

**Bankverbindung**  
Volksbank Ulm-Biberach eG  
IBAN DE49 6309 0100 0001 5710 01  
BIC ULMVDE66

[www.liv-schornsteinfeger.de](http://www.liv-schornsteinfeger.de)

Bevor wir auf die Kritikpunkte im Einzelnen eingehen wollen, möchten wir Ihnen die dahinterstehende datenschutzrechtliche Thematik kurz skizzieren. Im Schornsteinfegerhandwerk wird der bevollmächtigte Schornsteinfeger als Beliehener hoheitlich tätig und nimmt öffentliche Aufgaben wahr. Die Verwaltung des Kehrbezirks und die damit verbundene Führung des Kehr-  
buchs bedeutet, dass in diesem Zusammenhang verschiedene personenbezogene Daten vom bevollmächtigten Schornsteinfeger erhoben, verarbeitet und übermittelt werden. Die Datenverarbeitung der personenbezogenen Daten der betroffenen Personen durch den bevollmächtigten Schornsteinfeger erfolgt aufgrund des Schornsteinfeger-Handwerksgesetzes und ist damit datenschutzrechtlich auch legitimiert. Mit der Ausführung eines Bundesgesetzes wird der Anwendungsbereich des Bundesdatenschutzgesetzes n.F. eröffnet und das zukünftige Landesdatenschutzgesetz findet unmittelbar auf die Kkehrbuchführung keine Anwendung. Als Beliehene unterliegen die bevollmächtigten Schornsteinfeger der Aufsicht der Bestellungskörperschaften. Das Schornsteinfeger-Handwerksgesetz sieht als Aufsichtsmaßnahme u. a. vor, dass sich die Aufsicht führende Stelle das Kkehrbuch in digital verwertbarer Form vorlegen lassen kann. Für diese Landesbehörden bzw. Kommunalbehörden ist dann der Anwendungsbereich des Landesdatenschutzgesetzes eröffnet. Aus unserer Sicht deckt sich das Schutzniveau nicht vollständig.

An dieser Stelle knüpfen unsere Anregungen an, die wir Ihnen anhand der Vorschriften mit einem abweichenden Schutzniveau erläutern wollen.

#### § 6 Übermittlung personenbezogener Daten

Die Vorschrift regelt die Verantwortung für die Zulässigkeit der Übermittlung personenbezogener Daten und legt die anlassbezogene Pflicht zu Prüfung der Rechtmäßigkeit des Ersuchens fest.

Die bevollmächtigten Schornsteinfeger kommen in diesem Kontext in eine problematische Situation, die nur schwer lösbar ist. Grundsätzlich sind sie als öffentliche Stelle für die Zulässigkeit der Übermittlung verantwortlich.

Zwar geht die Verantwortung auf eine öffentliche Stelle über, die um Übermittlung von personenbezogenen Daten ersucht. Insoweit wäre bei Aufsichtsmaßnahmen die Aufsichtsbehörde in der Verantwortung. Dennoch haben die bevollmächtigten Schornsteinfeger als übermittelnde Stelle bei Anlass die Rechtmäßigkeit zu prüfen.

Der bevollmächtigte Schornsteinfeger unterliegt der Aufsicht der bestellenden Behörde. Als aufsichtsrechtliche Maßnahme kann sich diese Behörde das Kkehrbuch und die Kkehrbuchdaten in elektronischer Form und digital verwertbar übermitteln lassen. Hierdurch erhält die Behörde auf ihr Ersuchen eine Vielzahl von personenbezogenen Daten, für deren datenschutzkonforme Verwendung sie auch verantwortlich wäre. Grundsätzlich dürfte sie die personenbezogenen Daten lediglich zur Aufsicht verwenden.

Wir sehen an dieser Stelle die Gefahr der Nutzung der personenbezogenen Daten aus dem Kkehrbuch zu anderen Zwecken als der Kkehrbuchprüfung.

Die zuvor genannten Bedenken haben einen konkreten Hintergrund. Die Stadt Stuttgart hat als aufsichtsrechtliche Maßnahme digital verwertbare Kkehrbuchdaten angefordert. Anhand dieser Datengrundlage wurde für den Vollzug der Verordnung der Landesregierung über Betriebsbeschränkungen für kleine Feuerungsanlagen (Luftqualitätsverordnung-Kleinfeuerungsanlagen) eine neue Datenbank erstellt, die zur Kontrolle der Verbrennungsverbote verwendet wird.

Die Selbstverwaltungskörperschaften der Aufsicht führenden Behörden sind häufig Alleingesellschafter von Energieversorgern oder sonstigen Anbietern von Leistungen der Daseinsfürsorge.

Seite 3 Stellungnahme zum Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzes

Wir sehen die Gefahr, dass die personenbezogenen Daten auch für die Markterschließung oder die strategische Betriebsplanung eingesetzt und damit zu einem anderen Zweck verwendet werden.

Das Spannungsverhältnis zwischen Prüfpflicht und Aufsicht muss klarstellend dahingehend gelöst werden, dass dem prüfenden und einen Verstoß rügenden bevollmächtigenden Schornsteinfeger kein aufsichtsrechtlicher Nachteil entstehen darf. Hier sollte eine Klarstellung ins Gesetz aufgenommen werden.

§ 13 Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken

Das LDSG n.F. richtet sich an die Kommunen, und von kommunaler Seite werden immer wieder Wünsche nach gebäudescharfen Daten an den Landesinnungsverband herangetragen. Das Anonymisieren von personenbezogenen Daten bei gebäudescharfen Daten würde ohne eine aggregierte Zusammenstellung in bestimmten Gemeindegebieten einen Rückschluss auf einzelne Anlagenbetreiber zulassen. Die Anonymisierung kann daher zur Sicherstellung angemessener und spezifischer Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Personen nicht ausreichen, wenn aufgrund der Art und Anzahl von beispielsweise nur einmal vorhandener Anlagen ein konkreter Rückschluss auf die Identität des Anlagenbetreibers gezogen werden kann.

Hier könnte entsprechend § 27 Abs. 1 Satz 2 BDSG n.F. ein Verweis auf § 3 LDSG n.F. Abhilfe schaffen. Eine angemessene und spezifische Maßnahme zur Wahrung der Interessen der betroffenen Person könnte dann die aggregierte Zusammenstellung der personenbezogenen Daten als eine Form der Pseudonymisierung (vgl. § 3 Nr. 6 LDSG n.F.) sein.

Ebenso möchten wir auf die Bedenken und Anregungen des Baden-Württembergischen Handwerkstags verweisen, dessen Argumente wir in vollem Umfang mittragen.

Wir bitten Sie um Berücksichtigung unserer Anregungen und stehen Ihnen für Fragen selbstverständlich gerne zur Verfügung.

Freundliche Grüße

  
Stefan Eisele  
Präsident

  
Stephan Perschke  
Geschäftsführer  
Rechtsanwalt (Syndikusrechtsanwalt)



## **Stellungnahme der Landesrektorenkonferenz Baden-Württemberg zum Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679**

### **1. § 8 – Beschränkung der Informationspflicht**

Im Bereich der wissenschaftlichen Forschung kann die Erfüllung der Informationspflichten nach Art. 13, 14 DS-GVO zu einer Verfälschung des Forschungsergebnisses führen. Beispielsweise gilt dies für den Bereich der psychologischen Forschung, wenn es darum geht, menschliche Verhaltensweisen wissenschaftlich zu untersuchen. Sobald betroffene Personen wissen, dass sie Teil an einer wissenschaftlichen Untersuchung sind, ist nicht auszuschließen, dass sie ihre Verhaltensweisen (ggf. auch unbewusst) anpassen und so kein unverfälschtes Ergebnis der wissenschaftlichen Forschung mehr möglich ist.

Dies ist nicht auf psychologische Forschung begrenzt, sondern kann bspw. auch der Fall sein, wenn im Bereich der Mobilitätsforschung z.B. Fußgängerströme per Video aufgezeichnet werden sollen, um Bewegungsprofile zu erkennen. Wer weiß, dass genau das analysiert wird, wird möglicherweise gerade nicht mehr die Abkürzung über die Grünfläche nehmen.

Aus diesem Grund muss es im Interesse des Wissenschaftsstandorts Baden-Württemberg möglich sein, in diesen spezifischen Fällen Einschränkungen von der Informationspflicht vorzusehen. Die Möglichkeit dazu ergibt sich aus Art. 23 Abs. 1 lit. e DS-GVO.

Die Einschränkung der Informationspflicht, die sich direkt aus Art. 14 Abs. 5 lit. b DS-GVO ergibt, beschränkt sich darauf, dass personenbezogene Daten nicht bei der betroffenen Person erhoben werden, die Erteilung der Information sich als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordert und macht somit nachstehend vorgeschlagene Regelung der Einschränkung der Informationspflicht nicht entbehrlich.

Vorgeschlagen wird daher **eine Ergänzung** in § 8 Abs. 1 Satz 1 des Entwurfs zum LDSG, Stand 14.12.2017 (LDSG-E):

„5. die Information den wissenschaftlichen Forschungszweck unmöglich machen oder ernsthaft beeinträchtigen würde“

## **2. § 9 – Beschränkung des Auskunftsrechts**

### **2.1. Folgeänderung**

Folgt man dem vorstehenden Vorschlag der Ergänzung von § 8 Abs. 1 Satz 1 LDSG-E durch die Nr. 5 wäre der Verweis in § 9 Abs. 1 LDSG-E auf die Fallgestaltungen des § 8 Abs. 1 Satz 1 Nr. 1 – 4 LDSG-E zu beschränken. Einschränkungen des Art. 15 DS-GVO bei der Verarbeitung zu wissenschaftlichen oder historischen Forschungszwecken werden bereichsspezifisch in § 13 Abs. 4 LDSG-E geregelt.

### **2.2. Präzisierung des Auskunftersuchens**

Die Regelung des Absatz 2 wird begrüßt. In der Praxis wird sich die Frage stellen, was „eine große Menge von Informationen“ ist. Im Interesse der Rechtssicherheit wäre eine Präzisierung, was der Landesgesetzgeber hierunter versteht, wünschenswert.

## **3. § 13 – Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken**

### **3.1. Erforderlichkeit einer Rechtsgrundlage**

§ 13 enthält in Absatz 1 nur eine Rechtsgrundlage für die Verarbeitung besonderer Kategorien personenbezogener Daten für wissenschaftliche oder historische Forschungszwecke. Die Verarbeitung von nicht unter Artikel 9 der DS-GVO fallende Daten richtet sich – so ausdrücklich die Gesetzesbegründung – unmittelbar nach der DS-GVO.

Dabei kommen insbesondere in Betracht Art. 6 Abs. 1 lit. a DS-GVO (Forschungsvorhaben, bei denen die Probanden einwilligen), Art. 6 Abs. 1 lit. e in Verbindung mit Absatz 3 DS-GVO und Art. 6 Abs. 1 lit. f DS-GVO.

Bei den Forschungsvorhaben, bei denen Daten ohne Einwilligung der betroffenen Personen verarbeitet werden (müssen), die keine Daten im Sinne von Art. 9 DS-GVO sind, käme demnach als Rechtsgrundlage Art. 6 Abs. 1 lit. e in Verbindung mit Absatz 3 lit. b DS-GVO in Verbindung mit § 4 LDSG-E in Betracht. § 4 LDSG-E ist – so auch die Gesetzesbegründung (S. 14) – eine „allgemeine Rechtsgrundlage für Datenverarbeitung mit **geringer** Eingriffsintensität in die Rechte der betroffenen Personen“ (Hervorhebung durch den Unterzeichner).

Bei Forschungsvorhaben können jedoch auch Daten, die nicht Art. 9 DS-GVO unterfallen, in erheblichem Umfang oder in einer Art (z.B. Einsatz von Videotechnologie, Forschung mit Sprachaufzeichnungen) verarbeitet werden, die zu einer **großen** Eingriffsintensität führen.

Ob von Seiten der Hochschulen für eine solche Datenverarbeitung, die im Rahmen ihrer Aufgabe erfolgt, überhaupt auf Art. 6 Abs. 1 lit. f DS-GVO zurückgegriffen werden könnte, ist in Frage zu stellen. Denn Art. 6 Abs. 1 lit. f DS-GVO gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommenen Verarbeitungen.

Für den Fall von Forschungsvorhaben, bei denen Daten ohne Einwilligung der betroffenen Personen verarbeitet werden (müssen), ist daher eine normenklare und hinreichend bestimmte Rechtsgrundlage erforderlich. Die Möglichkeit für den Landesgesetzgeber eine solche zu schaffen, ergibt sich aus Art. 6 Abs. 3 lit. b, Abs. 2 DS-GVO.

So sieht der Entwurf aus NRW vom 14.12.2017 eine solche Rechtsgrundlage in § 16 DSGVO NRW-E für die Forschung vor. Auch der Entwurf aus Brandenburg (Drucksache 6/7365) sieht in § 24 Abs. 1 Satz 1 Alt. 1 BbgDSG-E eine solche Rechtsgrundlage vor.

Hier gilt es, für den Wissenschaftsstandort Baden-Württemberg Nachteile zu vermeiden.

### **3.2. „Erhebliches“ Überwiegen schwächt Forschungsstandort Baden-Württemberg**

Ergänzt man den vorstehenden Punkt in § 13 Abs. 1 LDSG-E, ist als Folgeänderung eine Umformulierung notwendig, mit der sichergestellt ist, dass zumindest bei anderen Daten als Daten im Sinne von Art. 9 DS-GVO die Interessen der öffentlichen Stelle nicht „erheblich“ überwiegen müssen, was der notwendigen und auch vom Gesetzgeber gewollten Privilegierung der Wissenschaft zuwiderlaufen würde.

Aber auch **unabhängig** von der vorgeschlagenen Änderung unter 3.1. und alleine schon im Hinblick auf die Verarbeitung besonderer Arten personenbezogener Daten ist fraglich, ob das Kriterium der Erheblichkeit sachgerecht ist. Die Öffnungsklausel des Art. 9 Abs. 2 lit. j DS-GVO stellt keine derartige Anforderung an die mitgliedstaatliche Vorschrift. Danach muss die nationale Ausnahmvorschrift für Forschungszwecke in angemessenem Verhältnis zu dem verfolgten Ziel stehen, den Wesensgehalt des Rechts auf Datenschutz wahren und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsehen. Diesen Anforderungen wird bereits dadurch ausreichend Rechnung getragen, dass § 13 Abs. 1 LDSG-E ein Überwiegen der Interessen der Betroffenen verlangt und voraussetzt, dass der Forschungszweck auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann. Auch durch die Vorgaben zur Anonymisierung und Pseudonymisierung in § 13 Abs. 2 LDSG-E werden angemessene weitere Maßnahmen zum

Schutz der betroffenen Personen getroffen. Schließlich ist durch § 3 LDSG-E sichergestellt, dass die Betroffenen ausreichend geschützt werden. Die Vorschrift ist nach ihrem Sinn und Standort auf alle Verarbeitungen - und damit auch solchen nach § 13 LDSG-E - anwendbar und soll ausweislich der Gesetzesbegründung (S.13) gerade auch der Umsetzung von Art. 9 DS-GVO dienen.

Artikel 9 Abs. 4 DS-GVO erlaubt den Mitgliedstaaten zusätzliche Bedingungen, einschließlich Beschränkungen bei der Verarbeitung besonderer Kategorien personenbezogener Daten einzuführen, soweit die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten betroffen sind (siehe auch Erwägungsgrund 53). Wenn der Gesetzgeber im Rahmen einer Interessenabwägung die Erheblichkeit betonen will, so wäre diese einzuschränken auf genetische, biometrische oder Gesundheitsdaten.

Hält der Gesetzgeber an der uneingeschränkten Interessensabwägung der Erheblichkeit ohne Einschränkung auf ggf. genetische, biometrische oder Gesundheitsdaten fest, wird der Forschungsstandort Baden-Württemberg geschwächt. Forschungsvorhaben, die im Ergebnis in der Wertung der Interessenabwägung in Baden-Württemberg nicht möglich sind, weil die Interessen der forschenden Stelle nicht erheblich überwiegen, werden verlagert in Bundesländer, deren derzeit ersichtliche landesrechtliche Regelungen diese weitergehenden Anforderungen einer Erheblichkeit bei der Interessensabwägung nicht vorsehen (wie in Bayern, Nordrhein-Westfalen und Brandenburg).

### 3.3. Formulierungsvorschlag für § 13 Abs. 1 LDSG-E

Insgesamt werden aus den soeben dargestellten zwei Punkten folgende Änderungen in § 13 Abs. 1 LDSG-E vorgeschlagen (Ergänzungen in fett gedruckt, Streichungen markiert):

(1) Öffentliche Stellen dürfen **personenbezogene Daten einschließlich** besondere Kategorien personenbezogener Daten für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke verarbeiten, wenn die Zwecke auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden können und die Interessen der öffentlichen Stelle an der Verarbeitung die ~~Interessen~~ **schutzwürdigen Belange** der betroffenen Person an einem Ausschluss der Verarbeitung ~~erheblich~~ überwiegen. Besondere Kategorien personenbezogener Daten sind die in Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 genannten Daten.

Durch die vorgeschlagene Verwendung des Begriffs „schutzwürdige Belange“ wird auf eine in § 5 Abs. 2 LDSG-E verwendete Terminologie zurückgegriffen.

### 3.4. Frühestmögliche Anonymisierung aller Daten

Nach der DS-GVO sind personenbezogene Daten zu vermeiden (Art. 5 Abs. 1 lit. c DS-GVO) und zu löschen, wenn sie nicht mehr benötigt werden (Art. 17 Abs. 1 lit. a DS-GVO). Diesen schon bislang im Datenschutzrecht normierten Grundsätzen trug schon § 35 LDSG Rechnung, indem er für alle personenbezogenen Daten die frühestmögliche Anonymisierung vorsah.

Ausweislich der Gesetzesbegründung zu § 13 LDSG-E (S. 24) soll nun die Anonymisierung nur für Daten im Sinne von Art. 9 DS-GVO gelten, während für die anderen die Pseudonymisierung gilt. Für die unterschiedliche Behandlung ist, gerade vor den eingangs erwähnten Grundsätzen der DS-GVO, kein Grund ersichtlich.

Es wird daher vorgeschlagen, § 13 Abs. 2 LDSG-E wie folgt zu ändern (Streichung markiert):

(2) ~~Die besonderen Kategorien~~ Personenbezogene Daten sind zu anonymisieren, sobald dies nach dem Forschungs- oder Statistikzweck möglich ist. Bis zur Anonymisierung sind die Merkmale gesondert zu speichern, mit denen Einzelangaben einer bestimmten oder bestimmbarer Person zugeordnet werden können. Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungszweck dies erfordert.

### 3.5. Veröffentlichung personenbezogener Daten durch wissenschaftliche Forschung betreibende öffentliche Stellen

Wissenschaftspolitisch ist es gewollt, dass Forschungsdaten und wissenschaftliche Publikationen im Wege des Open Access zur Verfügung gestellt werden<sup>1</sup>. Baden-Württemberg hat als eines der wenigen Bundesländer bisher mit dem „Fachkonzept zur Weiterentwicklung der wissenschaftlichen Infrastruktur“<sup>2</sup> eine Open Access-Strategie vorgestellt, die auch Konzepte zum Forschungsdatenmanagement im allgemeinen enthält und die Klärung auch datenschutzrechtlicher Fragestellungen umfassen soll.

Im Europäischen Forschungsraum wird Open Access u.a. durch „Horizont 2020“, dem Rahmenprogramm der Europäischen Union für Forschung und Innovation, befördert, das schon heute Regeln zur Publikation auch von Forschungsdaten umfasst. Zunehmend verpflichten

---

<sup>1</sup> Siehe Ministerium für Wissenschaft, Forschung und Kunst Baden-Württemberg, „E-Science – Wissenschaft unter neuen Rahmenbedingungen; Fachkonzept zur Weiterentwicklung der wissenschaftlichen Infrastruktur in Baden-Württemberg“, insbesondere Teil A, Kapitel 2.3 und 2.4.; abrufbar unter [https://mwk.baden-wuerttemberg.de/fileadmin/redaktion/m-mwk/intern/dateien/pdf/Forschung/066\\_PM\\_Anlage\\_E-Science\\_Web.pdf](https://mwk.baden-wuerttemberg.de/fileadmin/redaktion/m-mwk/intern/dateien/pdf/Forschung/066_PM_Anlage_E-Science_Web.pdf). Siehe außerdem: Bundesministerium für Bildung und Forschung, „Open Access in Deutschland – Die Strategie des Bundesministeriums für Bildung und Forschung“; abrufbar unter [https://www.bmbf.de/pub/Open\\_Access\\_in\\_Deutschland.pdf](https://www.bmbf.de/pub/Open_Access_in_Deutschland.pdf)

<sup>2</sup> siehe Fußnote 1

Forschungsmittelgeber die Drittmittelempfänger, neben den Forschungsergebnissen auch die primären (oft personenbezogenen) Forschungsdaten zu veröffentlichen.

