Universität Bremen

✉ Universität Bremen · **Fachbereich 06** · Postfach 33 04 40 · 28334 Bremen

An die
Vorsitzende des Ausschusses für Inneres
und Sport
Frau Petra Berg

Franz-Josef-Röder-Straße 7

66119 Saarbrücken

Fachbereich 06
Rechtswissenschaft

Dr. Dennis-Kenji Kipker

Universitätsallee
GW 1, Raum 2010
28359 Bremen

Telefon (0421) 218 – 66049
Fax (0421) 218 – 66052
eMail kipker@uni-bremen.de

Ihr Zeichen:	Ihre Nachricht vom:	Unser Zeichen:	Datum: 29.04.20

Dr. Dennis-Kenji Kipker

Stellungnahme zur Anhörung des Ausschusses für Inneres und Sport des Landtags des Saarlandes am 7. Mai 2020 zum Entwurf eines Gesetzes zur Neuregelung der polizeilichen Datenverarbeitung im Saarland (Drucksache 16/1180)

A. Hintergründe und Systematik

Der vorliegende Gesetzentwurf befasst sich mit dringend notwendigen Änderungen an den Vorschriften zur polizeilichen Datenverarbeitung im Saarland, die auf den Entwicklungen des europäischen Rechts und der aktuellen verfassungsrechtlichen Entwicklung basieren. Zu nennen sind dabei zuvorderst die EU JI-Richtlinie, die in das nationalstaatliche Recht umzusetzen ist, die Vereinbarungen aus dem Koalitionsvertrag, die BVerfG-Entscheidung zum BKA-Gesetz vom 20. April 2016 (1BvR 966/09, 1 BvR 1140/09), erkannte Defizite im Hinblick auf polizeiliche Befugnisse, sowie Forderungen aus der polizeilichen Praxis und des Unabhängigen Datenschutzzentrums UDZ im Saarland. In den Gesetzentwurf einfließen soll ebenfalls die Umsetzung des Programms „Polizei 2020“.

Die polizeiliche Datenverarbeitung als eine Ausprägung staatlicher Datenverarbeitung befindet sich seit jeher an der Schnittstelle zweier, teils kollidierender Interessen: der informationellen Freiheit und der staatlichen Sicherheit. Ziel einer europa- und insbesondere verfassungskonformen Neuregelung der polizeilichen Datenverarbeitung muss es deshalb sein, den Widerstreit dieser Interessen, soweit vorhanden, zueinander in einen angemessenen Ausgleich zu bringen. Das ist in der Vergangenheit nicht immer der Fall gewesen. Verwiesen sei in diesem Zusammenhang beispielsweise auf die ebenfalls von mir getätigte Stellungnahme zur Anhörung des Ausschusses für Inneres und Sport am 21. April 2016 zum Gesetzentwurf zur Änderung des Saarländischen Polizeigesetzes vom 10. März 2016, Drs. 15/1734, die die Aufnahme einer Rechtsgrundlage für den polizeilichen Body-Cam-Einsatz zum Gegenstand hatte.

Grundsätzlich ist es jedoch zu begrüßen, dass nunmehr eine eigenständige Rechtsgrundlage zur polizeilichen Datenverarbeitung im Saarland geschaffen wird, und vor diesem Hintergrund und den teils sehr speziellen Befugnissituationen, die sich daraus ergeben, im Wesentlichen davon abgesehen wird, allgemeine