Weder mit § 13 Abs. 3 LDSG-E noch mit einer anderen Norm sieht der vorliegende Entwurf eine Ermächtigungsnorm vor, aufgrund derer personenbezogene Forschungsdaten ohne Einwilligung veröffentlicht werden dürfen.

Das Einholen und Verwalten der Einwilligung stellt einen erheblichen administrativen Aufwand dar und ist zudem oft gar nicht möglich, weil zwar die Forschungsdaten personenbeziehbar sind, aber von den Betroffenen keine Kontaktdaten vorhanden sind und das Recherchieren und Einholen der Einwilligungen einen enormen Aufwand bedeuten würde.

Es wird daher vorgeschlagen, eine normenklare Rechtsvorschrift zu schaffen, die die Veröffentlichung auch personenbezogener Forschungsdaten im Sinne von Artikel 6 Abs. 1 lit. e in Verbindung mit Artikel 6 Abs. 3 DS-GVO - ggf. unter zu definierenden Rahmenbedingungen und Beschränkungen - erlaubt.

So könnten zukunftsweisende (datenschutz)rechtliche Rahmenbedingungen zur Durchsetzung von Open Access geschaffen werden und damit auch die Möglichkeit, einer Verpflichtung zur Veröffentlichung seitens der Drittmittelgeber nachzukommen.

Der Verzicht auf eine solche Ermächtigungsnorm könnte den Forschungsstandort Baden-Württemberg dann benachteiligen, wenn andere Bundesländer oder europäische Länder Regelungen vorsehen, die die Veröffentlichung von personenbezogenen Forschungsdaten ohne eine Einwilligung gestatten.

#### **4. § 14 Abs. 8 – Zuverlässigkeitsüberprüfung**

Nach dem Allgemeinen Teil der Gesetzesbegründung unter II. 1. d) (S. 3 f.) soll für Zuverlässigkeitsprüfungen „von Bewerberinnen und Bewerbern für öffentliche Leistungen sowie Besucherinnen und Besuchern eine eigene gesetzliche Grundlage geschaffen werden. Die öffentliche Stelle ist daher in Zukunft nicht mehr auf eine Einwilligung der betroffenen Person angewiesen [...]“.

Nach dem Wortlaut von § 14 Abs. 8 LDSG-E und der Gesetzesbegründung dazu bedarf es jedoch der Einwilligung der betroffenen Person. Hier ist zum einen in sich die Gesetzesbegründung widersprüchlich. Es entspricht auch nicht der Systematik des Datenschutzes, dass laut Gesetzesbegründung zusätzlich zu der Anforderung „Erforderlichkeit“ eine Einwilligung verlangt wird (so die Gesetzesbegründung zu Absatz 8).

Zum anderen ist die Einwilligung als Zulässigkeitsvoraussetzung problematisch: Mitarbeiter von Unternehmen und anderen Organisationen sowie die eigenen Mitarbeiter (diese könnten unter „sonstige Personen“ im Sinne des § 14 Abs. 8 LDSG-E fallen) müssen vielfach im Rahmen ihrer Tätigkeit in sicherheitsrelevante Bereiche gelangen. Sie haben keine echte Wahl, einzuwilligen oder nicht, weil sie andernfalls ihre Tätigkeit nicht ausüben können. Damit sind aber die Voraussetzungen an eine Einwilligung nicht gewahrt. Vielmehr bedarf es einer Ermächtigungsnorm für die Überprüfung der Zuverlässigkeit, die nicht die Einwilligung als Zulässigkeitsvoraussetzung hat.

#### **5. § 28 – Strafvorschrift**

In § 28 Abs. 1 Nr. 1 lit a LDSG-E wird vorgeschlagen, statt der Einzelbegriffe den Begriff „verarbeitet“ zu verwenden und damit die Begrifflichkeit des Art. 4 Nr. 2 DS-GVO.

#### **6. Datengeheimnis**

Das LDSG-E enthält nicht mehr wie früher eine Definition des Datengeheimnisses, welches aber in § 7 LDSG-E ausdrücklich genannt wird. Die Gesetzesbegründung führt aus, die DS-GVO setze die Einhaltung des Datengeheimnisses als Schutzmaßnahme voraus. Unklar ist damit aber, ob beschäftigte Personen auf das Datengeheimnis verpflichtet werden müssen oder ob es qua lege gilt. Im Interesse eines effizienten Verwaltungsvollzugs wäre es, wenn das Datengeheimnis - wie bislang - gesetzlich normiert wäre und kein Verwaltungsaufwand durch eine individuelle Verpflichtung beschäftigter Personen entstünde.

Es wird daher vorgeschlagen, das Datengeheimnis wie bislang ausdrücklich im LDSG zu regeln. Die Möglichkeit dazu ergibt sich aus Art. 6 Abs. 2 DS-GVO.

Stuttgart, 30. Januar 2018

---

**Von:** kontakt@lsb-bw.de  
**Gesendet:** Freitag, 26. Januar 2018 11:19  
**An:** Registratur 2 (IM)  
**Cc:**  
**Betreff:** Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679

Sehr geehrte Damen und Herren,  
die Unterlagen zu dem o.g. Entwurf wurde den Mitgliedern des Landesschulbeirats zugesandt; es gab keine Einwände.

Mit freundlichen Grüßen

Ingeborge Schöffel-Tschinke  
• Vorsitzende –  
Weingartenstraße 21, 77948 Friesenheim

[kontakt@lsb-bw.de](mailto:kontakt@lsb-bw.de) [www.lsb-bw.de](http://www.lsb-bw.de)



LSV Baden-Württemberg e.V. / Fritz-Walter-Weg 19 / 70372 Stuttgart

Ministerium für Inneres, Digitalisierung und Migration  
Baden-Württemberg

Bernd Röber  
Referent für Sportpolitik

per Mail

17.01.2018

**Aktenzeichen 2-0557.8/1**

**Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679**

Sehr geehrte Frau  
sehr geehrte Damen und Herren,

haben Sie vielen Dank für Ihr Schreiben vom 19.12.2017 zu obigem Sachverhalt und der Möglichkeit, im Rahmen der Verbändeanhörung Stellung nehmen zu können.

Der Landessportverband Baden-Württemberg e. V. hat keine Änderungsvorschläge und kann dem vorgelegten Entwurf uneingeschränkt folgen.

Bitte lassen Sie uns freundlicherweise den finalen Gesetzentwurf zur Kenntnis zukommen. Dafür vorab vielen Dank!

Mit freundlichen Grüßen

Bernd Röber  
Referent für Sportpolitik

Landessportverband  
Baden-Württemberg e. V.  
Fritz-Walter-Weg 19  
70372 Stuttgart

[www.lsvbw.de](http://www.lsvbw.de)

BW Bank  
IBAN DE02 6005 0101 0001 2736 30  
BIC SOLADEST600

VR 3310 Amtsgericht Stuttgart  
Steuer-Nr. 99059/04169



Ministerium für Inneres, Digitalisierung und  
Migration  
Baden-Württemberg  
Postfach 10 34 65  
70029 Stuttgart

30.01.2018

**Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und  
sonstiger Vorschriften an die Verordnung (EU) 2016/679**

Ihr Schreiben vom 19.12.2017, Az.: 2-0557.8/1

Sehr geehrte Damen und Herren,

wir bedanken uns für die Gelegenheit zur Stellungnahme zu o.g. Entwurf und erlauben  
uns nachfolgende Anmerkungen:

I. Allgemeine Anmerkungen:

Der Datenschutz ist in der Digitalisierungsstrategie des Landes Baden-Württemberg als Querschnittsthema verankert. Der Datenschutz ist ein hohes Gut. Zugleich schreitet die Digitalisierung der Verwaltung stetig voran. Ein Prozess, der zwangsläufig auch neue Verwaltungsabläufe innerhalb der Verwaltung, aber auch zwischen den Ebenen von Bund, Land und Kommunen mit sich bringen wird. Deshalb muss es gelingen, dass Anforderungen des Datenschutzes gleichwohl wie die der Digitalisierung in einem gedeihlichen Verhältnis zum Nutzen des Bürgers abgewogen werden.

Um das Innovationspotential von digitalisierten Verwaltungsabläufen umfänglich ausschöpfen zu können, bedarf es insofern einer entsprechenden "Experimentierklausel": Pilotprojekte sollen mehr rechtlichen Spielraum erhalten, um neue Lösungen zu erproben und rechtlichen Anpassungsbedarf zu identifizieren. Wir fordern daher die Aufnahme einer „Experimentierklausel“ sowie nach 2 Jahren eine Evaluierung des novellierten Landesdatenschutzgesetzes.

## II. Anmerkungen im Einzelnen:

### Zu § 2 Absatz 1 Nr. 3 Landesdatenschutzgesetz-neu (LDSG-neu)

Der Wortlaut von § 2 Abs. 1 Nr. 3 LDSG-neu entspricht Artikel 1 Absatz 1 der Richtlinie (EU) 2016/680.

Da insbesondere Kreis- und Ortpolizeibehörden in Baden-Württemberg die Aufgabe der Abwehr von Gefahren für die öffentliche Sicherheit zukommt, sollte in der Gesetzesbegründung klargestellt werden, ob diese Aufgaben vom Anwendungsbereich des LDSG-neu umfasst sind. Bislang stellt die Gesetzesbegründung lediglich auf den Wortlaut der vorgenannten Richtlinie ab. Eine Klarstellung, ob hier formal nach Behördenbegriff oder materiell nach der wahrgenommenen Aufgabe differenziert werden soll, wäre wünschenswert. Die Abgrenzungsproblematik könnte durch eine Ergänzung der Begründung entschärft werden, indem die jeweiligen Anwendungsbereiche und -grenzen deutlicher, evtl. sogar beispielhaft, herausgearbeitet werden.

Nach dem vorliegenden Entwurf unterliegen grundsätzlich alle Ämter einer Behörde im Land dem Anwendungsbereich des LDSG-neu. Leitet ein Amt einer Behörde ein Ordnungswidrigkeitenverfahren ein, ist in diesem Zusammenhang anstelle des LDSG-neu das Gesetz zur Umsetzung der Richtlinie (EU) 2016/680 anzuwenden. In der Konsequenz würde dies bedeuten, dass die Ämter einer Behörde je nach Tätigkeit, unterschiedliche Vorschriften anzuwenden haben. Dies würde in der Praxis zu erheblichen Abgrenzungs- und Umsetzungsschwierigkeiten führen. Wir bitten daher, um eine möglichst einheitliche Regelung.

### Zu § 2 Absatz 4 LDSG-neu

Die bei der Stellungnahme zu § 2 Abs. 1 Nr. 3 LDSG-neu geschilderte Abgrenzungsproblematik tritt an dieser Stelle erneut auf, da hier der Anwendungsbereich der Richtlinie (EU) 2016/680 in der Gesetzesbegründung nur noch auf die „Polizei“ bezogen wird. Unklar ist, ob hiermit die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit insgesamt gemeint sein sollen.

In § 29 LDSG-neu ist demgegenüber von „Polizeibehörden und Polizeivollzugsdienst“ die Rede. Hier sollte ein Gleichlauf der Begrifflichkeiten erreicht werden.

Gemäß § 2 Abs. 4 Satz 2 LDSG-neu gelten die Artikel 30, 35 und 36 der Verordnung(EU) 2016/679 nur, soweit die Verarbeitung personenbezogener Daten automatisiert erfolgt oder die Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen. In der Begründung zu § 2 Abs. 4 Satz 2 LDSG-neu wird darauf verwiesen, dass auch für die nicht-elektronische Datenverarbeitung die Geltung der Verordnung angeordnet wird. Zugleich wird bei der nicht-elektronischen Datenverarbeitung u. a. auf die Pflicht zur Führung eines Verzeichnisses (Artikel 30 Verordnung(EU) 2016/679) verzichtet. Dabei wird übersehen, dass § 2 Abs. 4 Satz 2 LDSG-neu von einem "Dateisystem" spricht, das entsprechend der Definition in Artikel 4 Nr. 6 der Verordnung (EU) 2016/679 auch die nicht-

elektronische Verarbeitung mit einbezieht. Bislang waren nach § 11 LDSG-alt nur die automatisierten Verfahren einbezogen. Demnach sind künftig alle "Verarbeitungstätigkeiten" erfasst und dazu zählen auch die nicht-elektronischen.  
Wir bitten daher dahingehend um Klarstellung, dass auch künftig lediglich automatisierte Verfahren einbezogen werden.

Zu § 5 Absatz 1 Nr. 1 LDSG-neu

Mit dem Ziel des Gleichlaufs mit dem Bundesdatenschutzgesetz (BDSG) sollte auch in das LDSG-neu die Zweckänderung zur Wahrung erheblicher Belange des Gemeinwohls aufgenommen werden.

Generell begrüßenswert bei den Tatbeständen der Zweckänderung wäre ein Gleichlauf mit dem novellierten (BDSG-neu), um eine weitere Rechtszersplitterung zwischen EU-Datenschutz-Grundverordnung, BDSG-neu und LDSG-neu zu vermeiden und damit eine höhere Anwender-freundlichkeit zu erreichen.

Wir schlagen daher vor, in § 5 Absatz 1 Nr. 1 LDSG-neu zusätzlich die Wörter „zur Wahrung erheblicher Belange des Gemeinwohls“ aufzunehmen.

Zu § 5 Absatz 1 letzter Halbsatz LDSG-neu

Nach der Gesetzesbegründung dient die Regelung in § 5 LDSG-neu dazu, die Tatbestände zu regeln, in denen gemäß Artikel 6 Absatz 4 der Verordnung (EU) 2016/679 eine Verarbeitung personenbezogener Daten für andere Zwecke eine „notwendige und verhältnismäßige“ Maßnahme zum Schutz der in Artikel 23 Absatz 1 der Verordnung (EU) 2016/679 genannten Ziele darstellt. Artikel 23 Absatz 1 der Verordnung (EU) 2016/679 sieht vor, dass durch Rechtsvorschriften der [...] Mitgliedstaaten Pflichten und Rechte [...] im Wege von Gesetzgebungsmaßnahmen beschränkt werden, sofern eine solche Beschränkung [...] in einer demokratischen Gesellschaft „eine notwendige und verhältnismäßige Maßnahme“ darstellt.

Ob es sich um eine notwendige und verhältnismäßige Maßnahme handelt, ist damit ein Beurteilungsauftrag an den Gesetzgeber bei der Schaffung entsprechender gesetzlicher Tatbestände und nicht an die Verwaltung bei der Gesetzesanwendung gerichtet. Werden vom Gesetzgeber entsprechende Tatbestände geschaffen, so wurde bereits seitens des Gesetzgebers die Wertung vorgenommen, dass es sich um eine notwendige und verhältnismäßige Maßnahme handelt. Dies sollte daher keine zusätzliche Tatbestandsvoraussetzung im Rahmen von § 5 Abs. 1 LDSG-neu darstellen.

Auch das novellierte BDSG sieht eine solche zusätzliche Voraussetzung nicht vor. Sollte hiermit lediglich auf den datenschutzrechtlichen Grundsatz der Erforderlichkeit abgestellt werden, so ist dieser Zusatz wegen dessen bereits europarechtlich angeordneter Geltung zu streichen.

Wir regen daher an, in § 5 Absatz 1 letzter Halbsatz LDSG-neu „soweit die Verarbeitung notwendig und verhältnismäßig ist“ zu streichen.

### Zu § 5 Absatz 3 LDSG-neu

Wir schlagen vor, vor „eine Information“ in Satz 1 die Wörter „Abweichend von Artikel 13 der Verordnung (EU) 2016/679“ aufzunehmen. Mit dem Zusatz würde bereits im Gesetzestext klargestellt, dass von dem Grundsatz der Informationspflicht nach Artikel 13 der Verordnung (EU) 2016/679 abgewichen wird. Dies würde die Anwendung und Lesbarkeit des neuen Rechts im Gesamtzusammenhang mit den Regelungen der EU-Datenschutz-Grundverordnung erleichtern.

### Zu § 6 LDSG-neu

§ 6 LDSG-neu ist überschrieben mit „Übermittlung personenbezogener Daten“, regelt jedoch nicht die Übermittlung selbst, sondern lediglich die Verantwortung bei der Übermittlung. In der Gesetzesbegründung zum LDSG-neu (Seite 17) wird ausgeführt, dass die Übermittlung personenbezogener Daten nach der Verordnung (EU) 2016/679 wie eine Zweckänderung behandelt wird; ihre Zulässigkeit ist somit nach Artikel 6 Absätze 1, 3 und 4 der Verordnung (EU) 2016/679 sowie § 5 zu beurteilen. Angelehnt an die Gesetzesbegründung sollte bereits im Gesetzestext vorangestellt werden, wonach sich die Zulässigkeit der Übermittlung richtet. Dies stellt lediglich einen Hinweis auf das geltende EU-Recht dar, ohne dieses zu wiederholen.

Wir regen daher an, einen neuen Absatz 1 einzufügen: „Die Zulässigkeit der Übermittlung richtet sich nach Artikel 6 Absätze 1, 3 und 4 der Verordnung (EU) 2016/679 und § 5 dieses Gesetzes.“ Die bisherigen Absätze 1 und 2 würden dann zu Absatz 2 und 3.

Generell wäre eine Bezugnahme auf relevante Vorschriften der EU-Datenschutz-Grundverordnung wünschenswert, wo dies europarechtlich ohne Verstoß gegen das Wiederholungsverbot zulässig ist. Dies würde generell die Verzahnung des LDSG-neu mit der EU-Datenschutz-Grundverordnung verdeutlichen und die Anwendung des neuen Rechtsregimes für Verwaltung und Bürgerinnen und Bürger vereinfachen. Auch Erwägungsgrund 8 der Verordnung (EU) 2016/679 erlaubt eine solche Vorgehensweise, wenn in dieser Verordnung Präzisierungen oder Einschränkungen ihrer Vorschriften durch das Recht der Mitgliedstaaten vorgesehen sind. Dann können die Mitgliedstaaten „Teile dieser Verordnung in ihr nationales Recht aufnehmen, soweit dies erforderlich ist, um die Kohärenz zu wahren und die nationalen Rechtsvorschriften für die Personen, für die sie gelten, verständlicher zu machen.“

Auch bezieht sich der bisherige § 16 LDSG nur auf Übermittlungen an Stellen innerhalb des öffentlichen Bereiches, während für Übermittlungen aus dem öffentlichen Bereich heraus an private Stellen bislang § 18 LDSG umfängliche Regelungen trifft.

§ 6 Abs. 1 LDSG-neu regelt die Verantwortung für Übermittlungen an den privaten Bereich und an den öffentlichen Bereich unterschiedlich. Wird an eine öffentliche Stelle aufgrund eines Ersuchens übermittelt, so trägt grundsätzlich die ersuchende Behörde die Verantwortung. Wird hingegen an eine private Stelle übermittelt, so trägt nach § 6 Abs. 1 Satz 1 LDSG-neu alleine die übermittelnde Behörde die Verantwortung. Während aber im Einzelfall bei gegebenem Anlass bei Übermittlungen an eine öffentliche Stelle die Rechtmäßigkeit des Ersuchens zu prüfen ist, obliegt der übermittelnden Behörde bei einem

Übermittlungersuchen einer privaten Stelle diese Pflicht nicht. Eine Darstellung in der Begründung wäre wünschenswert, warum § 6 LDSG-neu die bisherige Unterscheidung zwischen Übermittlungen an öffentliche und an nichtöffentliche Stellen aufgibt. Demgegenüber regelt das novellierte BDSG in § 25 Abs. 2 ausdrücklich die Voraussetzungen, unter denen die Übermittlung an nichtöffentliche Stellen zulässig ist. Warum eine solche Regelung sich im LDSG-neu nicht mehr wiederfindet, bleibt unklar.

Zu § 8 LDSG-neu

Wir regen an, die landesrechtliche Regelungen an die verwaltungsvereinfachenden Regelungen des BDSG anzugleichen.

§ 12 Abs. 1 LDSG-neu

Dort heißt es: „Personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen und die von der zur...“  
Das Wörtchen „von“ ist zu streichen. Es geht um Daten, die dem Normadressaten übermittelt oder auf sonstige Weise bekannt gegeben wurden, die also ihm zugeflossen sind. Für diese zugeflossenen Informationen wird hier eine im Vergleich zu § 5 verengte Zweckbindung vorgesehen, die sich auf die Sphäre des Normadressaten als Informationsempfänger bezieht, nicht hingegen auf eine evtl. Funktion als Informationslieferant, wie es durch das Wörtchen „von“ vermittelt wird.

Zu § 17 LDSG-neu

Es wird begrüßt, dass das Tatbestandsmerkmal der tatsächlichen Anhaltspunkte für eine Gefährdung entfällt.  
Unklar erscheint die in § 17 Abs. 6 LDSG-neu geforderte zusätzliche Mitteilungspflicht an den oder die Datenschutzbeauftragte, die neben die von der EU-Datenschutz-Grundverordnung (Art. 35) geforderte Datenschutzfolgenabschätzung tritt. Auch nach Art. 35 Abs. 2 der Verordnung (EU) 2016/279 hat der Verantwortliche den Rat des Datenschutzbeauftragten einzuholen. Daneben bleibt unklar, welche Aufgaben des Datenschutzbeauftragten aus dieser Mitteilung resultieren. Die Gesetzesbegründung spricht hier von „interner Vorabkontrolle“, ohne dass diese selbst aus dem Gesetzestext heraus ersichtlich wäre. Eine Doppelung von Verfahren sollte wegen des erhöhten Verwaltungsaufwandes vermieden werden.

Laut Begründung zu § 17 LDSG-neu richtet sich die Videoüberwachung zur Wahrung des Hausrechts und berechtigter Interessen allein nach Artikel 6 Absatz 1 Buchstabe f Verordnung (EU) 2016/279. Gemäß Artikel 6 Abs. 1 letzter Satz Verordnung (EU) 2016/279 gilt jedoch nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.

Wir bitten um Klarstellung, wann Behörden Maßnahmen zur Videoüberwachung im Zuge

des Hausrechts und berechtigter privatrechtlicher Interessen vornehmen dürfen.

Wir wünschen uns möglichst klare und einfache Hinweise und Handlungsempfehlungen seitens des Landesbeauftragten für Datenschutz und Informationsfreiheit, insbesondere zu Verkehrsleitplansystemen sowie Video-Türsprechanlagen.

#### § 27 LDSG-neu

Gemäß § 2 Abs. 2 letzter Satz LDSG-neu werden nicht-öffentliche Stellen, die hoheitliche Aufgaben der öffentlichen Verwaltung wahrnehmen, den öffentlichen Stellen im Sinne des LDSG gleichgestellt. § 2 Abs. 6 LDSG-neu bestimmt, dass bei öffentlichen Stellen, die als Unternehmen mit eigener Rechtspersönlichkeit am Wettbewerb teilnehmen, das BDSG neu anzuwenden ist.

Es stellt sich daher die Frage, weshalb § 27 LDSG-neu auf öffentliche Stellen Bezug nimmt, die am Wettbewerb teilnehmen, obwohl für diese das LDSG-neu nicht anzuwenden ist?

Wir bitten daher um Klarstellung, inwiefern gegen Kommunen Bußgelder erhoben werden können.

#### Weitere Anmerkungen

Weder in § 14 LDSG-neu noch in 83 LBG-neu ist eine abschließende Rechtsetzung hinsichtlich der Befugnis einer öffentlichen Stelle, Personalaktendaten für die Außendarstellung der öffentlichen Stelle (insbesondere Internet-Auftritt) verwenden zu dürfen, enthalten. In der Datenschutzpraxis muss zur Beantwortung dieser rechtlichen Frage auf heterogene Gerichtsurteile zurück gegriffen werden und/oder § 3 Abs. 1 EGovG BW und die §§ 83 und 84 LBG interpretiert werden. Wir regen deshalb an, durch eine gesetzliche Klarstellung diesen Zustand zu beenden.

Für eine Berücksichtigung der Anmerkungen wären wir dankbar.

Mit freundlichen Grüßen

Dr. Alexis v. Komorowski

Hauptgeschäftsführer

Norbert Brugger

Dezernent



Liga der freien Wohlfahrtspflege  
in Baden-Württemberg e.V.

Liga der freien Wohlfahrtspflege Stauffenbergstr. 3 70173 Stuttgart

Ministerium für Inneres, Digitalisierung und Migration  
Baden-Württemberg

Postfach 10 34 65  
70029 Stuttgart

Vorab per E-Mail: [Registatur2@im.bwl.de](mailto:Registatur2@im.bwl.de),

Liga der freien Wohlfahrtspflege  
in Baden-Württemberg e.V.  
Stauffenbergstr. 3  
70173 Stuttgart

Telefon: 0711 / 61967 - 0  
Fax: 0711 / 61967 - 67  
E-Mail: [info@liga-bw.de](mailto:info@liga-bw.de)  
Internet: [www.liga-bw.de](http://www.liga-bw.de)

Bank für Sozialwirtschaft  
IBAN: DE1160120500009700500  
BIC: BFSWDE33STG  
Stuttgart, 30.01.2018

**Stellungnahme zum Entwurf eines Gesetzes zur Anpassung des allgemeinen  
Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU)  
2016/679**

**Ihr Schreiben vom 19.12.2017, Az: 2-0557.8/1**

Sehr geehrter Herr  
sehr geehrte Frau

wir danken für die Möglichkeit, zum vorliegenden Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679 Stellung nehmen zu können.

Vor dem Hintergrund der langjährigen Erfahrungen unserer Verbände in der Beratung im Bereich des Ausländer- und Flüchtlingsrechts und insbesondere auch der Beratung in Abschiebungshafteinrichtungen möchten wir von der Möglichkeit der Stellungnahme Gebrauch machen.

Mit dem Gesetzentwurf soll neben vielen Änderungen verschiedener Vorschriften im Kontext der Umsetzung des Datenschutzrechtes der EU anlässlich dieser Änderungen auch das Abschiebungshaftvollzugsgesetz geändert werden (siehe Art. 15 des Gesetzentwurfes). Das Gesetzesvorhaben wird damit begründet, dass die Änderungen notwendig seien, um das Landesdatenschutzgesetz (LDSG) sowie sonstige bereichsspezifische Datenschutzregelungen an die Regelungen der EU-Datenschutz-Grundverordnung anzupassen. Anlässlich dieser Gesetzesänderung soll in das Abschiebungshaftvollzugsgesetz eine Regelung der **Videoüberwachung** innerhalb der Abschiebungshafteinrichtung eingeführt werden (geplante Änderung von §10 Abs. 4 Abschiebungshaftvollzugsgesetz).

Seite 1 von 2

In einer Abschiebungshafteinrichtung werden vollziehbar ausreisepflichtige Ausländer untergebracht, um zu verhindern, dass sich diese der Abschiebung entziehen. Es handelt sich um keine Haft für Straftäter und um keine Untersuchungshaft. Oft werden dort Menschen in Haft genommen, die keinerlei Straftaten begangen haben. Abschiebungshaft ist immer ultima-Ratio und die Inhaftierung ein schwerer Grundrechtseingriff, bei der auch die Regelungen über den Abschiebungshaftvollzug besonders streng dem Verhältnismäßigkeitsgrundsatz gerecht werden müssen. Eine Videoüberwachung von inhaftierten Personen in Krankenzimmern oder sonstigen Räumen, in denen sich die jeweiligen Personen während längerer Zeit ausschließlich und nicht freiwillig aufhalten, ist eine totale 24-h-Überwachung der inhaftierten Personen und von daher unverhältnismäßig. Die Gesetzesbegründung gibt auch keinerlei Begründung, warum diese Regelung überhaupt erforderlich sein soll und mildere Mittel nicht zur Verfügung stehen. Wenn eine solche Regelung überhaupt eingeführt werden soll, müsste sie zumindest sehr strengen Kriterien der Notwendigkeit unterworfen werden und bedarf zum Grundrechtsschutz der Betroffenen der richterlichen Anordnung. Sofern Personen wegen vorhandenen psychischen Erkrankungen oder akuter Suizidalität überwacht werden sollen, ist schon der Vollzug von Abschiebungshaft unverhältnismäßig und dürfte erst gar nicht erfolgen.

Zur Vermeidung von Wiederholungen dürfen wir auf unsere Stellungnahme zum Entwurf eines Abschiebungshaftvollzugsgesetzes vom 17.09.2015 verweisen und auf unsere Stellungnahme zur Abschiebungshaftvollzugsverordnung vom 29.01.2016.

Für ein Gespräch stehen wir gerne zur Verfügung.

Mit freundlichen Grüßen



Jürgen Blechinger

Vorsitzender des Liga-Fachausschusses Migration



Notarkammer Baden-Württemberg • Friedrichstr. 9a • 70174 Stuttgart

Ministerium für Inneres, Digitalisierung und Migration  
Baden-Württemberg  
Willy-Brandt-Straße 41  
70173 Stuttgart

E-Mail [info@notarkammer-baden-wuerttemberg.de](mailto:info@notarkammer-baden-wuerttemberg.de)

29. Januar 2018

## Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679

Sehr geehrter Herr  
sehr geehrte Damen und Herren,

für die Möglichkeit der Stellungnahme zum Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679 danken wir. Wir nehmen diese Möglichkeit hiermit gerne wie folgt wahr:

### I. Anwendung auf Notare, Subsidiarität

Notare sind als Organe der (vorsorgenden) Rechtspflege Träger eines öffentlichen Amtes (§§ 1, 2 BNotO), die durch Hoheitsakt bestellt werden (§ 12 BNotO) und der Dienstaufsicht der Landesjustizverwaltung unterliegen (§ 92 ff. BNotO). Sie sind daher nach Auffassung des Bundesgerichtshofs (BGHZ 112, 178 = NJW 1991, 568) sowie nach allgemeiner Ansicht in der Literatur (statt vieler Klingler, RNotZ 2013, 57 m. w. N.) als öffentliche Stellen der Länder im Sinne des geltenden Datenschutzrechts anzusehen. Auch die EU-Datenschutz-Grundverordnung („DSGVO“) trifft insoweit keine andere Regelung oder Wertung. Die Notare fallen also gemäß § 2 Abs. 1 S. 1 des Entwurfs des Landesdatenschutzgesetzes („LDSG-E“) in den Anwendungsbereich des Gesetzes. Die notarielle Amtstätigkeit und das Beurkundungsverfahren sind in der Bundesnotarordnung, dem Beurkundungsgesetz und in weiteren Verfahrensordnungen (etwa FamFG, ZPO) umfassend spezialgesetzlich durch Bundesrecht geregelt. Dieses Berufs- und Verfahrensrecht enthält an zahlreichen Stellen

Anschrift Notarkammer Baden-Württemberg  
Friedrichstraße 9a  
70174 Stuttgart  
Telefon (0711) 30 58 77 0  
Telefax (0711) 30 58 77 69

Präsident Notar Peter Wandel, Esslingen  
Geschäftsführung Dr. Carsten Walter, M.Jur (Oxford)  
E-Mail [info@notarkammer-baden-wuerttemberg.de](mailto:info@notarkammer-baden-wuerttemberg.de)  
Internet [www.notarkammer-baden-wuerttemberg.de](http://www.notarkammer-baden-wuerttemberg.de)

Bankverbindung BW Bank  
IBAN DE48 6005 0101 0001 2820 01  
BIC



2-0557.8/1/185

datenschutzrechtliche Regelungen oder Regelungen mit Bezug auf den Datenschutz, die auch weitgehend tatbestandskongruent zum allgemeinen Datenschutzrecht sind. Dazu zählen allen voran die umfassende notarielle Verschwiegenheitspflicht (§ 18 BNotO) – dazu genauer unter II. – und die sie begleitenden Vorschriften, aber auch Regelungen zu Mitteilungspflichten, zu Einsichtsrechten, zur Führung von Akten und Verzeichnissen, zu Speicherfristen etc.

Den Notaren kommt eine Sonderrolle zu: Sie sind die einzigen Berufsträger außerhalb des unmittelbaren Staatsdienstes, auf die das Landesdatenschutzgesetz anwendbar ist.

## **II. Die Bedeutung der notariellen Verschwiegenheitspflicht**

Die in § 18 BNotO normierte und durch weitere gesetzliche Regelungen flankierte notarielle Verschwiegenheitspflicht gründet darauf, dass es sich bei den dem Notar von den Beteiligten anvertrauten Informationen überwiegend um personenbezogene Daten, häufig sogar um besonders sensible Daten aus dem persönlichen Lebens- und Geheimbereich handelt. Die Verschwiegenheitspflicht ist dabei Ausfluss des Grundrechts der Beteiligten auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, Art. 2 Abs. 1 Verfassung des Landes Baden-Württemberg). Durch ihre strenge Ausgestaltung sowie die begleitende strafrechtliche Sanktionierung (§ 203 Abs. 1 Nr. 3 StGB) und die damit korrespondierenden strafprozessualen Zeugnisverweigerungsrechte und Beschlagnahmeverbote ist die notarielle Verschwiegenheitspflicht eine über das allgemeine Datenschutzrecht weit hinausreichende, geradezu die strengste denkbare Datenschutzregelung (vgl. Rüpke, NJW 1991, 548). Da die Verschwiegenheitspflicht eines der höchsten Güter des Notarberufs ist, ist der Datenschutz dem Notaramt insoweit also nicht nur immanent, sondern eines seiner Wesensmerkmale und gehört richtigerweise zum Selbstverständnis der Notare. Insoweit sind sie als „geborene Datenschützer“ einzuordnen, zumal sie aufgrund ihrer Neutralität und Unabhängigkeit die von ihnen verarbeiteten Daten eben nicht im einseitigen Interesse eines Auftraggebers, sondern ohne Weisungsgebundenheit im Interesse aller Beteiligten und zum Schutz des Rechtsverkehrs hüten.

Außerdem ist die notarielle Verschwiegenheitspflicht der Garant dafür, dass die Rechtssuchenden dem Notar persönlich und/oder wirtschaftlich sensible personenbezogene Informationen anvertrauen, die ihm überhaupt erst seine Amtstätigkeit als unabhängiges, neutrales und als vertrauenswürdig anerkanntes Organ der vorsorgenden Rechtspflege ermöglichen. Die Verschwiegenheitspflicht und ihr gesetzlicher Schutz – auch vor Eingriffen des Staates in die dem Notar anvertrauten Informationen, soweit der Notar nicht gesetzlich

ausdrücklich zur Mitteilung an andere staatliche Stellen verpflichtet ist – sind daher unabdingbar für den Bestand des Notariats.

### III. Grundsätzliche Anmerkungen

Wir begrüßen die mit der DSGVO und dem Entwurf des LDSG einhergehende Stärkung des Datenschutzes. Für Notare ist aus den unter II. genannten Gründen ein effektiver Datenschutz seit jeher ein besonderes Anliegen.

### IV. Zu Abschnitt 3 (Rechte der betroffenen Person)

#### 1. Spannungsverhältnis zwischen Betroffenenrechten und notarieller Schweigepflicht

Abschnitt 3 basiert auf Art. 14 Abs. 1, 15 und 34 DSGVO. Art. 14 Abs. 1 DSGVO sieht vor, dass der jeweils Verantwortliche verpflichtet ist, einer Person über die Erhebung ihrer personenbezogenen Daten zu informieren. Art. 15 DSGVO begründet ein Auskunftsrecht der betroffenen Person. Art. 34 DSGVO regelt eine Benachrichtigungspflicht nach einer Rechtsverletzung.

Eine unbesehene Anwendung dieser Betroffenenrechte könnte zu einer schwerwiegenden Beeinträchtigung der Rechte von Mandanten bei Notaren sowie sonstigen Berufsgeheimnisträgern führen. Insbesondere wäre es denkbar, dass ein Notar, der von seinem Mandanten Informationen über dritte Personen erhält, gegenüber diesen dritten Personen das Mandatsverhältnis offenlegen müsste. Eine solche Pflicht zur Offenlegung könnte den Notar etwa infolge eines Auskunftsverlangens nach Art. 15 Abs. 1 DSGVO treffen. Dies wäre angesichts der unter II. geschilderten Bedeutung der notariellen Verschwiegenheitspflicht den Mandanteninteressen in hohem Maße abträglich. Auch das bisherige Datenschutzrecht enthält in § 21 Abs. 5 Nr. 3 LDSG einen ausdrücklichen Vorrang der Geheimhaltungspflichten vor dem Auskunftsrecht, das es anders als die Informations- und Benachrichtigungspflicht bereits im geltenden Recht gibt.

#### 2. Keine ausreichende Regelung im LDSG-E

Nach unserer Auffassung ist nach dem Entwurf des LDSG zwar im Ergebnis ein Schutz der notariellen Schweigepflicht gegeben, zwingend ist diese Rechtsauffassung jedoch nicht:

- Zunächst kann §§ 8 Abs. 1 Nr. 4, 9 Abs. 1 Satz 1, 11 Nr. 2 LDSG-E als Ausschluss der Betroffenenrechte angesehen werden. Es ist durchaus naheliegend, eine Geheimhaltungspflicht zum Schutze der Rechte einer anderen Person zu bejahen,

wenn die andere Person durch die notarielle Schweigepflicht geschützt ist. Es könnte jedoch auch angeführt werden, dass der Entwurf des LDSG – anders als § 29 Abs. 1 Satz 2 und 3 BDSG-neu und § 21 Abs. 5 Nr. 3 des noch geltenden LDSG – gerade keine Beschränkung der Betroffenenrechte *durch eine Rechtsvorschrift* kennen. Daraus könnte geschlossen werden, dass die auf § 203 Abs. 1 Nr. 3 StGB, § 18 BNotO beruhende notarielle Schweigepflicht gerade nicht von §§ 8 Abs. 1 Nr. 4, 9 Abs. 1 Satz 1, 11 Nr. 2 LDSG-E erfasst wird.

- Auch § 2 Abs. 3 LDSG-E ist nach unserer Auffassung keine sichere Grundlage für den Schutz der notariellen Schweigepflicht. Die Vorschrift sieht nur vor, dass besondere Rechtsvorschriften (also auch § 203 Abs. 1 Nr. 3 StGB, § 18 BNotO) dem LDSG-E vorgehen. Damit regelt der Entwurf des LDSG nichts zum Verhältnis von notarieller Schweigepflicht zur DSGVO. Ob § 203 Abs. 1 Nr. 3 StGB, § 18 BNotO selbst „Beschränkungsnormen“ i.S.v. Art. 23 Abs. 1 lit. e) und i) DSGVO darstellen, lässt der Entwurf des LDSG offen. Aus unserer Sicht wäre ein solches Verständnis zwar naheliegend. Ob sich diese Auffassung letztlich durchsetzen würde, ist aus unserer Sicht aber unklar.

Der Bundesgesetzgeber hat sich in § 29 Abs. 1 Satz 2 und 3 BDSG-neu dazu entschieden, die Betroffenenrechte auch durch eine Rechtsvorschrift zu beschränken. Ohne eine solche Beschränkung bestünde nur für die Informationspflicht in Art. 14 Abs. 5 lit. d) DSGVO eine zufriedenstellende Ausnahmeregelung. Für das Auskunftsrecht und die Benachrichtigungspflicht wäre zu befürchten, dass es zu einer Verkürzung der Mandantenrechte bei Inanspruchnahme notarieller Dienstleistungen und zu Rechtsunsicherheit käme. Nach bundesverfassungsgerichtlicher Rechtsprechung darf das Mandatsverhältnis nicht mit Unsicherheiten hinsichtlich seiner Vertraulichkeit belastet sein (vgl. BVerfG, Urteil vom 12. April 2005 – 2 BvR 1027/02). Die Rechtsunsicherheit könnte zu einer Belastung der für Notare zuständigen Aufsichtsbehörden durch Entscheidungsgesuche führen (vgl. § 18 Abs. 3 BNotO).

### 3. Unser Vorschlag

Aus unserer Sicht sollte der Entwurf des LDSG um eine dem § 29 Abs. 1 BDSG-neu entsprechende Vorschrift ergänzt werden. Die könnte durch eine Erweiterung der §§ 8 Abs. 1 Nr. 4, 9 Abs. 1 Satz 1, 11 Nr. 2 LDSG-E oder durch einen zusätzlichen Absatz in § 12 LDSG-E, der den Umgang mit Daten regelt, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen.

## V. Zu § 25 Absatz 1 LDSG-E

### 1. Regelungen in DSGVO, BDSG-neu und LDSG-E

Nach Art. 90 Abs. 1 DSGVO können die Mitgliedstaaten die Befugnisse der Aufsichtsbehörden im Sinne des Art. 58 Abs. 1 lit. e) und f) gegenüber Berufsheimnisträgern regeln, soweit dies notwendig und verhältnismäßig ist, um das Recht auf Schutz der personenbezogenen Daten mit der Pflicht zur Geheimhaltung in Einklang zu bringen.

Bei der von Art. 90 Abs. 1 DSGVO vorgesehenen Einschränkungsmöglichkeit geht es um die nach dem Wortlaut des Art. 58 Abs. 1 lit. e) und f) DSGVO unbeschränkte Zugangs- und Durchsuchungsbefugnis der Aufsichtsbehörde bezüglich aller Daten, Informationen, Geschäftsräume, Datenverarbeitungsanlagen und -geräte. Nicht von der Einschränkungsmöglichkeit erfasst ist die Verantwortlichkeit als solche von Heimnisträgern gegenüber der Aufsichtsbehörde; die Pflicht zur Rechenschaft und Erteilung aller Informationen und Auskünfte gegenüber der Aufsichtsbehörde (Art. 58 Abs. 1 lit. a) bis d)) DSGVO soll ebenso unberührt bleiben wie die übrigen Befugnisse der Aufsichtsbehörde.