datenschutzrechtliche Vorschriften als Auffangtatbestand zu verwenden. Insoweit ist der hier gewählte Ansatz einer Vollregelung durchaus sinnvoll und kann im Zweifelsfall auch zu einer Akzeptanzsteigerung des informationellen polizeilichen Handelns gegenüber dem Bürger beitragen. In systematischer Hinsicht sieht der Gesetzentwurf vor, dass durch Artikel 1 in erster Linie die Befugnisse zur polizeilichen Datenverarbeitung, die bisher in den §§ 26-40 des Saarländischen Polizeigesetzes verortet waren, nunmehr gestrichen werden. Artikel 2 sieht das Saarländische Gesetz über die Verarbeitung personenbezogener Daten durch die Polizei (SPolDVG) als Neuregelung vor. Der Entwurf enthält detaillierte Vorgaben unter anderem zur Datenschutzkontrolle, zu den Rechten der betroffenen Person, zu den Rechtsgrundlagen der Verarbeitung personenbezogener Daten, zu besonderen polizeilichen Datenverarbeitungsbefugnissen, zur Datenübermittlung, zur Auftragsdatenverarbeitung und zur sicheren Datenhaltung. Artikel 3 hebt die durch Artikel 2 obsolet gewordene Verordnung über die Zulassung der Übermittlung personenbezogener Daten von der Polizei an ausländische Polizeibehörden auf. Artikel 4 dient der Umsetzung des Zitiergebots im Hinblick auf die mit dem Gesetz verbundenen Grundrechtseingriffe. Artikel 5 enthält Übergangsregelungen, Artikel 6 des Gesetzes regelt dessen Inkrafttreten.

Die vorliegende Stellungnahme beschränkt sich in ihrem Kern auf den Artikel 2 des Gesetzentwurfs, da hier die meisten für eine juristische Beurteilung relevanten Änderungen zu verorten sind.

B. Zu den Regelungen im Einzelnen

I. Artikel 2: Saarländisches Gesetz über die Verarbeitung personenbezogener Daten durch die Polizei (SPolDVG)

1. § 1 Abs. 1

In formaler Hinsicht fehlt hier in der Aufzählung der Verarbeitungszwecke ein Komma zwischen den Worten „Ermittlung“ und „Verfolgung“.

2. § 10 Abs. 2

Die Betroffenenrechte sind zentrale Elemente zur effektiven Wahrnehmung der informationellen Selbstbestimmung. Dies muss gerade für die Datenverarbeitung durch staatliche Stellen gelten, denn auf diese hat die betroffene Person – im Gegensatz zur regelmäßig praktizierten datenschutzrechtlichen Einwilligung in der Privatwirtschaft – kaum oder regelmäßig keinen unmittelbaren Einfluss. Ausgangspunkt für alle nachfolgenden Betroffenenrechte wie z.B. Korrektur oder Löschung ist die Benachrichtigung der betroffenen Person, denn muss sie hierfür erst Kenntnis von den Datenverarbeitungsvorgängen erlangen. Ausweislich der Entwurfsbegründung setzt Art. 10 den Art. 13 Abs. 2 der JI-Richtlinie um und orientiert sich im Wesentlichen an § 56 BDSG 2018. Trotz der Tatsache, dass der Entwurf an dieser Stelle eine bundesrechtliche Regelung quasi spiegelbildlich wiedergibt, sollte erwogen werden, einen anderen Ansatz zu wählen. Nicht selten ist es gerade so, dass spezialgesetzliche Rechtsvorschriften, die eine Benachrichtigungspflicht statuieren, selbst schon Ausnahmetatbestände hiervon enthalten. Um einer übermäßigen Einschränkung der grundlegenden Benachrichtigungspflicht entgegenzuwirken, sollte deshalb erwogen werden, Abs. 2 zu streichen – oder zumindest aber eine Einschränkung dahingehend vorzusehen,

dass die Regelung aus Abs. 2 nur dann Anwendung findet, soweit nicht schon eine spezialgesetzliche Regelung die Benachrichtigung und deren Ausschluss regelt.