Der Bundesgesetzgeber hat von der von der DSGVO eingeräumten Regelungsmöglichkeit in § 29 Abs. 3 BDSG-neu erfreulicherweise Gebrauch gemacht und eine Ausnahme für Stellen geschaffen, die Geheimhaltungsvorschriften unterliegen. Der Entwurf des LDSG hingegen bestimmt ausdrücklich nichts dazu. Vielmehr könnte aus § 24 Abs. 5 LDSG-E gefolgert werden, dass die notarielle Schweigepflicht der Zugangs- und Durchsuchungsbefugnis nicht entgegengehalten werden kann.

### 2. Regelung im LDSG-E wird Mandanteninteressen nicht gerecht

Diese Regelung ist angesichts der vorstehend (unter II.) geschilderten Bedeutung beruflicher Verschwiegenheitspflichten entschieden abzulehnen. Sie greift in unangemessener Weise in die Geheimhaltungsbedürfnisse der Bürger ein, die Notaren, Rechtsanwälten, Ärzten und anderen Berufsheimnisträgern schützenswerte, zumeist sogar besonders sensible und persönliche Informationen in dem Wissen anvertrauen, dass sie absolut geheim behandelt werden und gesetzlich streng vor dem Zugriff Dritter geschützt werden, und zwar auch und gerade vor dem Zugriff staatlicher Stellen, wozu auch der Landesdatenschutzbeauftragte gehört, unabhängig davon, ob diese staatlichen Stellen wiederum einem Amtsheimnis verpflichtet sind. Diese beruflichen bzw. amtlichen Verschwiegenheitspflichten sollen gerade das Recht der Bürger auf informationelle Selbstbestimmung – auch vor dem Staat –

schützen. Sie garantieren die Funktionsfähigkeit der jeweiligen Berufe im System der Rechtspflege, des Gesundheitswesens etc. und erfüllen somit eine wichtige soziale und rechtsstaatliche Funktion, weshalb sie auch verfassungsrechtlich geschützt sind.

Das Vertrauen der Bevölkerung in Notare, Rechtsanwälte und Ärzte und andere in § 203 StGB genannte Berufsheimnisträger würde erheblich erschüttert, wenn der Landesdatenschutzbeauftragte voraussetzungs- und einschränkungslos die Geschäftsräume, Datenverarbeitungsanlagen und Akten der Berufsheimnisträger durchsuchen dürfte. Eine solche Befugnis gegenüber Berufsheimnisträgern gibt es im deutschen Recht in keinem anderen Rechtsgebiet. Sie wäre auch unverhältnismäßig, weil sie zum Schutz und zur Durchsetzung des informationellen Selbstbestimmungsrechts der Betroffenen unnötig ist: Berufliche Verschwiegenheitspflichten gelten zum Schutz des informationellen Selbstbestimmungsrechts und unterliegen daher der Disposition der Betroffenen, m.a.W. die Betroffenen haben es in der Hand, den Geheimnisträger von der Pflicht zur Verschwiegenheit zu entbinden. Soweit Betroffene ein Interesse daran haben, dass der Landesdatenschutzbeauftragte seine Untersuchungsbefugnisse bei dem Berufsheimnisträger ausübt, können sie den Berufsheimnisträger einfach von der Verschwiegenheitspflicht befreien, so dass der Landesdatenschutzbeauftragte seine Befugnisse problemlos und ungehindert gegenüber dem Berufsheimnisträger ausüben kann. Aufgabe des Landesdatenschutzbeauftragten ist der Schutz des informationellen Selbstbestimmungsrechts betroffener Personen. Erfolgt eine Befreiung durch die Betroffenen von der Verschwiegenheitspflicht nicht, ist deshalb kein Grund ersichtlich, warum der Landesdatenschutzbeauftragte gegen den Willen der Betroffenen den Geheimnisschutz brechen können sollte.

In der Gesetzesbegründung wird – richtigerweise – darauf hingewiesen, dass § 25 Abs. 1 LDSG-E im Verhältnis zum alten Recht (vgl. § 29 Abs. 2 LDSG) keine Änderung enthält. Bisher war ein ausdrücklicher Schutz von Berufsheimnissen in den Landesdatenschutzgesetzen deswegen nicht erforderlich, weil diesen § 18 BNotO nach verbreiteter Auffassung vorging (Kanzleiter in Schippel/Bracker, § 18 BNotO, Rn. 66, m.w.N.). Ob dies mit der DSGVO noch gilt, ist jedenfalls fraglich (vgl. Bremkamp in Eylmann/Vaasen, § 18 BNotO, Rn. 170; Klingler, RNotZ 2013, 57, 81). Es besteht deswegen Bedarf für eine Regelung zum Schutz der Mandanten von Berufsheimnisträgern.

Der Bundesgesetzgeber hat sich entschieden, § 29 Abs. 3 BDSG-neu, der keine Entsprechung im geltenden Recht hat, einzuführen. Nach der Gesetzesbegründung (BT-Drucks. 18/11325, S. 101) würde es „ohne eine Einschränkung der Befugnisse der Aufsichtsbehörden [...] zu einer Kollision mit Pflichten des Geheimnisträgers [kommen]. Gerade bei den freien Berufen schützt die berufsrechtliche Schweigepflicht das Vertrauen

des Mandanten und der Öffentlichkeit in den Berufsstand. Nach bundesverfassungsgerichtlicher Rechtsprechung darf das Mandatsverhältnis nicht mit Unsicherheiten hinsichtlich seiner Vertraulichkeit belastet sein (vgl. BVerfG, Urteil vom 12. April 2005 – 2 BvR 1027/02).“

### 3. Unser Vorschlag

Wir möchten daher vorschlagen, die Regelung des § 29 Abs. 3 BDSG-neu in das LDSG als ausdrückliche Einschränkung der Informations- und Kontrollbefugnisse zu übernehmen. Diese Änderung ist sachgerecht und schützt das Recht auf informationelle Selbstbestimmung angemessen, indem sie die Einschränkung der Befugnisse der Aufsichtsbehörde auf das Geheimhaltungsinteresse der Betroffenen begrenzt.

Eine solche Regelung könnte in § 12 LDSG-E oder in § 25 LDSG-E in einem neuen Absatz zwischen Absatz 1 und 2 erfolgen.

Mit freundlichen Grüßen



P. Wandel  
Präsident



**Stellungnahme LRK-PH**  
**zum Anhörungsentwurf „Anpassung des allgemeinen Daten-**  
**schutzrechts und sonstiger Vorschriften**  
**an die Verordnung (EU) 2016/679**  
**Hier: Artikel 1 Neufassung des Landesdatenschutzgesetzes**

**Anhörungsentwurf Stand 14.12.2017**

Die Landesrektorenkonferenz der Pädagogischen Hochschulen bedankt sich für die Möglichkeit der Stellungnahme.

- Im Folgenden werden die wesentlichen Änderungsanliegen der LRK-PH dargestellt. Diese beziehen sich hauptsächlich auf Regelungen, die die Freiheit der Wissenschaft, insbesondere der Forschung, betreffen, und unserer Ansicht nach dazu führen, dass der Wissenschaftsstandort Baden-Württemberg, konkret die Wissenschaftlichen Hochschulen in Baden-Württemberg die Gefahr eines Wettbewerbsnachteils erfährt.

- Zu der Kostenfolge, Vorblatt unter D., wird darauf hingewiesen, dass der für die Landesverwaltung und somit für die Hochschulen entstehende zusätzliche Kostenaufwand bei dem Landesbeauftragten für den Datenschutz unmittelbar durch die Neuregelungen des LDS verursacht werden. Insgesamt ist im Hinblick auf die Verpflichtungen der Hochschulen aufgrund der Datenschutz-Grundverordnung (DS-GVO) und der Neufassung des LDSG eine finanzielle Unterstützung durch das Land zwingend erforderlich.

**1. § 8 Abs. 1 Satz 1 LDSG-E, Beschränkung der Informationspflicht**

Es wird die folgende Ergänzung vorgeschlagen:

**„5. die Information den wissenschaftlichen Forschungszweck unmöglich machen oder ernsthaft beeinträchtigen würde“.**

Die Notwendigkeit ergibt sich aus der Freiheit der wissenschaftlichen Forschung, die Rechtsgrundlage aus Art. 23 Abs. 1 e. DS-GVO.

**2. § 9 LDSG-E, Beschränkung des Auskunftsrechts**

**a. § 9 Abs. 1, Folgeänderung**

Im Hinblick auf die unter Ziff. 1 vorgeschlagene Änderung muss § 9 entsprechend angepasst werden, d.h., der Verweis in § 9 Abs. 1 LDSG-E muss auf die Fallgestaltungen des § 8 Abs. 1 Satz 1 Nr. 1 – 4 LDSG-E zu beschränkt werden.

Einschränkungen des Art. 15 DS-GVO bei der Verarbeitung zu wissenschaftlichen oder historischen Forschungszwecken werden bereichsspezifisch in § 13 Abs. 4 LDSG-E geregelt.





#### b. § 9 Abs. 2, Präzisierung des Auskunftersuchens

***Im Interesse der Rechtssicherheit und damit für die Anwendung der Regelung in der Praxis ist eine Definition bzw. Präzisierung des Begriffs „eine große Menge von Informationen“ erforderlich.***

#### 3. § 13 LDSG-E, Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken

##### a. § 13 Abs. 1 LDSG-E

- Es wird gebeten zu prüfen, ob bei Forschungsvorhaben, für die Daten, die nicht Art. 9 DS-GVO unterfallen, und in erheblichem Umfang oder in einer Art (z.B. Einsatz von Videotechnologie, Forschung mit Sprachaufzeichnungen) verarbeitet werden, die zu einer großen Eingriffsintensität führen, eine hinreichend bestimmte Rechtsgrundlage vorhanden ist. Insbesondere für den Fall von Forschungsvorhaben, bei denen Daten ohne Einwilligung der betroffenen Personen verarbeitet werden bzw. im Hinblick auf das Forschungsziel verarbeitet werden müssen, ist diese dringend erforderlich.

Insbesondere wegen des oben dargestellte Änderungs- bzw. Klärungsbedarfs, aber auch unabhängig davon, insbesondere im Hinblick auf die Verarbeitung besonderer Arten personenbezogener Daten ist fraglich, ob das Kriterium der Erheblichkeit in § 13 Abs. 1 LDSG-E sachgerecht ist. Die Öffnungsklausel des Art. 9 Abs. 2 j. DS-GVO stellt keine derartige Anforderung an die mitgliedstaatliche Vorschrift, sondern die nationale Ausnahmvorschrift für Forschungszwecke muss in angemessenem Verhältnis zu dem verfolgten Ziel stehen, den Wesensgehalt des Rechts auf Datenschutz wahren und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsehen. Da in § 13 Abs. 1 LDSG-E ein Überwiegen der Interessen der Betroffenen verlangt und voraussetzt, dass der Forschungszweck auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann, ist diese Anforderung erfüllt, auch ohne dass darüber hinaus eine „erhebliches“ Überwiegen gefordert wird. Weitere Schutzmaßnahmen betreffend die Daten der betroffenen Personen sind in § 13 Abs. 2 LDSG-E geregelt. Stattdessen sollte der Begriff „schutzwürdige Belange“ entsprechend § 5 Abs. 2 LDSG-E verwendet werden.

#### **Änderungsvorschlag zu § 13 Abs. 1 LDSG-E**

***„(1) Öffentliche Stellen dürfen personenbezogene Daten einschließlich besondere Kategorien personenbezogener Daten für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke verarbeiten, wenn die Zwecke auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden können und die Interessen der öffentlichen Stelle an der Verarbeitung die Interessen schutzwürdigen Belange der betroffenen Person an einem Ausschluss der Verarbeitung erheblich überwiegen. Besondere Kategorien personenbezogener Daten sind die in Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 genannten Daten.*“**



**b. § 13 Abs. 2 LDSG-E**

Bereits § 35 LDSG sieht vor, dass personenbezogene Daten zu vermeiden und zu löschen sind, wenn sie nicht mehr benötigt werden, ebenso sieht dies die DS-GVO vor, Art. 5 Abs. 1 c. und Art. 17 Abs. 1 a. Nunmehr soll zwischen Anonymisierung und Pseudonymisierung differenziert werden (Gesetzesbegründung s. 24 zu § 3 Abs. 2). Ein Grund für diese Differenzierung ist nicht ersichtlich.

**Änderungsvorschlag zu § 13 Abs. 2 LDSG-E**

• **„(2) ~~Die besonderen Kategorien~~ Personenbezogene Daten sind zu anonymisieren, sobald dies nach dem Forschungs- oder Statistikzweck möglich ist. Bis zur Anonymisierung sind die Merkmale gesondert zu speichern, mit denen Einzelangaben einer bestimmten oder bestimmbarer Person zugeordnet werden können. Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungszweck dies erfordert.“**

**c. § 13 Abs. 3 LDSG-E**

• Vor dem Hintergrund der Open Access-Strategie des Europäischen Forschungsraums und des Landes Baden-Württemberg fällt auf, dass weder § 13 Abs. 3 LDSG-E noch eine andere Norm in dem vorliegenden Entwurf eine Ermächtigungsnorm darstellt, auf deren Grundlage personenbezogene Forschungsdaten ohne Einwilligung veröffentlicht werden dürfen.

Das Einholen und Verwalten der Einwilligung bedeutet für die Hochschulen einen sehr hohen Verwaltungsaufwand dar, oft ist es außerdem nicht möglich, die Einwilligung einzuholen, weil die erforderliche Kontaktdaten nicht, bzw. nicht in dem dafür notwendigen Umfang vorliegen.

**Es wird daher angeregt, eine eindeutige Rechtsvorschrift zu schaffen, die die Veröffentlichung auch personenbezogener Forschungsdaten, soweit erforderlich unter zu definierenden Rahmenbedingungen und Beschränkungen, erlaubt.**

**4. § 28 LDSG-E**

**Es wird vorgeschlagen, anstelle der Einzelbegriffe in § 28 Abs. 1 Nr. 1 a. LDSG-E die Begrifflichkeit des Art. 4 Nr. 2 DS-GVO, also den Begriff „verarbeitet“ zu verwenden.**



## 5. § 7 LDSG-E, Datengeheimnis

Eine Definition des „Datengeheimnisses“ ist im LDSG-E nunmehr nicht mehr enthalten, gleichwohl wird dieses in § 7 Abs. 1 Satz 5 LDSG-E ausdrücklich genannt: „Hinsichtlich der Daten, die sie im Rahmen ihrer Tätigkeit für die fremde Behörde zur Kenntnis nehmen, haben sie das Datengeheimnis gegenüber ihrer eigenen Dienststelle zu wahren.“

Die Gesetzesbegründung (Seite 17, zu § 7) führt aus, die DS-GVO setze die Einhaltung des Datengeheimnisses als Schutzmaßnahme voraus. Damit bleibt offen, ob beschäftigte Personen auf das Datengeheimnis verpflichtet werden müssen oder ob es dies Kraft Gesetzes gilt.

- **Es wird vorgeschlagen, das Datengeheimnis wie bislang ausdrücklich im LDSG zu regeln.**

Die Pädagogischen Hochschulen weisen abschließend ausdrücklich darauf hin, dass die den Hochschulen zusätzlich übertragenen Aufgaben nicht ohne den Einsatz zusätzlicher Ressourcen wahrgenommen werden können.

•

Prof. Dr. Ulrich Druwe, Rektor der PH Freiburg  
Stellv. Vorsitzenden der Landesrektorenkonferenz  
der Pädagogischen Hochschulen,

Pädagogische Hochschule Schwäbisch Gmünd  
Oberbettringer Straße 200  
73525 Schwäbisch Gmünd  
Zentrale: 07171 - 983 - 0



**RECHNUNGSHOF  
BADEN-WÜRTTEMBERG  
Stabelstraße 12, 76133 Karlsruhe**

**poststelle@rh.bwl.de  
Telefon 0721 926-3104 • Telefax 0721 926-2173**

Ministerium für Inneres, Digitalisierung  
und Migration  
Baden-Württemberg  
Willy-Brandt-Straße 41  
70173 Stuttgart

Datum 17.01.2018

Aktenzeichen P-0557.2/2

(Bitte bei Antwort angeben)

**Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und  
sonstiger Vorschriften an die EU-DSGVO**

**Schreiben des Innenministeriums vom 19.12.2017**

Sehr geehrte Frau

der Rechnungshof Baden-Württemberg bedankt sich für die Beteiligung im Rahmen des Verfahrens zur Anpassung des Landesrechts an die Europäische Datenschutz-Grundverordnung und die Zusage unserer Stellungnahme vom 16. November 2017 in das Anhörungsverfahren einzubeziehen.

Mit freundlichen Grüßen

gez. Dr. Otto Häußler

**Baden-Württemberg**

RECHNUNGSHOF

Rechnungshof Baden-Württemberg · Postfach 11 11 52 · 76061 Karlsruhe

Ministerium für Inneres, Digitalisierung  
und Migration  
Baden-WürttembergWilly-Brandt-Straße 41  
70173 Stuttgart

Datum 16.11.2017

Aktenzeichen P-0277.8/175

(Bitte bei Antwort angeben)

** Anpassung des Landesrechts an die Verordnung (EU) 2016/679 (Datenschutz Grundverordnung)**

Sehr geehrter Herr

der Rechnungshof Baden-Württemberg bedankt sich für die Beteiligung im Rahmen des Verfahrens zur Anpassung des Landesrechts an die Europäische Datenschutz-Grundverordnung (DSGVO).

Im vorliegenden Entwurf des Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) bitten, wir folgende Änderung zu berücksichtigen:

Nach § 2 Absatz 4 Satz 3 LDSG n.F. finden auf die Prüfungstätigkeit des Rechnungshofs Artikel 30 und Kapitel VI der Datenschutz-Grundverordnung sowie die §§ 23 und 24 des neuen Landesdatenschutzgesetzes keine Anwendung.

Damit wird der verfassungsrechtlich garantierten Unabhängigkeit des Rechnungshofs in Bezug auf seine Prüfungstätigkeit wie bisher in § 2 Abs. 3 LDSG a.F. Rechnung getragen. Gegenüber der alten Regelung wird jedoch insoweit abgewichen, dass die staatlichen Rechnungsprüfungsämter nicht mehr erwähnt werden.

Es wird darum gebeten, die staatlichen Rechnungsprüfungsämter neben dem Rechnungshof ausdrücklich in der Regelung des § 2 Absatz 4 Satz 3 LDSG n.F. zu erwähnen. Bei den staatlichen Rechnungsprüfungsämtern handelt es sich um eigenständige höhere Sonderbehörden im Geschäftsbereich des Rechnungshofs. Sie bilden zusammen mit dem Rechnungshof die staatliche Finanzkontrolle Baden-Württemberg.

Damit die Bereichsausnahme auch für die Prüfungstätigkeit der Staatlichen Rechnungsprüfungsämter gilt, müssen diese in die Regelung aufgenommen werden.

Mit freundlichen Grüßen

  
Dr. Otto Häußer

---

**Von:** Tilman Winkler  
**Gesendet:** Freitag, 2. Februar 2018 10:47  
**An:** Registratur 2 (IM)  
**Cc:**  
**Betreff:** Stellungnahme: Gesetz zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679

Sehr geehrte Damen und Herren,

ich teile für die Rechtsanwaltskammer Freiburg mit, dass wir die Stellungnahme der Rechtsanwaltskammer Stuttgart zum Gesetz zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679 unterstützen.

Mit freundlichen Grüßen

RA Tilman Winkler  
(Geschäftsführer)

Rechtsanwaltskammer Freiburg  
Körperschaft des öffentlichen Rechts

Bertoldstraße 44, 79098 Freiburg  
Postfach 1369, 79013 Freiburg

[info@rak-freiburg.de](mailto:info@rak-freiburg.de)

weitere Informationen, insbesondere nach der DL-InfoV:  
[www.rak-freiburg.de](http://www.rak-freiburg.de)

Rechtsanwaltskammer  
Stuttgart

Rechtsanwaltskammer Stuttgart Postfach 10 37 12 70032 Stuttgart

**per E-Mail**Ministerium für Inneres, Digitalisierung  
und Migration Baden-WürttembergPostfach 103465  
70029 Stuttgart

Unser Zeichen/Name

Mi/tj

Telefon/E-Mail

Datum

31.01.2018

**Gesetz zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die  
Verordnung (EU) 2016/679****Hier: Stellungnahme der Rechtsanwaltskammer Stuttgart zum Referentenentwurf**

Sehr geehrte Frau

wir bedanken uns für die Gelegenheit zur Stellungnahme im oben genannten Gesetzgebungsverfahren. Unsere Stellungnahme möchten wir auf die Regelungen des § 24 Abs. 1 Satz 2 und § 27 des Entwurfs beschränken.

Gemäß § 24 Abs. 1 Satz 2 ist die oder der Landesdatenschutzbeauftragte zugleich Aufsichtsbehörde für den Datenschutz für nichtöffentliche Stellen nach § 40 des Bundesdatenschutzgesetzes. Mangels Ausnahmeregelung unterfallen damit auch die Mitglieder der Rechtsanwaltskammern der Kontrolle durch den Landesdatenschutzbeauftragten bzw. die Landesdatenschutzbeauftragte.

Obwohl § 51 der Datenschutzgrundverordnung die Möglichkeit eines sektoralen Datenschutzes eröffnet, hat der Bundesgesetzgeber hiervon im Hinblick auf die Datenschutzkontrolle über Rechtsanwältinnen und Rechtsanwälte keinen Gebrauch gemacht. Der Vorschlag der Bundesrechtsanwaltskammer, einen Bundesdatenschutzbeauftragten der Anwaltschaft zu installieren, wurde nicht umgesetzt. Nach Auffassung der Rechtsanwaltskammer Stuttgart kann jedoch nur auf diese Weise gewährleistet werden, dass die berufsspezifischen Regelungen genügend Berücksichtigung finden. Die Rechtsanwaltskammer Stuttgart setzt sich daher, gemeinsam mit der

**Rechtsanwaltskammer  
Stuttgart**Körperschaft  
des öffentlichen RechtsKönigstraße 14  
70173 StuttgartPostfach 10 37 12  
70032 StuttgartTelefon: + 49 (0) 7 11 - 22 21 55-0  
Telefax: + 49 (0) 7 11 - 22 21 55-11Seite 1 von 2  
info@rak-stuttgart.de  
www.rak-stuttgart.de



Bundesrechtsanwaltskammer, weiter für die Installation eines Bundesdatenschutzbeauftragten der Anwaltschaft ein.

Auf Landesebene könnte man sich nach Auffassung der Rechtsanwaltskammer Stuttgart dem Konzept des sektoralen Datenschutzes im Interesse der Wahrung der rechtsstaatlichen Funktion und Aufgaben der Anwaltschaft, die insbesondere durch die Unabhängigkeit der anwaltlichen Berufsausübung geprägt sind, dadurch nähern, dass die/der Landesdatenschutzbeauftragte und die Rechtsanwaltskammern bei Ausübung der Datenschutzaufsicht über die Mitglieder der Rechtsanwaltskammer eng zusammenarbeiten. Vorstellbar wäre nach unserer Auffassung insoweit eine Kooperation im Wege der Amtshilfe. Im konkreten Einzelfall könnten hierdurch die Aufsichtsbefugnisse des Landesdatenschutzbeauftragten gegenüber den Rechtsanwältinnen und Rechtsanwälten durch die zuständigen Rechtsanwaltskammern wahrgenommen werden. Parallel dazu benennen die Rechtsanwaltskammern Baden-Württembergs einen gemeinsamen Datenschutzbeauftragten, der die Mitglieder der Rechtsanwaltskammern und die Rechtsanwaltskammern bei der Wahrnehmung ihrer Aufgaben beratend unterstützt.

Gemäß § 27 des Entwurfs dürfen gegen öffentliche Stellen keine Geldbußen verhängt werden. Die Rechtsanwaltskammer Stuttgart begrüßt dies ausdrücklich. Kritisch wird hingegen die Einschränkung gesehen, dass Geldbußen dann verhängt werden können, wenn die öffentliche Stelle als Unternehmen mit eigener Rechtspersönlichkeit am Wettbewerb teilnimmt. Insoweit spricht sich die Kammer dafür aus, dass das Verbot gegen öffentliche Stellen Geldbußen zu verhängen, umfassende Wirkung hat.

Mit freundlichen Grüßen

A handwritten signature in blue ink, appearing to read 'H. Milsch', is written over the printed name.

i.A.  
Heidi Milsch  
Geschäftsführerin  
Rechtsanwältin



Rechtsanwaltskammer Tübingen  
Christophstraße 30 • 72072 Tübingen

**Nur per mail**  
Ministerium für Inneres, Digitalisierung und Migration  
Baden-Württemberg  
Willy-Brandt-Straße 41  
70173 Stuttgart

■ **Präsident**

Christophstraße 30  
72072 Tübingen

E-Mail: [info@rak-tuebingen.de](mailto:info@rak-tuebingen.de)  
Internet: [www.rak-tuebingen.de](http://www.rak-tuebingen.de)

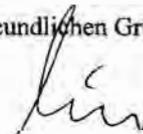
Tübingen, den 31.01.2018

**Gesetz zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679**

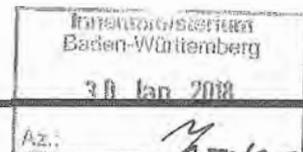
Sehr geehrte Frau

die Rechtsanwaltskammer Tübingen schließt sich ausdrücklich der Stellungnahme der Rechtsanwaltskammer Stuttgart gemäß Schreiben vom 31.01.2018 an. Auch die Rechtsanwaltskammer Tübingen befürwortet eine entsprechende Zusammenarbeit zwischen dem Landesdatenschutzbeauftragten und den Rechtsanwaltskammern, wonach die Aufsichtsbefugnisse des Landesdatenschutzbeauftragten über die Rechtsanwältinnen und Rechtsanwälte von der jeweils zuständigen Rechtsanwaltskammer wahrgenommen werden.

Mit freundlichen Grüßen



Albrecht Luther  
Rechtsanwalt  
(Präsident)



**Von:** Dreßler, Dr. Tomas (RPF)  
**Gesendet:** Montag, 29. Januar 2018 17:19  
**An:** Registratur 2 (IM)  
**Cc:**  
**Betreff:** Entwurf eines Gesetzes zur Anpassung des allg. Datenschutzrechts u.a.

Sehr geehrte Damen und Herren,

wir bedanken uns für die Gelegenheit zur Stellungnahme zu dem übersandten Gesetzentwurf.

1.

Weil das in der Gesetzesbegründung mehrfach angesprochene Wiederholungsverbot offenbar eine Kodifikation aus einem Guss verbietet, bleibt das neue Landesdatenschutzgesetz leider „Flickwerk“. Der Entwurf enthält daher nur ergänzende Regelungen, soweit die EU-Öffnungsklausel gesetzgeberischen Spielraum lässt und nach Auffassung des Landesgesetzgebers geeignet, erforderlich und verhältnismäßig erscheinen. Dies bedeutet, dass die EU-DSGVO stets mitgelesen werden muss.

Dies soll an einem Beispiel verdeutlicht werden:  
Datenverarbeitung zu anderen Zwecken (sog. Zweckdurchbrechung).  
Allein die Ausnahmen sind künftig in § 5 LDSG geregelt, aber auch nur, soweit sie nicht bereits in der DS-GVO zugelassen sind.

Das IM wird gebeten, nach Erlass des LDSG einen Gesamtkontext aus DS-GVO und LDSG zur Verfügung zu stellen, um den Behörden die Gesetzesanwendung zu erleichtern.

2.

Anmerkung zu § 6 Abs. 1 S. 2 Entwurf LDSG (Übermittlung auf Ersuchen)

Die im bisherigen § 16 Abs. 2 LDSG (alt) vorgenommene Verlagerung der grds. Verantwortung für die Zulässigkeit der Übermittlung auf die ersuchende Behörde soll im Entwurf des LDSG beibehalten bleiben. Dies steht im Widerspruch zur grundsätzlichen Verantwortlichkeit der verarbeitenden Stelle für die Nutzung bzw. Weitergabe nach Art. 6 EU-DSGVO. Die Gründe, weshalb von diesem Grundsatz abgewichen wird bzw. im Rahmen der Öffnungsklausel abgewichen werden darf, lassen sich der Gesetzesbegründung S. 17 nicht entnehmen. Die Gesetzesbegründung schweigt zu dieser doch zentralen Ausnahmeregelung.

Mit freundlichen Grüßen

*Dr. Tomas Dreßler*  
Datenschutzbeauftragter des Regierungspräsidiums Freiburg



2-0557.8/1/145

---

**Von:** - Stbk Stuttgart  
**Gesendet:** Donnerstag, 1. Februar 2018 15:35  
**An:** Registratur 2 (IM)  
**Cc:**  
**Betreff:** Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679

**Ihr Schreiben vom 19.12.2017**  
**Aktenzeichen 2-0557.8/1**

---

Sehr geehrter Herr

wir nehmen gerne die Gelegenheit wahr, zu Ihrem Schreiben vom 19.12.2017 Stellung zu nehmen.

In unserer Stellungnahme wollen wir auf das Schreiben der Architektenkammer Baden-Württemberg vom 31.01.2018 an Ihr Ministerium verweisen. Wir schließen uns den Ausführungen in der Stellungnahme der Architektenkammer Baden-Württemberg vollinhaltlich an.

Insbesondere gilt dies für die Hinweise im Schreiben der Architektenkammer Baden-Württemberg unter 1. und 3., wo angeregt wird, die Ausnahmeregelungen in §§ 4 und 5 LDSG (neu) auszudehnen auf das „Recht auf Einschränkung der Verarbeitung“ (Artikel 18 EU DSGVO) und auf das „Widerspruchsrecht“ nach Artikel 21 EU DSGVO.

Mit freundlichen Grüßen

Kürner  
-Geschäftsführer-

Steuerberaterkammer Stuttgart  
-Körperschaft des öffentlichen Rechts-  
Hegelstraße 33  
70174 Stuttgart

E-Mail: [mail@stbk-stuttgart.de](mailto:mail@stbk-stuttgart.de)  
Internet: [www.stbk-stuttgart.de](http://www.stbk-stuttgart.de)



SWR Postfach 37 40 55027 Mainz

Ministerium für Inneres, Digitalisierung  
und Migration Baden-Württemberg  
Postfach 10 34 65  
70029 Stuttgart

Südwestrundfunk  
Anstalt des öffentlichen Rechts

Der Justitiar  
Am Fort Gonsenheim 139  
55122 Mainz  
Telefon 06131 929 32900  
Telefax 06131 929 32090

Per E-Mail: [Registatur2@im.bwl.de](mailto:Registatur2@im.bwl.de)

31. Januar 2018

## Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679

Sehr geehrte Damen und Herren,

wir bedanken uns für die Möglichkeit einer Stellungnahme zum Entwurf eines landesrechtlichen Datenschutzanpassungsgesetzes an die EU-Datenschutz-Grundverordnung (insbesondere Änderung des LDSG BW). Unsere Anmerkungen zu den Dokumenten vom 14.12.2017 (Text und Begründung) beschränken sich auf die nachfolgenden drei Punkte:

### 1. Klarstellung des Vorrangs bereichsspezifischer Vorschriften:

In § 2 Abs. 3 des Entwurfs ist festgehalten, dass spezielle Vorschriften vorgehen. Aufgrund des Umfangs und der praktischen Bedeutung des Rundfunkbeitragseinzugs mit seinen 7,2 Millionen Rundfunkteilnehmern im Bereich des SWR (Baden-Württemberg und Rheinland-Pfalz) regen wir an, *in der Begründung* zu § 2 Abs. 3 (Seite 10 des Begründungsteils) nach dem ersten Satz zur Begründung von Abs. 3 einzufügen:

*„Dies gilt beispielsweise auch für die als Landesgesetz erlassenen Regelungen des Rundfunkbeitrags-Staatsvertrages.“*

### 2. Regelungen zum Auskunftsrecht (§ 9):

Im Text von § 9 Abs. 1 Satz 2 wird festgehalten, dass keine Auskunft verlangt werden kann, soweit die Daten ausschließlich zu Zwecken der Datensicherung gespeichert sind. Keine Regelung wird für Daten getroffen, die nur deshalb gespeichert sind, weil sie nur noch aufgrund zwingender gesetzlicher Aufbewahrungsvorschriften gespeichert sind. Nach Art. 23 Abs. 1 Ziff. e der EU-Datenschutz-Grundverordnung können Einschränkungen bei den Rechten der Betroffenen erfolgen, u.a. wenn öffentliche finanzielle Interessen berührt sind. Genannt wird insbesondere der Haushalts- und Steuerbereich (worunter auch landesgesetzliche Steuern oder Abgaben oder der Rundfunkbeitrag fallen dürften). Wie bei Landes- und Kommunalbehörden werden auch im Rahmen des Beitragseinzugs personenbezogene Daten gespeichert, die nur noch deshalb gespeichert sind und nicht gelöscht wurden, weil Aufbewahrungsvorschriften aus

Der SWR ist Mitglied der Arbeitsgemeinschaft  
der öffentlich-rechtlichen Rundfunkanstalten  
der Bundesrepublik Deutschland (ARD) ©



haushaltsrechtlichen, steuerrechtlichen oder handelsrechtlichen Vorschriften bestehen. Eine Auskunft hierüber sollte in diesen Bereichen des strikten Gesetzesvollzugs beschränkt werden können. Notwendig und ausreichend ist für die Betroffenen lediglich eine Auskunft über die aktuellen Daten. Wir schlagen deshalb vor, § 9 Abs. 1 Satz 2 wie folgt zu ergänzen:

„Die betroffene Person kann ferner keine Auskunft verlangen, soweit und solange die personenbezogene Daten ausschließlich zu Zwecken der Datensicherung, der Datenschutzkontrolle oder nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen und eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist und deswegen das Interesse der betroffenen Person an der Auskunftserteilung zurücktreten muss.“

### 3. Regelungen zum Rundfunkbeauftragten für den Datenschutz (§ 26):

Zu § 26 möchten wir folgende drei Punkte vortragen:

#### a) Regelung zu Besoldung in Abs. 3 Satz 3:

Nach dem bisherigen Wortlaut sollen die näheren Bestimmungen der Vergütung in einer Satzung geregelt werden. Eine Satzung muss aber veröffentlicht werden und dies würde deshalb bedeuten, dass letztlich das konkrete Gehalt und zwar in Bezug auf die konkrete Situation veröffentlicht wird (und nicht nur abstrakt wie beispielsweise beim Landesdatenschutzbeauftragten, bei dem nur die möglichen Komponenten wie Familienzuschlag aufgeführt sind). Nach unserer Auffassung gibt es zwei Möglichkeiten diesen Eingriff in das Persönlichkeitsrecht des Rundfunkbeauftragten zu vermeiden:

Entweder es werden am Ende von Abs. 3 Satz 3 lediglich die Worte „in einer Satzung“ weggelassen oder aber, es werden statt diesen drei Wörtern eingefügt „in entsprechender Anwendung von § 22 Abs. 4“.

#### b) Andere bzw. sonstige Aufgaben des Rundfunkbeauftragten für den Datenschutz (Abs. 4 Sätze 1 und 2):

Nach Abs. 4 Satz 1 kann das Amt des Rundfunk-Datenschutzbeauftragten „nicht neben anderen Aufgaben“ wahrgenommen werden. In Satz 2 heißt es, „sonstige Aufgaben“ müssten mit dem Amt vereinbar sein. Nach unserer Auffassung sind dies widersprüchliche Aussagen. Ausgangspunkt einer landesrechtlichen Regelung ergeben sich für diese Fragen aus Art. 52 Abs. 3 EU-Datenschutz-Grundverordnung. Danach muss von allen Aufgaben bei der Amtsausübung abgesehen werden, die als damit „nicht zu vereinbarende Handlungen“ anzusehen sind. Die EU-Verordnung stellt also auf die Aufgaben und deren Unvereinbarkeit und nicht den Umfang von Tätigkeiten ab. Die Intention des Gesetzgebers, einen hauptamtlichen Datenschutzbeauftragten und nicht nur eine Teilzeittätigkeit zu schaffen, ist uns indessen bewusst. Dies könnte aber auch in der Gesetzesbegründung zum Ausdruck kommen. Im Übrigen wird damit einer im Rahmen der Zusammenarbeit der ARD notwendigen Flexibilität entgegen gewirkt. Denn wir halten es durchaus für denkbar, dass der Datenschutzbeauftragte des SWR beispielsweise auch gleichzeitig Datenschutzbeauftragter des SR sein könnte (wenn alle Gremien der beiden Anstalten dies wünschten und entsprechende Personalkapazitäten im Unterbau vorhanden sind).



Die Sätze 1 und 2 könnten deshalb durch folgenden Satz ersetzt werden:

*„Die oder der Rundfunkbeauftragte für den Datenschutz kann nur in geringfügigem Umfang andere Aufgaben wahrnehmen, sofern diese anderen Tätigkeiten mit der Aufgabenerfüllung des Amtes vereinbar sind und ihre oder seine Unabhängigkeit nicht gefährden. „*

c) Klarstellung zum Fortbestand der Amtszeit des bisherigen Rundfunk-Datenschutzbeauftragten:

In der Begründung wird im Hinblick auf Art. 85 EU-Verordnung unter Ziff. 2 f auf den Seiten 4/5 festgestellt, dass bereits die jetzigen Regelungen in § 39 des Staatsvertrages über den SWR „in Einklang mit der Verordnung (EU) 2016/679“ stehen.

Der Rundfunkrat des SWR hat am 18. Juli 2014 mit Zustimmung des Verwaltungsrats am 19.9.2014 den Rundfunkbeauftragten für den Datenschutz für die Zeit ab 1. Oktober und für die Dauer von 8 Jahren (und damit bis zum 30.9.2022) bestellt. Dies geschah aufgrund Art. 39 SWR-Staatsvertrag in Verbindung mit § 38 LDSG BW, deren Regelungen zur Bestellung bereits mit der Änderung des SWR-StV den europarechtlichen Erfordernissen und den Entscheidungen des EuGH angepasst worden waren. Die Änderungen des LDSG machen deshalb weder eine Neuwahl erforderlich, noch wäre diese aufgrund der Entscheidung des EuGH vom 8. April 2014 (C-288/12) zulässig (kein Eingriff in bestehende Amtszeiten). Auch dürfte ein Eingriff des Gesetzgebers in die von Staatsferne geprägten autonomen Entscheidungen des Rundfunkrates und Verwaltungsrates nicht gewollt sein. Wie beim LfD bleibt es deshalb bei der Amtszeit des jetzt gewählten Rundfunk-Datenschutzbeauftragten bis zu deren Ablauf zum 30.9.2022. Dies sollte aber entweder im Text, oder aber der Begründung **klargestellt** werden.

Eine **textliche Klarstellung** könnte in § 30 (Überleitungsvorschriften) erfolgen und zwar dergestalt, dass am Ende von Abs. 2 steht:

*„Die Amtszeit des von den Gremien des SWR gewählten gegenwärtigen Rundfunkbeauftragten für den Datenschutz, der bereits den gesetzlichen Anforderungen entspricht, endet zum 30. September 2022.“*

Möglich wäre auch, diesen klarstellenden Satz **in die Begründung** aufzunehmen und zwar am sinnvollsten am Ende der Begründung zu § 26. Danach könnte noch zur Erläuterungen eingefügt werden:

*Die Änderungen des LDSG erfordern weder eine Neuwahl noch einen Eingriff des Gesetzgebers in die von Staatsferne geprägten autonomen Entscheidungen der SWR-Gremien und berücksichtigen die Entscheidung des EuGH vom 8. April 2014 (C-288/12).*

Mit freundlichen Grüßen

A handwritten signature in blue ink, appearing to read 'H. Eicher', written in a cursive style.

Dr. Hermann Eicher



Vorstand

Klinikumsvorstand • Hoppe-Seyler-Straße 6 • 72076 Tübingen

Ministerium für Inneres, Digitalisierung und  
Migration Baden-Württemberg

Hoppe-Seyler-Straße 6  
72076 Tübingen  
Telefon 07071 29-88500  
Fax 07071 29-25031

- per E-Mail -

31. Januar 2018

**Aktenzeichen 2-0557.8/1**

**Entwurf eines Gesetzes zur Anpassung des allgemeinen Daten-  
schutzrechts und sonstiger Vorschriften an die Verordnung (EU)  
2016/679**

Sehr geehrte Frau

nachfolgend übersenden wir Ihnen die Stellungnahme zum oben  
genannten Gesetzesentwurf seitens des Universitätsklinikums  
Tübingen. Bei Rückfragen stehen wir Ihnen selbstverständlich gerne  
zur Verfügung

Mit freundlichen Grüßen

Prof. Dr. med. Michael Bamberg  
Leitender Ärztlicher Direktor  
und Vorstandsvorsitzender

Gabriele Sonntag  
Kaufmännische Direktorin

Universitätsklinikum Tübingen  
Anstalt des öffentlichen Rechts  
Sitz Tübingen  
Geissweg 3 • 72076 Tübingen  
Tel. 07071 29-0  
www.medizin.uni-tuebingen.de  
Steuer-Nr. 86156/09402  
USt.-ID: DE 146 889 674

Aufsichtsrat  
Ulrich Steinbach (Vorsitzender)

Vorstand  
Prof. Dr. Michael Bamberg (Vorsitzender)  
Gabriele Sonntag (Stellv. Vorsitzende)  
Prof. Dr. Karl Ulrich Bartz-Schmidt  
Prof. Dr. Ingo B. Autenrieth  
Klaus Tischler

Baden-Württembergische Bank Stuttgart  
BLZ 600 501 01 Konto-Nr. 7477 5037 93  
IBAN: DE41 6005 0101 7477 5037 93  
BIC (SWIFT-Code): SOLADEST600  
Kreissparkasse Tübingen  
BLZ 641 500 20 Konto-Nr. 14 144  
IBAN: DE79 6415 0020 0000 0141 44  
BIC (SWIFT-Code): SOLADES1TUB



Vorstand

## LDSG BaWü neu (Referentenentwurf vom 14.12.2017) Stellungnahme (Vorlage/Entwurf, Stand 29.1.2018)

Hinweis: Die Stellungnahme teilt sich in die Teile  
zur wissenschaftlichen Forschung (A) und allgemein zum Gesetzestext (B)

### A Wissenschaft, Forschung im Referentenentwurf

#### Allgemein

Es ist auch in unseren Augen sinnvoll, wenn die föderative Gesetzgebung nicht zu sehr voneinander abweicht, um über Landesgrenzen hinweg eine sinnvolle und effiziente Zusammenarbeit zu ermöglichen. Allerdings sollte das Ziel gleichzeitig sein, den Wissenschaftsstandort Baden-Württemberg nicht unangemessen einzuschränken (insbesondere im Vergleich mit anderen Bundesländern), ihn vielmehr zu stärken. Entsprechend ist ein Ansatz gefragt, der eine Ausgewogenheit zwischen diesen Zielen gewährleistet.