3. § 10 Abs. 3 und Abs. 4

Auch § 10 Abs. 3 entspricht gedanklich der Regelung des § 56 Abs. 3 BDSG 2018. Die Formulierung in der Entwurfsbegründung, dass dabei die Datenverarbeitung der Nachrichtendienste „mittelbar privilegiert“ werden soll, ist nicht nachvollziehbar. Zwar besteht ein Interesse der Nachrichtendienste an Geheimhaltung, genauso in einem bestimmten Maß aber auch ein Informationsinteresse des Bürgers, wenn in seine informationellen Grundrechte für ihn unbemerkt von staatlicher Seite eingegriffen wird. Deshalb sollte auch hier überlegt werden, die Auffangregelung des § 10 Abs. 4, die gegenwärtig nur für die allgemeinen Fälle des Abs. 2 gilt, dem Gedanken nach ebenfalls auf Abs. 3 zu beziehen. Dies ist freilich nicht 1:1 möglich, da hier verschiedene Behörden, Regulierungsebenen, Verfahren und Zuständigkeiten involviert sind. Zumindest aber sollte angedacht werden, die Dokumentationsregelung aus § 11 Abs. 8 des Gesetzentwurfs auch auf die Fälle des § 10 Abs. 3 zu beziehen, da die Polizeibehörde für die Übermittlung der personenbezogenen Daten an weitere Stellen verantwortlich ist.

4. § 10 Abs. 6

§ 10 Abs. 6 legt die Fälle fest, in denen eine Benachrichtigung generell unterbleiben muss. Unter anderem ist dies dann der Fall, wenn schutzwürdige Belange anderer Personen entgegenstehen (Nr. 3). Weder im Wortlaut der Vorschrift noch in der Entwurfsbegründung findet sich ein klarer Hinweis darauf, was im Einzelnen unter den schutzwürdigen Belangen zu verstehen ist. Unabhängig von der Konkretisierung des Begriffs durch die Rechtsprechung sollte im Sinne der Normenklarheit zumindest in die Entwurfsbegründung eine zusätzliche Erläuterung aufgenommen werden.

5. § 11 Abs. 3

Auch für das Auskunftsrecht der betroffenen Person findet eine Übernahme der Regelungen des BDSG 2018, hier § 57, statt. Das Auskunftsrecht kann demnach beschränkt werden, wenn die betroffene Person keine Angaben macht, die das Auffinden der Daten ermöglichen, und deshalb der für die Erteilung der Auskunft erforderliche Aufwand außer Verhältnis zu dem von der betroffenen Person geltend gemachten Informationsinteresse steht. Im Generellen stellt sich (auch für die bundesrechtliche Regelung) im Zeitalter von digitaler und vernetzter Datenverarbeitung die Frage, in wie vielen Fällen eine solche Ausnahmeregelung des unverhältnismäßigen Aufwands zur Informationsbeschaffung durch die verantwortliche Stelle noch einschlägig bzw. zeitgemäß ist, da auch das Auskunftsrecht der betroffenen Person eine zentrale Regelung zur effektiven Wahrnehmung informationeller Selbstbestimmung darstellt.

6. § 11 Abs. 4

Hier wird auf die Ausführungen zu § 10 Abs. 6 verwiesen.

7. § 11 Abs. 6

§ 11 Abs. 6 regelt die grundsätzliche schriftliche Unterrichtungspflicht für den Fall einer Auskunftsverweigerung oder Auskunftseinschränkung. Auch hier orientiert sich der Entwurf erneut am BDSG 2018. Von der Unterrichtung kann in den Fällen des § 10 Abs. 2, 5 oder 6 abgesehen werden. Ergänzt werden sollte hier eine zusätzliche Überprüfungsregelung, nach der die Polizeibehörde beispielsweise nach Ablauf eines Zeitraums von zwölf Monaten feststellt, ob weiterhin Gründe vorliegen, die gegen eine Unterrichtung der betroffenen Person sprechen. Die sachlichen bzw. rechtlichen Gründe für eine entsprechende Entscheidung sind zu dokumentieren, vgl. auch § 11 Abs. 8.

8. § 12 Abs. 1

§ 12 regelt die Rechte auf Berichtigung und Löschung sowie Einschränkung der Verarbeitung personenbezogener Daten. Gem. Abs. 1 S. 5 kann die betroffene Person außerdem verlangen, dass unvollständige personenbezogene Daten ergänzt werden, soweit dies unter Berücksichtigung der Verarbeitungszwecke angemessen ist. Um für Einzelfälle eine übermäßige Ergänzung zu vermeiden, sollte der Vorschrift ein Halbsatz bzw. Satz hinzugefügt werden, dass hierbei auch der Grundsatz der Datensparsamkeit zu berücksichtigen ist.

9. § 12 Abs. 4

Hier wird auf die Ausführungen zu § 11 Abs. 6 verwiesen.

10. § 15 Abs. 3

Richtigerweise kann die Polizei, soweit offenkundig unbegründete oder exzessive Anträge betroffener Personen vorliegen, eine angemessene Bearbeitungsgebühr festsetzen oder die Bearbeitung des Antrags verweigern. Der derzeitige S. 3 sieht in diesem Zusammenhang vor, dass die Polizei den offenkundig unbegründeten oder exzessiven Charakter des Antrags „belegen können“ muss. Art. 12 Abs. 4 der JI-Richtlinie spricht hier davon, dass der Verantwortliche den „Nachweis“ für den rechtsmissbräuchlichen Charakter des Antrags „zu erbringen“ hat. Trotz des auch hier wieder gegebenen inhaltlichen Gleichlaufs mit der bundesrechtlichen Vorschrift des § 59 BDSG 2018 ist anzuregen, auch für diese Fälle zumindest in aller gebotenen Kürze im Sinne der Informationsfreiheit zu begründen, worin die Rechtsmissbräuchlichkeit zu sehen ist. Eine solche Ergänzung würde ebenfalls dem vorgenannten, anderen Wortlaut der JI-Richtlinie entgegenkommen.

11. § 17 Abs. 2

Art. 6 der JI-Richtlinie schreibt sinnvollerweise vor, dass bei der Datenverarbeitung zwischen unterschiedlichen Kategorien betroffener Personen zu unterscheiden ist. § 17 Abs. 2 regelt die vollzugspolizeiliche Datenverarbeitung. Wie bereits in verschiedenen weiteren Anhörungen angemerkt wurde, stößt hier die Regelung gem. Nr. 2 lit. a Alt. 1 auf Bedenken. So können nahezu sämtliche der gesetzlich geregelten, polizeilichen Operationen zur Datenverarbeitung inkl. verdeckter Maßnahmen gegen solche Personen gerichtet werden, bei denen Tatsachen die Annahme rechtfertigen, dass sie von der Planung oder der Vorbereitung der Straftaten oder der Verwertung der Tatvorteile Kenntnis haben, und die nicht nur im zufälligen Kontakt zur betroffenen Person stehen. Gesetzlich vorausgesetzt wird aber gerade nicht, dass sie zu der Tat in einem irgendwie gearteten engeren Zusammenhang stehen, der über eine bloße potenzielle Kenntnis von Vorgängen hinausgeht (vgl. Alt. 2). Auch diese Personen dem vollen polizeilichen Eingriffsinstrumentarium zur Informationsverarbeitung auszusetzen, erscheint unverhältnismäßig. Eine Streichung ist jedoch ebenfalls nicht interessengerecht. Vielmehr ist vorzuschlagen, diese Personengruppe rechtlich gesondert zu behandeln bzw. aufzuführen. Im Besonderen stellt sich dieselbe Frage überdies für an sich unbeteiligte Personen, wie Zeuginnen und Zeugen, Hinweisgeberinnen oder Hinweisgeber, und sonstige Auskunftspersonen, wie sie in Art. 17 Abs. 1 Nr. 4 und Art. 17 Abs. 2 Nr. 4 genannt werden.

12. § 19

§ 19 ist als Regelung vollständig und ersatzlos zu streichen. Bereits aus der Entwurfsbegründung wird deutlich, dass die Möglichkeit, eine polizeiliche Datenverarbeitung mittels Einwilligung herbeizuführen, äußerst restriktiv zu bewerten und allerhöchstens als mitgliedstaatliche Option vorzusehen ist, die aber für den Regelfall nicht ausgeübt werden sollte und zwangsläufig mit ganz