#### 1. Regelungen der DS-GVO als Basis

Es ist nur eine Option des nationalen Gesetzgebers, die Regelungen der DS-GVO zur Forschung durch nationale Regelungen zu konkretisieren und einzuschränken, kein Muss (Art.9 Abs.4 DS-GVO). Soweit von dieser Option nicht Gebrauch gemacht würde (also keinerlei Regelung zur Wissenschaft im Landesrecht, unmittelbare Geltung der DS-GVO), wäre die Situation folgende:

- Gesundheitsdaten dürften von den Universitätsklinika/Universitäten genutzt werden, wenn die **Verarbeitung zur wissenschaftlichen Forschung erforderlich** ist (Art.9 Abs. 2j i.V.m. Abs.1 DS-GVO verkürzt).
- Dabei gilt die **Weiterverarbeitung/Zweckänderung** von Gesundheitsdaten, die für die Versorgung erhoben wurden, als **vereinbar mit dem ursprünglichen Zweck und rechtmäßig**. Die Zulässigkeit ergibt sich aus der initialen Rechtsgrundlage (Erwägungsgrund 50 DS-GVO verkürzt). Für die Vereinbarkeit gibt es weitere (aus unserer Sicht erfüllbare) Voraussetzungen.
- Die Verarbeitung muss geeigneten **Garantien für die Rechte und Freiheiten des Betroffenen** unterliegen (Art.89 Abs.1 DS-GVO verkürzt). Der Katalog von Garantien umfasst aus unserer Sicht neben den herausgehobenen Pseudonymisierungsansätzen u.a. Alles, was in aktuellen wissenschaftlichen Initiativen mit dem Oberbegriff „**Governance**“ zusammengefasst wird.

Fazit: Mit diesen Regelungen **könnten die Universitätsklinika/med.Fakultäten leben**. Sie sind darauf vorbereitet und sehen das in ihren Konzepten für aktuelle Projekte/Initiativen stets vor. Diese Ansätze ermöglicht die Forschung, die im Interesse der Allgemeinheit heute erhebliche Fortschritte verspricht. Es ist nicht nachvollziehbar, warum einschränkende Regelungen erforderlich sind. Zu lösen ist dann noch der Zielkonflikt zwischen dem Grundsatz der Datenminimierung und BigData-Ansätzen; dies ist jedoch durch die nationale Gesetzgebung nicht beeinflussbar.

Universitätsklinikum Tübingen  
Anstalt des öffentlichen Rechts  
Sitz Tübingen  
Geissweg 3 + 72076 Tübingen  
Tel. 07071 29-0  
www.medizin.uni-tuebingen.de  
Steuer-Nr. 86156/09402  
USt.-ID: DE 146 889 674

Aufsichtsrat  
Ulrich Steinbach (Vorsitzender)

Vorstand  
Prof. Dr. Michael Bamberg (Vorsitzender)  
Gabriele Sonntag (Stellv. Vorsitzende)  
Prof. Dr. Karl Ulrich Bartz-Schmidt  
Prof. Dr. Ingo B. Autenrieth  
Klaus Tischler

Baden-Württembergische Bank Stuttgart  
BLZ 600 501 01 Konto-Nr. 7477 5037 93  
IBAN: DE41 6005 0101 7477 5037 93  
BIC (SWIFT-Code): SOLADEST600

Kreissparkasse Tübingen  
BLZ 641 500 20 Konto-Nr. 14 144  
IBAN: DE79 6415 0020 0000 0141 44  
BIC (SWIFT-Code): SOLADES1TUB



Vorstand

## 2. Wirkung der nationalen Gesetzgebung gemäß vorliegendem Entwurf

Der vorliegende Entwurf der Regelungen im LDSG-neu stellt (verkürzt dargestellt) folgende zusätzliche Bedingungen auf:

- Die Zwecke der Verarbeitung dürfen **anders nicht oder nur mit unverhältnismäßigem Aufwand** erreichbar sein. Der entsprechende Nachweis müsste stets geführt werden.
- Die Interessen der Universitätsklinik/med.Fakultäten müssen die Interessen der betroffenen Person am Unterlassen **erheblich überwiegen**.

Begründet werden diese Regelungen mit:

- Im Interesse der Wissenschafts- und Forschungsfreiheit soll die Verarbeitung von Gesundheitsdaten zugelassen werden (sinngemäß)
- Einschränkungen sind soweit vorgesehen, wie es die informationelle Selbstbestimmung gebietet.

Festzustellen ist aus unserer Sicht hierzu:

- Ohne die landesrechtlichen Regelungen gemäß vorliegendem Entwurf hätten wir mit den Regelungen der DS-GVO eine geeignete Basis für die heute anstehenden wissenschaftlichen Herausforderungen im Interesse der Allgemeinheit.
- Natürlich muss das Recht auf informationelle Selbstbestimmung gewährleistet sein. Dies gebietet das Urteil des Bundesverfassungsgerichtes zur Volkszählung 1983. Danach sind Einschränkungen dieses Rechts nur im überwiegenden Allgemeininteresse möglich.
- Der vorliegenden Entwurf (wie im BDSG-neu übrigens, aus dem er offensichtlich übernommen wurde) wiegt aber die Interessen der Uniklinika/med.Fakultäten gegen die Interessen der betroffenen Person auf. Das Allgemeininteresse bleibt im Gegensatz zu früheren gesetzlichen Formulierungen außen vor.
- Der Nachweis der Unmöglichkeit anderer Lösungen bzw. deren zu großer Aufwand sowie das „**erhebliche Überwiegen**“ als unbestimmter Rechtsbegriff eröffnet einen zu großen Interpretationsspielraum und erzeugen einen unangemessenen Argumentationszwang und -aufwand. Das Bundesverfassungsgericht selbst verwendete nur den Begriff „überwiegendes Allgemeininteresse“.
- Beides (c und d) halten wir nicht für sachgerecht, da wir der Überzeugung sind, dass anstehende Forschungsprojekte und -initiativen erhebliche Fortschritte im Interesse der Allgemeinheit erbringen können.
- Darüber hinaus meinen wir, dass die DS-GVO die informationelle Selbstbestimmung bereits hinreichend berücksichtigt und zusätzliche Regelungen an sich nicht erforderlich wären.
- Der neue hippokratische Eid verpflichtet die Ärzte, medizinisches Wissen zum Wohl der Patienten und zur Förderung der Gesundheitsversorgung mit ihren Kollegen zu teilen. Dem sollten keine unangemessenen Schranken im Wege stehen.

Universitätsklinikum Tübingen  
Anstalt des öffentlichen Rechts  
Sitz Tübingen  
Geissweg 3 • 72076 Tübingen  
Tel. 07071 29-0  
www.medizin.uni-tuebingen.de  
Steuer-Nr. 86156/09402  
USt.-ID: DE 146 889 674

Aufsichtsrat  
Ulrich Steinbach (Vorsitzender)

Vorstand  
Prof. Dr. Michael Bamberg (Vorsitzender)  
Gabriele Sonntag (Stellv. Vorsitzende)  
Prof. Dr. Karl Ulrich Bartz-Schmidt  
Prof. Dr. Ingo B. Autenrieth  
Klaus Tischler

Baden-Württembergische Bank Stuttgart  
BLZ 600 501 01 Konto-Nr. 7477 5037 93  
IBAN: DE41 6005 0101 7477 5037 93  
BIC (SWIFT-Code): SOLADEST600  
Kreissparkasse Tübingen  
BLZ 641 500 20 Konto-Nr. 14 144  
IBAN: DE79 6415 0020 0000 0141 44  
BIC (SWIFT-Code): SOLADES1TUB



Vorstand

### 3. Vorschlag/Forderung

Soweit möglich, könnten einschränkende nationale Regelungen analog zum Entwurf aus Bayern - entfallen.

Sollte dies nicht möglich sein, schlagen wir vor, ausgewogene Interessenlagen durch eine Formulierung wie die z.B. folgende herzustellen:

Öffentliche Stellen dürfen besondere Kategorien personenbezogener Daten für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke verarbeiten, sofern

- a. die Einholung einer Einwilligung der betroffenen Person nicht möglich ist oder mit einem unverhältnismäßigen Aufwand verbunden wäre,
- b. das Interesse der öffentlichen Stelle das Interesse der betroffenen Person an einem Ausschluss der Verarbeitung überwiegt,
- c. die Verarbeitung erhebliche Fortschritte im Allgemeininteresse ermöglicht<sup>1</sup> und
- d. die Verarbeitung geeigneten Garantien für die Rechte und Freiheiten der betroffenen Person gemäß der Verordnung (EU) 2016/679 unterliegt.

Besondere Kategorien personenbezogener Daten sind die in Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 genannten Daten.

Mit einer solchen Formulierung könnten die Universitätsklinika/med.Fakultäten ebenfalls „leben“. Sie ermöglicht die Umsetzung der anstehenden Projekte und Initiativen eher als der bisherige Entwurf. Alternativ könnte man sich an Vorlagen aus anderen Bundesländern (siehe unten) orientieren.

### 4. Vergleich mit anderen Bundesländern

**Bayern:** Der dortige Entwurf stellt keine zusätzlichen Voraussetzungen auf. Statt des Absatzes 1 des LDSG-BaWü neu legt der bayrische Entwurf die Zweckbindung von für wissenschaftliche Zwecke erhobenen Daten fest. Der restliche Regelungsgehalt entspricht sinngemäß dem der Absätze 2 bis 4 des LDSG BaWü neu.

**Fazit:** Im Vergleich zu Bayern klare **Nachteile durch den baden-württembergischen Entwurf.**

**Brandenburg:** „Öffentliche Stellen dürfen personenbezogene Daten einschließlich Daten im Sinne von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ohne Einwilligung für ein bestimmtes Forschungsvorhaben verarbeiten und an andere Stellen oder Personen zu diesem Zweck übermitteln, wenn schutzwürdige Belange der betroffenen Person wegen der Art der Daten, wegen ihrer Offenkundigkeit oder wegen der Art der Verwendung nicht beeinträchtigt werden oder das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange der betroffenen

<sup>1</sup> Alternative: „erwarten lässt“

Universitätsklinikum Tübingen  
Anstalt des öffentlichen Rechts  
Sitz Tübingen  
Geisweg 3 + 72076 Tübingen  
Tel. 07071 29-0  
www.medizin.uni-tuebingen.de  
Steuer-Nr. 86156/09402  
USt.-ID: DE 146 889 674

Aufsichtsrat  
Ulrich Steinbach (Vorsitzender)

Vorstand  
Prof. Dr. Michael Bamberg (Vorsitzender)  
Gabriele Sonntag (Stellv. Vorsitzende)  
Prof. Dr. Karl Ulrich Bartz-Schmidt  
Prof. Dr. Ingo B. Autenrieth  
Klaus Tischler

Baden-Württembergische Bank Stuttgart  
BLZ 600 501 01 Konto-Nr. 7477 5037 93  
IBAN: DE41 6005 0101 7477 5037 93  
BIC (SWIFT-Code): SOLADEST600

Kreissparkasse Tübingen  
BLZ 641 500 20 Konto-Nr. 14 144  
IBAN: DE79 6415 0020 0000 0141 44  
BIC (SWIFT-Code): SOLADES1TUB



Vorstand

Person überwiegt und der Zweck der Forschung nicht auf andere Weise erreicht werden kann. Die übermittelten Daten dürfen nicht für andere Zwecke verarbeitet werden.“

**Fazit:** Kein „erhebliches Überwiegen“; insgesamt wäre diese Formulierung auch sehr gut geeignet. Im Vergleich **klare Nachteile für Baden-Württemberg.**

**Mecklenburg-Vorpommern:** Nahezu wortgleich zu Brandenburg.

**Fazit:** Im Vergleich **klare Nachteile für Baden-Württemberg.**

**Sachsen:** „Die Verarbeitung personenbezogener Daten einschließlich solcher nach Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 zu wissenschaftlichen oder historischen Forschungszwecken ist zulässig, soweit dies für die Durchführung der wissenschaftlichen oder historischen Forschung erforderlich ist, insbesondere der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann, und wenn das öffentliche, insbesondere das wissenschaftliche oder historische Interesse an der Durchführung des Forschungsvorhabens das Interesse der betroffenen Person am Unterbleiben der Verarbeitung überwiegt.“

**Fazit:** Kein „erhebliches Überwiegen“; insgesamt wäre diese Formulierung auch sehr gut geeignet. Im Vergleich **klare Nachteile für Baden-Württemberg.**

## B Sonstige Bereiche des Entwurfs

### § 2 Anwendungsbereich

- a. Abs.6 „Unternehmen mit eigener Rechtspersönlichkeit“

Es wäre hilfreich/sinnvoll, hier zu definieren (zumindest in der Begründung), von welchem Unternehmensbegriff hier ausgegangen wird (angelehnt an Handelsrecht, Wettbewerbsrecht, Steuerrecht oder anderer?). Insbesondere, ob die Uniklinika als Anstalten des öffentlichen Rechts als solche gelten sollen.

### § 3 Sicherstellung des Datenschutzes

- a. Es handelt sich in weiten Teilen nicht um Konkretisierungen der DS-GVO-Regelungen sondern um Wiederholungen, aber teilweise dann doch nicht wortgleich und eindeutig formuliert. Das kann zu Verwirrung führen, der Normenklarheit schaden. Hier sollte auf eine redundante Wiederholung der Formulierungen aus der DS-GVO verzichtet werden. Unter Hinweis auf deren Ergänzung sollten die ergänzenden Regelungen des Landes aufgeführt werden.

Universitätsklinikum Tübingen  
Anstalt des öffentlichen Rechts  
Sitz Tübingen  
Geissweg 3 • 72076 Tübingen  
Tel. 07071 29-0  
www.medizin.uni-tuebingen.de  
Steuer-Nr. 86156/09402  
USt.-ID: DE 146 889 674

Aufsichtsrat  
Ulrich Steinbach (Vorsitzender)  
  
Vorstand  
Prof. Dr. Michael Bamberg (Vorsitzender)  
Gabriele Sonntag (Stellv. Vorsitzende)  
Prof. Dr. Karl Ulrich Bartz-Schmidt  
Prof. Dr. Ingo B. Autenrieth  
Klaus Tischler

Baden-Württembergische Bank Stuttgart  
BLZ 600 501 01 Konto-Nr. 7477 5037 93  
IBAN: DE41 6005 0101 7477 5037 93  
BIC (SWIFT-Code): SOLADEST600  
Kreissparkasse Tübingen  
BLZ 641 500 20 Konto-Nr. 14 144  
IBAN: DE79 6415 0020 0000 0141 44  
BIC (SWIFT-Code): SOLADES1TUB



Vorstand

## **§ 5 Datenverarbeitung zu anderen Zwecken**

---

- a. Abs.1: „soweit die Verarbeitung notwendig und verhältnismäßig ist.“ statt „erforderlich“  
Die Formulierung „notwendig und verhältnismäßig“ in der Verordnung, auf die Bezug genommen wird, bezieht sich in der Verordnung nicht auf eine Verarbeitung sondern auf eine Rechtsvorschrift als Maßnahme zum Schutz von in Artikel 23 genannten Zielen.
- b. § 5 Abs.4: „gespeichert“  
Alter Begriff, nicht definiert. Müsste „verarbeitet“ lauten.

## **§ 5 Datenverarbeitung zu anderen Zwecken**

---

- a. Abs.1: „soweit die Verarbeitung notwendig und verhältnismäßig ist.“ statt „erforderlich“  
Die Formulierung „notwendig und verhältnismäßig“ in der Verordnung, auf die Bezug genommen wird, bezieht sich in der Verordnung nicht auf eine Verarbeitung sondern auf eine Rechtsvorschrift als Maßnahme zum Schutz von in Artikel 23 genannten Zielen.
- b. § 5 Abs.4: „gespeichert“  
Alter Begriff, nicht definiert. Müsste „verarbeitet“ lauten.

## **§ 6 Übermittlung personenbezogener Daten**

---

- a. Begründung: „Nach der Verordnung (EU) 2016/679 wird die Übermittlung personenbezogener Daten wie eine Zweckänderung behandelt.“  
Erforderlich ist eine Klarstellung, auf welchen Artikel oder Erwägungsgrund der Verordnung sich dies bezieht.

## **§ 9 Beschränkung des Auskunftsrechts**

---

- b. Abs.2 : Differenzierung des Auskunftsumfangs  
Sehr gut vor dem Hintergrund der Vielfalt und Komplexität der Datenbestände in Krankenhäusern, speziell Uniklinika. Unbedingt beibehalten.

## **§ 12 Verarbeitung personenbezogener Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen**

---

- c. Abs.2, Nr.2: „die Voraussetzungen des § 5 Absatz 1 Nummern 1 oder 2 vorliegen und die zur Verschwiegenheit verpflichtete Stelle eingewilligt hat“  
Ergänzung zu“ (...) §5 Absatz 1 Nummern 1 oder 2 oder § 13 Abs.1 Satz 1 (...) . Sonst widersprechen sich durch das „nur“ in § 12 Abs.2 Satz 1 die §§ 12 und 13 bzw. fehlt die Klarheit.

Universitätsklinikum Tübingen  
Anstalt des öffentlichen Rechts  
Sitz Tübingen  
Geisweg 3 + 72076 Tübingen  
Tel. 07071 29-0  
www.medizin.uni-tuebingen.de  
Steuer-Nr. 86156/09402  
USt.-ID: DE 146 889 674

Aufsichtsrat  
Ulrich Steinbach (Vorsitzender)

Vorstand  
Prof. Dr. Michael Bamberg (Vorsitzender)  
Gabriele Sonntag (Stellv. Vorsitzende)  
Prof. Dr. Karl Ulrich Bartz-Schmidt  
Prof. Dr. Ingo B. Autenrieth  
Klaus Tischler

Baden-Württembergische Bank Stuttgart  
BLZ 600 501 01 Konto-Nr. 7477 5037 93  
IBAN: DE41 6005 0101 7477 5037 93  
BIC (SWIFT-Code): SOLADEST600

Kreissparkasse Tübingen  
BLZ 641 500 20 Konto-Nr. 14 144  
IBAN: DE79 6415 0020 0000 0141 44  
BIC (SWIFT-Code): SOLADES1TUB



Vorstand

### **§ 13 Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken**

---

Hierzu nehmen die Universitätsklinikum in ihrer Stellungnahme gegenüber dem Ministerium als unmittelbare Adressaten der Beteiligung selbst Stellung.

### **§ 14 Datenverarbeitung bei Dienst- und Arbeitsverhältnissen, Zuverlässigkeitsüberprüfung**

---

- a. Abs.8: Da es sich hier nicht ausschließlich um Beschäftigte handelt („Besucher“) ist der Absatz fehl am Platz. Der Bezug zu Abs.1 Satz 1 macht auch nicht eindeutig Sinn. Das gehört eher zu Sicherheitsmaßnahmen.

### **§ 27 Ordnungswidrigkeiten**

---

- a. „Gegen öffentliche Stellen im Sinne des § 2 Absatz 1 und 2 dürfen keine Geldbußen verhängt werden, es sei denn, die öffentlichen Stellen nehmen als Unternehmen mit eigener Rechtspersönlichkeit am Wettbewerb teil.“

Der zweite Halbsatz ist obsolet, da für diese Unternehmen gemäß §2 diese Regelungen ohnehin nicht gelten.

### **§ 28 Strafvorschrift**

---

1. Abs.1 Nr.1a: „speichert, nutzt, verändert, übermittelt oder löscht“  
Begriffe aus dem alten Datenschutzrecht. Müssten durch „verarbeitet“ ersetzt werden. Damit könnte bei künftigen Verpflichtungen hierauf auch gut Bezug genommen werden.
2. Abs.1 Nr.2: „die Übermittlung (...) erschleicht“  
Im Gegensatz zum alten Datenschutzrecht (woraus dieser Passus wortgleich stammt) ist der Begriff Übermittlung weder in der Verordnung noch im LDSG-neu definiert (früher: „Weitergeben“ oder „einsehen/abrufen“)

Universitätsklinikum Tübingen  
Anstalt des öffentlichen Rechts  
Sitz Tübingen  
Geissweg 3 + 72076 Tübingen  
Tel. 07071 29-0  
www.medizin.uni-tuebingen.de  
Steuer-Nr. 86156/09402  
USt.-ID: DE 146 889 674

Aufsichtsrat  
Ulrich Steinbach (Vorsitzender)

Vorstand  
Prof. Dr. Michael Bamberg (Vorsitzender)  
Gabriele Sonntag (Stellv. Vorsitzende)  
Prof. Dr. Karl Ulrich Bartz-Schmidt  
Prof. Dr. Ingo B. Autenrieth  
Klaus Tischler

Baden-Württembergische Bank Stuttgart  
BLZ 600 501 01 Konto-Nr. 7477 5037 93  
IBAN: DE41 6005 0101 7477 5037 93  
BIC (SWIFT-Code): SOLADEST600

Kreissparkasse Tübingen  
BLZ 641 500 20 Konto-Nr. 14 144  
IBAN: DE79 6415 0020 0000 0141 44  
BIC (SWIFT-Code): SOLADES1TUB

DIE DEUTSCHEN  
UNIVERSITÄTSKLINIKA\*

UNIVERSITÄTSKLINIKUM ULM | Kaufm. Vorstand | 89070 Ulm

Ministerium für Inneres, Digitalisierung und Migration  
Postfach 10 34 65  
70029 Stuttgart

## VORSTAND

Kaufmännischer Direktor  
Dr. Joachim Stumpp  
Albert-Einstein-Allee 29  
D-89081 Ulm

nur per Mail an [Registatur2@im.bwl.de](mailto:Registatur2@im.bwl.de)

**Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechtes  
und sonstiger Vorschriften an die Verordnung (EU) 2016/679  
Az. 2-0557 /8/1, Ihr Schreiben vom 19.12.2017**

30.01.2018  
KD/Bic

Sehr geehrte Damen und Herren,

vielen Dank für die Möglichkeit, zu dem im Betreff genannten Gesetzesentwurf Stellung nehmen zu können. Aus Sicht des Universitätsklinikums Ulm sind in verschiedenen Bereichen Klarstellungen und Anpassungen erforderlich, die nachfolgend dargestellt und im Einzelnen erläutert werden. Unsere Stellungnahme ist unterteilt in (A) „Wissenschaft, Forschung“ und (B) „Sonstige Bereiche, Allgemeines“.

**(A) Wissenschaft, Forschung**

Es ist auch in unseren Augen sinnvoll, wenn die föderative Gesetzgebung nicht zu sehr voneinander abweicht, um über Landesgrenzen hinweg eine sinnvolle und effiziente Zusammenarbeit zu ermöglichen. Allerdings sollte das Ziel gleichzeitig sein, den Wissenschaftsstandort Baden-Württemberg nicht unangemessen einzuschränken (insbesondere im Vergleich mit anderen Bundesländern), ihn vielmehr zu stärken. Entsprechend ist ein Ansatz gefragt, der eine Ausgewogenheit zwischen diesen Zielen gewährleistet.

**1. Regelungen der DS-GVO als Basis**

Es ist nur eine Option des nationalen Gesetzgebers, die Regelungen der DS-GVO zur Forschung durch nationale Regelungen zu konkretisieren und einzuschränken, kein Muss (Art.9 Abs.4 DS-GVO). Soweit von dieser Option nicht Gebrauch

UNIVERSITÄTSKLINIKUM ULM Anstalt des Öffentlichen Rechts, Sitz Ulm | UST-ID. Nr. DE147040060  
Vorsitzender des Aufsichtsrats: Ulrich Steinbach. Vorstand: Prof. Dr. Udo X. Kaisers (Vorsitzender),  
Dr. Joachim Stumpp (Stellv.), Prof. Dr. Peter Möller, Prof. Dr. Thomas Wirth, Silvia Cohnen.  
Sparkasse Ulm IBAN: DE16 6305 0000 0000 1064 78 BIC: SOLADES1ULM



gemacht würde (also keinerlei Regelung zur Wissenschaft im Landesrecht, unmittelbare Geltung der DS-GVO), wäre die Situation folgende:

- Gesundheitsdaten dürften von den Universitätsklinik/Universitäten genutzt werden, wenn die **Verarbeitung zur wissenschaftlichen Forschung erforderlich** ist (Art.9 Abs. 2j i.V.m. Abs.1 DS-GVO verkürzt).
- Dabei gilt die **Weiterverarbeitung/Zweckänderung** von Gesundheitsdaten, die für die Versorgung erhoben wurden, als **vereinbar mit dem ursprünglichen Zweck und rechtmäßig**. Die Zulässigkeit ergibt sich aus der initialen Rechtsgrundlage (Erwägungsgrund 50 DS-GVO verkürzt). Für die Vereinbarkeit gibt es weitere (aus unserer Sicht erfüllbare) Voraussetzungen.
- Die Verarbeitung muss geeigneten **Garantien für die Rechte und Freiheiten des Betroffenen** unterliegen (Art.8g Abs.1 DS-GVO verkürzt). Der Katalog von Garantien umfasst aus unserer Sicht neben den herausgehobenen Pseudonymisierungsansätzen u.a. Alles, was in aktuellen wissenschaftlichen Initiativen mit dem Oberbegriff „**Governance**“ zusammengefasst wird.

Fazit: Mit diesen Regelungen **könnten die Universitätsklinik leben**. Sie sind darauf vorbereitet und sehen das in ihren Konzepten für aktuelle Projekte/Initiativen stets vor. Diese Ansätze ermöglicht die Forschung, die im Interesse der Allgemeinheit heute erhebliche Fortschritte verspricht. Es ist nicht nachvollziehbar, warum einschränkende Regelungen erforderlich sind.

Zu lösen wäre dann noch der Zielkonflikt zwischen dem Grundsatz der Datenminimierung und BigData-Ansätzen; dies ist jedoch durch die nationale Gesetzgebung nicht beeinflussbar.

## 2. Wirkung der nationalen Gesetzgebung gemäß vorliegendem Entwurf

Der vorliegende Entwurf der Regelungen im LDSG-neu stellt (verkürzt dargestellt) folgende zusätzliche Bedingungen auf:

- Die Zwecke der Verarbeitung dürfen **anders nicht oder nur mit unverhältnismäßigem Aufwand** erreichbar sein. Der entsprechende Nachweis müsste stets geführt werden.
- Die Interessen der Universitätsklinik/Medizinischen Fakultäten müssen die Interessen der betroffenen Person am Unterlassen **erheblich überwiegen**.

Begründet werden diese Regelungen mit:

- Im Interesse der Wissenschafts- und Forschungsfreiheit soll die Verarbeitung von Gesundheitsdaten zugelassen werden (sinngemäß).
- Einschränkungen sind soweit vorgesehen, wie es die informationelle Selbstbestimmung gebietet.

Festzustellen ist aus unserer Sicht hierzu:

- a. Ohne die landesrechtlichen Regelungen gemäß vorliegendem Entwurf hätten wir mit den Regelungen der DS-GVO eine geeignete Basis für die heute anstehenden wissenschaftlichen Herausforderungen im Interesse der Allgemeinheit.
- b. Natürlich muss das Recht auf informationelle Selbstbestimmung gewährleistet sein. Dies gebietet das Urteil des Bundesverfassungsgerichtes zur Volkszählung 1983. Danach sind Einschränkungen dieses Rechts nur im überwiegenden Allgemeininteresse möglich.
- c. Der vorliegenden Entwurf (wie im BDSG-neu übrigens, aus dem er offensichtlich übernommen wurde) wiegt aber die Interessen der Uniklinika/Medizinischen Fakultäten gegen die Interessen der betroffenen Person auf. Das Allgemeininteresse bleibt im Gegensatz zu früheren gesetzlichen Formulierungen außen vor.
- d. Der Nachweis der Unmöglichkeit anderer Lösungen bzw. deren zu großer Aufwand sowie das „erhebliche Überwiegen“ als unbestimmter Rechtsbegriff eröffnet einen zu großen Interpretationsspielraum und erzeugen einen unangemessenen Argumentationszwang und -aufwand. Das Bundesverfassungsgericht selbst verwendete nur den Begriff „überwiegendes Allgemeininteresse“.
- e. Beides (c und d) halten wir nicht für sachgerecht, da wir der Überzeugung sind, dass anstehende Forschungsprojekte und -initiativen erhebliche Fortschritte im Interesse der Allgemeinheit erbringen können.
- f. Darüber hinaus meinen wir, dass die DS-GVO die informationelle Selbstbestimmung bereits hinreichend berücksichtigt und zusätzliche Regelungen an sich nicht erforderlich wären.
- g. Der neue hippokratische Eid verpflichtet die Ärzte, medizinisches Wissen zum Wohl der Patienten und zur Förderung der Gesundheitsversorgung mit ihren Kollegen zu teilen. Dem sollten keine unangemessenen Schranken im Wege stehen.

### 3. Vorschlag/Forderung

Soweit möglich, könnten einschränkende nationale Regelungen analog zum Entwurf aus Bayern entfallen.

Sollte dies nicht möglich sein, schlagen wir vor, ausgewogene Interessenlagen durch eine Formulierung wie die z.B. folgende herzustellen:

Öffentliche Stellen dürfen besondere Kategorien personenbezogener Daten für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke verarbeiten, sofern

- a. die Einholung einer Einwilligung der betroffenen Person nicht möglich ist oder mit einem unverhältnismäßigen Aufwand verbunden wäre,
- b. das Interesse der öffentlichen Stelle das Interesse der betroffenen Person an einem Ausschluss der Verarbeitung überwiegt,
- c. die Verarbeitung erhebliche Fortschritte im Allgemeininteresse ermöglicht<sup>1</sup> und
- d. die Verarbeitung geeigneten Garantien für die Rechte und Freiheiten der betroffenen Person gemäß der Verordnung (EU) 2016/679 unterliegt.

Besondere Kategorien personenbezogener Daten sind die in Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 genannten Daten.

Eine solche Formulierung wäre aus Sicht der Universitätsklinik/medizinischen Fakultäten ebenfalls akzeptabel. Sie ermöglicht die Umsetzung der anstehenden Projekte und Initiativen eher als der bisherige Entwurf. Alternativ könnte man sich an Vorlagen aus anderen Bundesländern (siehe unten) orientieren.

#### 4. Vergleich mit anderen Bundesländern

**Bayern:** Der dortige Entwurf stellt keine zusätzlichen Voraussetzungen auf. Statt des Absatzes 1 des LDSG-BaWü neu legt der bayrische Entwurf die Zweckbindung von für wissenschaftliche Zwecke erhobenen Daten fest. Der restliche Regelungsgehalt entspricht sinngemäß dem der Absätze 2 bis 4 des LDSG BaWü neu.

**Fazit:** Im Vergleich zu Bayern klare **Nachteile durch den baden-württembergischen Entwurf.**

**Brandenburg:** „Öffentliche Stellen dürfen personenbezogene Daten einschließlich Daten im Sinne von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ohne Einwilligung für ein bestimmtes Forschungsvorhaben verarbeiten und an andere Stellen oder Personen zu diesem Zweck übermitteln, wenn schutzwürdige Belange der betroffenen Person wegen der Art der Daten, wegen ihrer Offenkundigkeit oder wegen der Art der Verwendung nicht beeinträchtigt werden oder das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange der betroffenen Person überwiegt und der Zweck der Forschung nicht auf andere Weise erreicht werden kann. Die übermittelten Daten dürfen nicht für andere Zwecke verarbeitet werden.“

---

<sup>1</sup> Alternative: „erwarten lässt“

**Fazit:** Kein „erhebliches Überwiegen“; insgesamt wäre diese Formulierung auch sehr gut geeignet. Im Vergleich **klare Nachteile für Baden-Württemberg**.

**Mecklenburg-Vorpommern:** Nahezu wortgleich zu Brandenburg.

**Fazit:** Im Vergleich **klare Nachteile für Baden-Württemberg**.

**Sachsen:** „Die Verarbeitung personenbezogener Daten einschließlich solcher nach Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 zu wissenschaftlichen oder historischen Forschungszwecken ist zulässig, soweit dies für die Durchführung der wissenschaftlichen oder historischen Forschung erforderlich ist, insbesondere der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann, und wenn das öffentliche, insbesondere das wissenschaftliche oder historische Interesse an der Durchführung des Forschungsvorhabens das Interesse der betroffenen Person am Unterbleiben der Verarbeitung überwiegt.“

**Fazit:** Kein „erhebliches Überwiegen“; insgesamt wäre diese Formulierung auch sehr gut geeignet. Im Vergleich **klare Nachteile für Baden-Württemberg**.

## (B) Sonstige Bereiche / Allgemeines

### § 2 Anwendungsbereich

- a. Abs.6 „Unternehmen mit eigener Rechtspersönlichkeit“

Es wäre hilfreich/sinnvoll, hier zu definieren (zumindest in der Begründung), von welchem Unternehmensbegriff hier ausgegangen wird (angelehnt an Handelsrecht, Wettbewerbsrecht, Steuerrecht oder anderer?). Insbesondere, ob die Uniklinika als Anstalten des öffentlichen Rechts als solche gelten sollen.

### § 3 Sicherstellung des Datenschutzes

- a. Es handelt sich in weiten Teilen nicht um Konkretisierungen der DS-GVO-Regelungen sondern um Wiederholungen, aber teilweise dann doch nicht wortgleich und eindeutig formuliert. Das kann zu Verwirrung führen, der Normenklarheit schaden. Hier sollte auf eine redundante Wiederholung der Formulierungen aus der DS-GVO verzichtet werden. Unter Hinweis auf deren Ergänzung sollten die ergänzenden Regelungen des Landes aufgeführt werden.

**§ 5 Datenverarbeitung zu anderen Zwecken**

- a. Abs.1: „soweit die Verarbeitung notwendig und verhältnismäßig ist.“ statt „erforderlich“  
Die Formulierung „notwendig und verhältnismäßig“ in der Verordnung, auf die Bezug genommen wird, bezieht sich in der Verordnung nicht auf eine Verarbeitung sondern auf eine Rechtsvorschrift als Maßnahme zum Schutz von in Artikel 23 genannten Zielen.
- b. § 5 Abs.4: „gespeichert“  
Alter Begriff, nicht definiert. Müsste „verarbeitet“ lauten.

**§ 5 Datenverarbeitung zu anderen Zwecken**

- a. Abs.1: „soweit die Verarbeitung notwendig und verhältnismäßig ist.“ statt „erforderlich“  
Die Formulierung „notwendig und verhältnismäßig“ in der Verordnung, auf die Bezug genommen wird, bezieht sich in der Verordnung nicht auf eine Verarbeitung sondern auf eine Rechtsvorschrift als Maßnahme zum Schutz von in Artikel 23 genannten Zielen.
- b. § 5 Abs.4: „gespeichert“  
Alter Begriff, nicht definiert. Müsste „verarbeitet“ lauten.

**§ 6 Übermittlung personenbezogener Daten**

- a. Begründung: „Nach der Verordnung (EU) 2016/679 wird die Übermittlung personenbezogener Daten wie eine Zweckänderung behandelt.“  
Erforderlich ist eine Klarstellung, auf welchen Artikel oder Erwägungsgrund der Verordnung sich dies bezieht.

**§ 9 Beschränkung des Auskunftsrechts**

- a. Abs.2 : Differenzierung des Auskunftsumfangs  
Sehr gut vor dem Hintergrund der Vielfalt und Komplexität der Datenbestände in Krankenhäusern, speziell Uniklinika. Unbedingt beibehalten.

**§ 12 Verarbeitung personenbezogener Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen**

- a. Abs.2 Nr.2: „die Voraussetzungen des § 5 Absatz 1 Nummern 1 oder 2 vorliegen und die zur Verschwiegenheit verpflichtete Stelle eingewilligt hat“  
Ergänzung zu“ (...) §5 Absatz 1 Nummern 1 oder 2 oder § 13 Abs.1 Satz 1 (...) . Sonst widersprechen sich durch das „nur“ in § 12 Abs.2 Satz 1 die §§ 12 und 13 bzw. fehlt die Klarheit.

**§ 14 Datenverarbeitung bei Dienst- und Arbeitsverhältnissen, Zuverlässigkeitsüberprüfung**

- a. Abs.8: Da es sich hier nicht ausschließlich um Beschäftigte handelt („Besucher“) ist der Absatz fehl am Platz. Der Bezug zu Abs.1 Satz 1 macht auch nicht eindeutig Sinn. Das gehört eher zu Sicherheitsmaßnahmen.

**§ 27 Ordnungswidrigkeiten**

- a. „Gegen öffentliche Stellen im Sinne des § 2 Absatz 1 und 2 dürfen keine Geldbußen verhängt werden, es sei denn, die öffentlichen Stellen nehmen als Unternehmen mit eigener Rechtspersönlichkeit am Wettbewerb teil.“

Der zweite Halbsatz ist obsolet, da für diese Unternehmen gemäß §2 diese Regelungen ohnehin nicht gelten.

**§ 28 Strafvorschrift**

- a. Abs.1 Nr.1a: „speichert, nutzt, verändert, übermittelt oder löscht“  
Begriffe aus dem alten Datenschutzrecht. Müssten durch „verarbeitet“ ersetzt werden. Damit könnte bei künftigen Verpflichtungen hierauf auch gut Bezug genommen werden.
- b. Abs.1 Nr.2: „die Übermittlung (...) erschleicht“  
Im Gegensatz zum alten Datenschutzrecht (woraus dieser Passus wortgleich stammt) ist der Begriff Übermittlung weder in der Verordnung noch im LDSG-neu definiert (früher: „Weitergeben“ oder „einsehen/abrufen“)

Das Universitätsklinikum Ulm bittet um Berücksichtigung der o.g. Aspekte und Hinweise bei der Umsetzung der neuen datenschutzrechtlichen Gesetzesregelungen im Interesse der Allgemeinheit sowie der Standorte in Baden-Württemberg.

Mit freundlichen Grüßen

Professor Dr. Udo X. Kaisers  
Leitender Ärztlicher Direktor

Dr. Joachim Sturmpp  
Kaufmännischer Direktor



VfEW e.V. – Schützenstraße 6 – 70182 Stuttgart

Ministerium für Inneres, Digitalisierung u. Migration BW

Abtl. 2 / Referat Sparkassenwesen  
Willy-Brandt-Str. 41  
70173 Stuttgart

**Ihr Ansprechpartner**  
Torsten Höck  
008-18

Stuttgart, den 25.01.2018

### **Stellungnahme zum Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679**

Sehr geehrter Herr

herzlichen Dank für die Möglichkeit, zum Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679 Stellung zu nehmen.

Der VfEW e.V. vertritt als Verband der Energie- und Wasserwirtschaft über 230 Energie- und Wasserversorger in Baden-Württemberg. Darunter Großunternehmen aber auch kommunale Betriebe sowie kleine, teilweise private Gebietsversorger und Zweckverbände.

Insofern vertreten wir sowohl Unternehmen die in den Anwendungsbereich fallen wie auch solche Unternehmen, die nicht unmittelbar betroffen sind. Gemäß § 2 Abs. 6 LDSG-E ist das Gesetz nicht anwendbar bei Unternehmen die z.B. als Stadtwerke GmbH organisiert und im Wettbewerb (Energieversorgung) tätig sind. Hier ist aber zu beachten, dass es durchaus auch Eigenbetriebe der Gemeinden gibt, welche ebenfalls in der Energieversorgung tätig sind und somit im Wettbewerb. Diese sind nach unserem Verständnis im Anwendungsbereich des LDSG-E. Aus diesem Grund möchten wir darauf hinweisen, dass sowohl bei der Ausgestaltung des Datenschutzrechts wie auch bei der Anwendung sichergestellt werden muss, dass diese Unternehmen im Wettbewerb nicht schlechter gestellt werden, als Unternehmen die eine eigenständige Rechtsform haben.

**Anschrift**  
Verband für Energie- und  
Wasserwirtschaft Baden-  
Württemberg e.V.  
Schützenstraße 6 70182  
Stuttgart

[www.vfew-bw.de](http://www.vfew-bw.de)

beim Bundesverband der  
Energie- und Wasserwirt-  
schaft e.V. – BDEW –

**Amtsgericht Stuttgart**  
VR-Nr.: 72 04 84

**Präsident**  
Klaus Saiger

**Geschäftsführer**  
Torsten Höck

**Bankverbindungen**  
Commerzbank  
IBAN DE24 6004 0071  
0516 6764 00  
BIC COBADEFFXXX



Wir danken Ihnen für die frühzeitige Einbindung sowie die Möglichkeit zur  
Stellungnahme und bitten um die Berücksichtigung unserer Hinweise.