erheblichen Rechtsunsicherheiten verbunden ist. Der pauschale Verweis auf die Art. 7 ff. DS-GVO, der als Ersatzgrund ohne weitere Ausführungen genannt wird, vermag hierbei auch nicht zu helfen. Höchst zweifelhaft ist überdies, ob im polizeilichen Kontext überhaupt jemals eine freiwillige Einwilligung als essenzielle Wirksamkeitsvoraussetzung herbeigeführt werden kann. Aufgrund dieser immanenten Unsicherheit würde der polizeilichen Datenverarbeitung selbst bei Bestehen des Einwilligungstatbestands kein Gefallen getan. Außerdem kann die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen werden. Dass von der Schriftform der Einwilligung aus beliebigen Gründen abgesehen werden kann, erscheint vor dem Hintergrund der Nachweispflicht für die Einwilligung umso befremdlicher. Kritisch zu würdigen ist zudem die Formulierung in Abs. 2, wonach die Einwilligung auch noch „andere Sachverhalte“ betreffen kann. Die Einwilligung im polizeilichen Kontext auch als Legitimationsgrundlage zur Verarbeitung sensibler personenbezogener Daten (Abs. 5) heranzuziehen, ist nicht tragbar.

13. § 20 Abs. 1

Auch § 20 Abs. 1 ist im Hinblick auf die Ermächtigungsgrundlagen zur polizeilichen Verarbeitung sensitiver Daten zu modifizieren. Es wird zwar zunächst in Anlehnung an § 48 BDSG 2018 eine Einengung der Verarbeitungsbefugnis bestimmt, indem die polizeiliche Datenverarbeitung nur möglich ist, soweit dies zur Aufgabenerfüllung unbedingt erforderlich ist. Mit der Einbeziehung der Einwilligung in § 20 Abs. 1 Nr. 4 wird diese rechtlich notwendige Begrenzung aber wiederum völlig relativiert, indem auch die Einwilligung der betroffenen Person als Legitimationsgrund ausreichend sein soll. Für die Kritik im Einzelnen wird auf die entsprechenden Ausführungen schon zu § 19 des Entwurfs verwiesen.

14. § 20 Abs. 2

Geeignete technische und organisatorische Vorkehrungen sind essenziell für den Schutz von (sensiblen) personenbezogenen Daten. Da einige der nicht abschließend aufgeführten Maßnahmen jedoch eine höhere Relevanz als andere besitzen, sollte die Formulierung hier „sollten“, und nicht „können“, lauten. Alternativ sind spezifische Maßnahmen als verpflichtend zu beschreiben, z.B. die Datenverschlüsselung, die Zugangs- und Zugriffskontrolle sowie die Festlegung der Aussonderungsfristen.

15. § 21 Abs. 2

§ 21 Abs. 2 Nr. 2 sollte an den Wortlaut der Nr. 1 angepasst werden. So wird für die personengebundenen Hinweise für die Verarbeitung eine „Erforderlichkeit“ vorausgesetzt, wohingegen für die weiteren standardisierten Hinweise schon die „Geeignetheit“ ausreichend ist. Für den Gleichlauf der Vorschriften sollten deshalb auch hier an das Erforderlichkeitskriterium angeknüpft werden.

16. § 22 Abs. 1

§ 22 regelt die Kennzeichnungspflicht für Datenspeicherungen durch die Vollzugspolizei. Nach Abs. 1 S. 1 Nr. 1 hat die Angabe des Mittels der Erhebung der Daten, einschließlich der Angabe, ob die Daten offen oder verdeckt erhoben wurden, zu erfolgen. Abs. 1 S. 2 bestimmt, dass diese Kennzeichnung auch durch die Angabe der Rechtsgrundlage der jeweiligen Mittel der Datenerhebung ergänzt werden kann. Nicht ersichtlich ist, warum die Angabe der Rechtsgrundlage hier nicht obligatorisch sein sollte, da jede (vollzugs)polizeiliche Datenverarbeitung auf eine entsprechende Rechtsgrundlage zu stützen ist.