Mit freundlichen Grüßen

Torsten Höck  
Geschäftsführer



VKU • Geschäftsstelle Baden-Württemberg • Königstraße 4 • 70173 Stuttgart

Ministerium für Inneres, Digitalisierung und  
Migration Baden-Württemberg  
Postfach 10 34 65  
70029 Stuttgart

**Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und  
sonstiger Vorschriften an die Verordnung (EU) 2016/679**

Aktenzeichen: 2-0557.8/1

Sehr geehrte Damen und Herren,

für die Möglichkeit, zu o.g. Gesetzgebungsverfahren eine Stellungnahme abgeben zu können, bedanken wir uns sehr herzlich. In Baden-Württemberg sind 199 kommunale Unternehmen im Verband kommunaler Unternehmen (VKU) organisiert. Die VKU-Mitgliedsunternehmen in Baden-Württemberg leisten jährlich Investitionen in Höhe von 1,070 Milliarden Euro, erwirtschaften einen Umsatz von über 12 Milliarden Euro und sind wichtiger Arbeitgeber für rund 25.000 Beschäftigte.

Da der in § 2 Abs. 2 beschriebene Anwendungsbereich auch kommunale Unternehmen umfasst, haben wir den Gesetzentwurf auf die Auswirkungen für unsere Mitgliedsunternehmen geprüft. Im Wesentlichen stimmen wir den beabsichtigten Regelungen des Gesetzentwurfes zu, wollen aber nachfolgend einige Anregungen machen.

**Ad §3: Sicherstellung des Datenschutzes**

Die Aufzählung wird womöglich nicht alle Konstellationen erfassen. In der Begründung wird ausgeführt, dass die Aufzählung nicht abschließend ist, weshalb im Streitfall es denkbar wäre, dass eine von § 3 nicht erfasste Maßnahme trotzdem über die Begründung als vorzusehen gilt. Um diese Zweifel von Anfang an zu unterbinden, wäre es eventuell hilfreich, wenn sich die Ansicht aus der Begründung schon im Gesetzestext wiederfindet. Das wäre etwa möglich, indem es bei § 3 S. 2 heißen könnte: „Dabei sind insbesondere der Stand der Technik,...“



Dr. Tobias Bringmann  
Geschäftsführer  
Landesgruppe  
Baden-Württemberg

Königstraße 4  
70173 Stuttgart

**Hauptgeschäftsstelle**

Invalidenstraße 91  
10115 Berlin

Fon +49 30 58580-0  
Fax +49 30 58580-100

www.vku.de  
info@vku.de

30.01.2018

Hauptgeschäftsführerin:  
Katherina Reiche

Registriergericht:  
Amtsgericht Charlottenburg  
Registernummer:  
VR 27941 B

Bankverbindung:  
Berliner Sparkasse  
IBAN: DE95100500006600009100  
SWIFT: BELA2B33XXX  
Ust.-IdNr.: DE 123065069



**Ad §14 Abs. 8: Datenverarbeitung bei Dienst- und Arbeitsverhältnissen, Zuverlässigkeitsüberprüfung**

Bei der datenschutzrechtlichen Absicherung von Zuverlässigkeitsüberprüfungen durch öffentliche Stellen sollte zumindest in der Begründung explizit geregelt sein, dass dies auch auf Mitarbeiter kritischer Infrastrukturen anwendbar ist. Kritische Infrastrukturen haben ein erhöhtes Schutzbedürfnis, weshalb solche Zuverlässigkeitsüberprüfungen in jedem Falle zulässig sein sollten.

**Ad §17: Videoüberwachung öffentlich zugänglicher Räume**

In der Begründung sollte deutlich gemacht werden, dass auch öffentliche Parkhäuser von der Regelung erfasst sind.

**Ad §28: Strafvorschrift**

Die Präzisierung zur Strafvorschrift in § 28 Abs. 1 S.1 („...die nicht allgemein ofenkundig sind...“) ist aus unserer Sicht zu auslegungsbedürftig formuliert. § 42 Abs. 2 BDSG-neu spricht in diesem Zusammenhang von „nicht allgemein zugänglich“. Es wäre sinnvoll, diese klarere Formulierung des BDSG-neu auch im vorliegenden Gesetz zu verwenden.

Weitere Anmerkungen haben wir nicht. Wir möchten Sie aber höflichst um die Berücksichtigung der von uns aufgeführten Punkte bitten und wären über eine Rückmeldung hierzu sehr dankbar. Gerne bieten wir Ihnen an, die Thematik in einem Fachgespräch zu erörtern.

Mit freundlichen Grüßen

A handwritten signature in blue ink, appearing to be 'T. Bringmann', written over a horizontal line.

Dr. Tobias Bringmann  
Geschäftsführer  
Landesgruppe Baden-Württemberg

Innenministerium  
Baden-Württemberg

01. Feb. 2018

Az.: *70102*

**Von:** Recht <Recht@vwda.de>  
**Gesendet:** Mittwoch, 31. Januar 2018 11:08  
**An:** Registratur 2 (IM)  
**Betreff:** Stellungnahme zum Entwurf eines Gesetzes zur Anpassung des  
allgemeinen Datenschutzrechts und sonstiger Vorschriften an die VO (EU)  
2016/679

Sehr geehrte Damen und Herren,

im Rahmen der Anhörung möchten wir auf Artikel 1 Landesdatenschutzgesetz (LDSG) § 8 Beschränkung der Informationspflicht (Ergänzung zu Artikel 13 und 14 der Verordnung (EU) 2016/679) hinweisen. In Absatz 1 ist eine Abwägung der Interessen der öffentlichen Stelle an der Nichterteilung der Information und die Interessen der betroffenen Person vorgesehen. Fraglich ist, ob eine derartige - allgemein gehaltene - Abwägung die Vorschrift nicht zu weit öffnet.

Mit freundlichen Grüßen

Stephanie Riedl  
Geschäftsführerin  
Mitgliederverwaltung + Recht

Versorgungswerk der Architektenkammer  
Baden-Württemberg, K.d.ö.R.  
Danneckerstr. 52  
70182 Stuttgart

[recht@vwda.de](mailto:recht@vwda.de)  
[www.vwda.de](http://www.vwda.de)



2-0557.8/1/156



**Versorgungswerk**  
der Rechtsanwälte in Baden-Württemberg  
- Körperschaft des öffentlichen Rechts -

An das  
Ministerium für Inneres,  
Digitalisierung und Migration Baden-Württemberg

Ausschließlich per E-Mail  
An: [Registatur2@im.bwl.de](mailto:Registatur2@im.bwl.de)

Stuttgart, 31. Januar 2018

AZ: 2-0557.8/1 (Verbändeanhörung LDSG-Entwurf)

Entwurf (Stand: 14.12.2017) eines Gesetzes zur Anpassung des allgemeinen Daten-  
schutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679

**Hier: Stellungnahme des Versorgungswerkes der RAe in Baden-Württemberg**

Sehr geehrte Damen und Herren,

als berufsständisches Versorgungswerk in der Rechtsform einer Anstalt öffentlichen  
Rechts mit über 18.700 Mitgliedern (überwiegend Rechtsanwältinnen und Rechtsan-  
wälte) nehmen wir Stellung zu Ihrem Gesetzesentwurf. Unsere Stellungnahme kon-  
zentriert sich auf die für das Versorgungswerk wesentliche Neufassung des Landes-  
datenschutzgesetzes (Art. 1 Ihres Entwurfs, nachfolgend LDSG-E).

1. Behördliche Datenschutzbeauftragte für öffentliche Stellen

Für das Versorgungswerk ist es nachvollziehbar und folgerichtig, dass der LDSG-E  
die Vorschrift des heutigen § 10 LDSG 2000 ersatzlos streicht. Schließlich ergibt sich  
die gesetzliche Verpflichtung jeder öffentlichen Stelle, ab Geltung der Datenschutz-

1



## Versorgungswerk der Rechtsanwälte in Baden-Württemberg

– Körperschaft des öffentlichen Rechts –

Grundverordnung einen behördlichen Datenschutzbeauftragten zu benennen, unmittelbar aus Art 37 Abs. 1 DS-GVO. In diesem Sinne wird der Hinweis im Vorblatt des Gesetzentwurfs (Abschnitt D, 1. Absatz) auf die gesetzliche Verpflichtung jeder öffentlichen Stelle verstanden. Angesichts der detaillierten und abschließenden Regelung in Art. 37 DS-GVO zur Benennung von Datenschutzbeauftragten besteht für eine konkretisierende oder ergänzende Regelung im LDSG-E weder Bedarf noch ein Spielraum.

Sehr zu begrüßen ist die Ankündigung des Landesbeauftragten für Datenschutz und Informationsfreiheit auf seiner Website, ab März 2018 eine Möglichkeit zur Onlinemeldung der Kontaktdaten des (oder der) jeweils benannten behördlichen Datenschutzbeauftragten bereitzustellen. Diese Möglichkeit der Onlinemeldung sollte den mit der Meldepflicht (Art. 37 Abs. 7 DS-GVO) verbundenen bürokratischen Aufwand auf ein Minimum reduzieren.

### 2. Zu § 4 LDSG-E (Zulässigkeit der Datenverarbeitung)

Die Ausgestaltung von § 4 LDSG-E als subsidiärer Rechtsgrundlage für die Datenverarbeitung ist sprachlich eng angelehnt an § 3 des neuen BDSG. Dieser Gleichlauf der Normen auf Bundes- und Landesebene ist zu begrüßen, weil er die praktische Rechtsanwendung ganz erheblich vereinfachen wird. Wie die meisten anderen öffentlichen Stellen auch verarbeitet das Versorgungswerk personenbezogene Daten nur in dem Umfang, der für die Erfüllung seiner öffentlichen Aufgabe erforderlich ist; eine weitergehende Datenverarbeitung oder gar der Datenverkauf an Dritte sind beim Versorgungswerk ausgeschlossen. Für diese Fälle genügt § 4 LDSG-E in seiner allgemeinen Fassung als Erlaubnistatbestand (auf der Basis von Art. 6 Abs. 1 e), Abs. 3 DS-GVO).



**Versorgungswerk**  
der Rechtsanwälte in Baden-Württemberg  
– Körperschaft des öffentlichen Rechts –

### 3. Zu § 27 LDSG-E (Ordnungswidrigkeiten)

Die Ergänzung von Art. 83 Abs. 7 DS-GVO durch § 27 LDSG-E ist im Grundsatz zu begrüßen, denn der Ausschluss von Geldbußen gegen öffentliche Stellen scheint sachgerecht. Allerdings sollte im weiteren Gesetzgebungsverfahren kritisch hinterfragt werden, ob die in § 27 LDSG-E formulierte Einschränkung der Bußgeldfreiheit wirklich notwendig und sinnvoll ist. § 43 Abs. 3 BDSG neu kennt diese Einschränkung nicht, sondern schließt Bußgelder gegen öffentliche Stellen uneingeschränkt aus. Inhaltlich unterschiedliche Detailregelungen auf Bundes- und Landesebene erschweren in der Praxis die Rechtsanwendung und laufen außerdem dem Ziel der DS-GVO zuwider, Datenschutzregelungen europaweit zu vereinheitlichen einschließlich der Sanktionen für Datenschutzverletzungen (DS-GVO Erwägungsgründe 11, 13 ua.).

Das Versorgungswerk ist von der kritisierten Einschränkung der Bußgeldbefreiung (§ 27 LDSG-E letzter Halbsatz) nicht selbst betroffen, weil es nicht wettbewerblich tätig ist. Dennoch ist Kritik angezeigt an der vorgeschlagenen Regelung in § 27 LDSG-E sowie an ihrer Begründung. Die Begründung erweckt den Eindruck, die Einschränkung der Bußgeldbefreiung sei notwendig, um öffentliche Stellen im Land mit dem Druck von Bußgeldern zu rechtskonformer Datenverarbeitung anzuhalten. Diese Sichtweise unterstellt staatlichem Handeln (im unternehmerischen Wettbewerb) mangelnde Rechtstreue. Das ist zu pessimistisch: Weder die Tätigkeitsberichte des Landesbeauftragten für den Datenschutz noch veröffentlichte Entscheidungen legen nahe, dass es dieses Bußgeld-Druckmittels in Baden-Württemberg dringender bedürfte als auf Bundesebene. Im Interesse der möglichen Rechtsvereinheitlichung im Datenschutzrecht innerhalb des durch die DS-GVO gespannten Rahmens ist deshalb der letzte Halbsatz aus § 27 LDSG-E zu streichen.



**Versorgungswerk**  
der Rechtsanwälte in Baden-Württemberg  
– Körperschaft des öffentlichen Rechts –

Gerne stehen wir für evtl. Rückfragen und Erläuterungen zu dieser Stellungnahme zur Verfügung. Wir bitten darum, regelmäßig über den weiteren Verlauf des Gesetzgebungsverfahrens informiert zu werden.

Mit freundlichen Grüßen

- **Versorgungswerk der Rechtsanwälte** -

Rechtsanwalt Hartmut Kilger  
stv. Vorstandsvorsitzender

## Versorgungswerk der Steuerberater in Baden-Württemberg



Körperschaft des öffentlichen Rechts

Sophienstraße 13  
70178 Stuttgart

Telefon: 07 11 / 2 22 49 69-0

Telefax: 07 11 / 2 22 49 69-8

E-Mail: [service@stbvw-bw.de](mailto:service@stbvw-bw.de)

Internet: [www.stbvw-bw.de](http://www.stbvw-bw.de)

Ministerium für Inneres, Digitalisierung u. Migration  
Baden-Württemberg  
Postfach 10 34 65  
70029 Stuttgart

Stuttgart, den 01.02.2018

Per E-Mail an: [poststelle@im.bwl.de](mailto:poststelle@im.bwl.de)

### **Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679**

Sehr geehrte Damen und Herren,

wir schließen uns der Stellungnahme des Versorgungswerks der Rechtsanwälte vom 31.01.2018 zu o.g. Entwurf vollumfänglich an.

Wir bitten darum, über den weiteren Verlauf des Gesetzgebungsverfahrens regelmäßig informiert zu werden.

Mit freundlichen Grüßen

Michael Erhardt, StB  
Vorsitzender des Vorstands

Vorstandsvorsitzender  
**Michael Erhardt**  
Steuerberater

Geschäftsführerin  
**Bärbel Manck**  
Dipl.Verwalt.Wirtin(FH), Dipl.Wirt.Ing.(FH)

BW Bank Stuttgart  
Konto 787 150 6592 IBAN DE22 6005 0101 7871 5065 92  
BLZ 600 501 01 BIC SOLA DE ST



Zentrum für Kunst  
und Medien Karlsruhe

Center for Art and Media

Stiftung des öffentlichen Rechts Foundation under public law

z k m Lorenzstraße 19 76135 Karlsruhe

Ministerium für Inneres, Digitalisierung und  
Migration Baden-Württemberg  
Postfach 103465

70029 Stuttgart

Postanschrift Postal address  
Postfach 6909 P.O. Box 6909  
D-76049 Karlsruhe

Besuchsadresse Location  
Lorenzstraße 19  
76135 Karlsruhe

30. Januar 2018

-Ihr Aktenzeichen: 2-0557.8/1-

### Entwurf eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die DSGVO; Stellungnahme ZKM

Sehr geehrte Frau , sehr geehrter Herr 

haben Sie zunächst vielen Dank für die Übersendung des Entwurfs eines Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung – kurz: DSGVO). Gerne beteiligen wir uns an der Anhörung der Verbände mit der vorliegenden Stellungnahme.

Das Zentrum für Kunst und Medien (ZKM) ist als Stiftung des öffentlichen Rechts eine öffentliche Stelle des Landes Baden-Württemberg. Als solche wird das ZKM vom neuen Landesdatenschutzgesetz (LDSG-Entwurf) betroffen sein, welches durch das nun im Entwurf vorliegende Anpassungsgesetz eingeführt werden soll.

Wir begrüßen ausdrücklich, dass das bisherige Medienprivileg entsprechend dem Regelungsauftrag in Art. 85 DSGVO durch § 18 LDSG-Entwurf auf sämtliche Verarbeitungen personenbezogener Daten zu künstlerischen und literarischen Zwecken ausgeweitet werden soll. Allerdings ergeben sich aus dem vorgeschlagenen Wortlaut aus unserer Sicht an wenigen Stellen Unklarheiten, welche wir abschließend auch nicht unter Heranziehung der Begründung des Entwurfes klären konnten, und zu denen wir daher wie folgt Stellung nehmen möchten:

#### 1. Reichweite des Verweises in § 18 Abs. 1 S. 1 LDSG-Entwurf auf Art. 24 DSGVO

In § 18 Abs. 1 S. 1 LDSG-Entwurf wird unter anderem auf die Geltung von Art. 24 DSGVO verwiesen. Art. 24 DSGVO regelt die Verantwortung des für die Verarbeitung Verantwortlichen. Dieser muss gemäß Art. 24 Abs. 1 S. 1 DSGVO sicherstellen, dass die Verarbeitung gemäß dieser Verordnung erfolgt.

Dies wirft unseres Erachtens die Frage auf, ob nicht im Rahmen der Auslegung weitere Pflichten aus der DSGVO auch auf die Verarbeitung zu künstlerischen Zwecken übertragen werden könnten, unter anderem das Verbot mit Erlaubnisvorbehalt (Art. 5 Abs. 1 lit. a, Art. 6 DSGVO). Dies könnte die



Ausweitung des Medienprivilegs konterkarieren, denn demgemäß sollen diese besonderen datenschutzrechtlichen Anforderungen gerade nicht gelten, sondern nur die medienrechtlichen Fachgesetze oder Grundsätze. Es soll also – in Ermangelung entsprechender Fachgesetze – eine offenere Abwägung zwischen den betroffenen Rechtspositionen (wie dem allgemeinen Persönlichkeitsrecht und der Kunstfreiheit) stattfinden.

Nicht bestritten werden soll, dass auch den Verantwortlichen einer künstlerischen Datenverarbeitung gewisse Pflichten zum Schutz personenbezogener Daten gegen Missbrauch treffen, wie insbesondere die ebenfalls aufgeführten Regelungen zum Datengeheimnis und der Datensicherheit. Dabei wird allerdings die nicht einfache Frage aufgeworfen, welche technischen und organisatorischen Sicherheitsmaßnahmen gerade im künstlerischen Bereich angemessen sind, wozu in der Begründung gegebenenfalls noch Stellung genommen werden könnte.

Der Verweis auf Art. 24 DSGVO erscheint in seiner Reichweite aber jedenfalls unklar. Möglicherweise könnten insoweit im Wortlaut oder zumindest in der Begründung eine Klarstellung dahingehend aufgenommen werden, dass jedenfalls das datenschutzrechtliche Verbot mit Erlaubnisvorbehalt nicht gilt.

## 2. Rechte der betroffenen Personen

§ 18 Abs. 1 S. 3 LDSG-Entwurf verweist in Bezug auf die Rechte der betroffenen Personen lediglich auf Abs. 2 dieser Vorschrift (klassische medienrechtliche Maßnahmen wie Gegendarstellung usw.). Die Begründung des Entwurfes argumentiert insoweit (zu Abs. 2 der Vorschrift), dass das Recht auf freie Meinungsäußerung leerlaufen würde, wenn Berichtigungs- und Löschanträge vollumfänglich zur Geltung gelangten. Dies wirft allerdings die Frage auf, ob die Regelung auch datenschutzrechtliche Ansprüche auf bloße Auskunft ausgeschlossen werden sollen, was bestenfalls noch geklärt werden könnte.

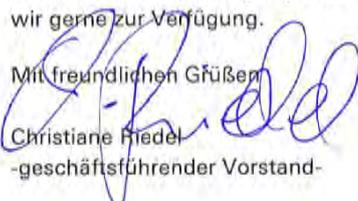
## 3. Bußgeldverantwortung im künstlerischen Bereich

Auch ist uns aufgefallen, dass der Südwestrundfunk in § 18a LDSG-Entwurf noch ein Stück weitergehend als der künstlerische Bereich insoweit privilegiert wird, als dass dort nicht nur die Schadensersatzpflicht nach Art. 82 DSGVO, sondern auch die Bußgeldverantwortung nach Art. 83 DSGVO auf das Datengeheimnis und die Datensicherheit beschränkt wird.

Zwar gelten unseres Erachtens der Sache nach für künstlerische Zwecke im Wesentlichen ohnehin nur das Datengeheimnis und die Datensicherheit, so dass insoweit auch die Bußgeldverantwortung entsprechend implizit beschränkt sein dürfte. Allerdings könnte man diesbezüglich noch eine Klarstellung in Wortlaut oder Begründung aufnehmen, da über den Verweis auf Kapitel VIII DSGVO grundsätzlich auch Art. 82 und 83 DSGVO für diesen Bereich gelten.

Über eine Berücksichtigung unserer Stellungnahmen würden wir uns freuen. Für Rückfragen stehen wir gerne zur Verfügung.

Mit freundlichen Grüßen

  
Christiane Fiedel  
-geschäftsführender Vorstand-