17. § 22 Abs. 2

In dieser Norm wird vorgeschrieben, dass personenbezogene Daten, die nicht der Kennzeichnungspflicht nach Abs. 1 genügen, nicht verarbeitet oder übermittelt werden dürfen. Ergänzt werden sollte diese Vorschrift um einen weiteren Satz, der eine Ausschlussfrist festsetzt: Soweit die Kennzeichnung (insbesondere die Benennung der Rechtsgrundlage und des Verarbeitungszwecks) nicht innerhalb eines Jahres erfolgt, sind die personenbezogenen Daten zu löschen.

18. § 23

§ 23 betrifft die grundsätzliche Zweckbindung von personenbezogenen Daten, die durch die Vollzugspolizei erhoben wurden. Zweckänderungen sind gemäß der verfassungsgerichtlichen Rechtsprechung nur unter Beachtung des Grundsatzes der hypothetischen Datenneuerhebung möglich. Für § 23 Abs. 3 S. 2 ist ein formaler Fehler zu beseitigen: „die im Wege der verdeckten akustischen Wohnraumüberwachung [erlangt wurden]“. Ein weiterer formaler Fehler findet sich in Abs. 4 S. 2, hier ist „wegen der“ als Dopplung zu streichen. Abs. 6 S. 1 ist in seiner gegenwärtigen Fassung überdies zu weit gefasst, soweit es um die Erstellung von Lagebildern geht: Weshalb hier die vorbeugende Kriminalitätsbekämpfung mit der Verkehrsüberwachung gleichgesetzt wird, ist nicht ersichtlich. Abs. 7 regelt die Verarbeitung von personenbezogenen Daten u.a. zu Ausbildungszwecken. Hier sollte in Abs. 1 ergänzt werden, dass eine Verwendung personenbezogener Daten für diese Zwecke nur möglich ist, soweit eine Anonymisierung „technisch“ nicht möglich ist (selbiges gilt für Abs. 8 S. 1 der Vorschrift). Für Abs. 7 S. 3 stellt sich die Frage, weshalb sich die ausschließlich anonymisierte Form der Datenverwendung nur auf solche Daten bezieht, die mittels Einsatzes technischer Mittel in oder aus Wohnungen erhoben wurden – das informationsbezogene polizeiliche Eingriffsrepertoire sieht an dieser Stelle eine

Vielzahl an Mitteln vor, die geeignet sind, den höchstpersönlichen Lebensbereich der betroffenen Person zu tangieren.

19. § 26 Abs. 3

Gem. § 26 Abs. 3 S. 1 Nr. 4 unterbleiben Löschung und Vernichtung von personenbezogenen Daten, wenn eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit einem unverhältnismäßigen Aufwand möglich ist. Ein derartiger Auffangtatbestand, der aus älteren bzw. bestehenden polizeirechtlichen Regelungen entnommen wurde, entspricht zwar durchaus noch dem Standard, sollte in seiner Weite aber konkretisiert werden, dies kann in erster Linie durch die Aufzählung von Regelbeispielen geschehen. So ist zumindest zurzeit nicht erkennbar, in welchen Fällen bei einer grds. digitalen Datenspeicherung ein unverhältnismäßiger Aufwand bestehen soll. Auch die Entwurfsbegründung liefert hier keine Hinweise.

20. § 27 Abs. 1

Das Führen von Protokolldaten ist zwingend notwendig, um wichtig Schutzziele der IT- und Datensicherheit zu erfüllen, wozu vor allem die Authentizität und Integrität digitaler Daten zählen, sollen diese zu polizeilichen Ermittlungszwecken eingesetzt werden. Zu jedem Managementsystem der Informationssicherheit gehört die zweifelsfreie Identifizierbarkeit von Nutzern, die Zugriff auf Datenbestände hatten. Hier kann es somit nicht ausreichend sein, wenn das Gesetz lediglich vorschreibt, dass die Identifizierung der datenverarbeitenden Personen nur „so weit wie möglich“ stattfinden soll, da mittels Verwendung eindeutiger Benutzerkennungen eine zweifelsfreie Identifizierbarkeit technisch möglich ist.

21. § 28 Abs. 1

§ 28 Abs. 1 S. 4 der Entwurfsfassung bestimmt, dass ein Abgleich der gem. § 17 Abs. 1 Nr. 5-8 erlangten personenbezogenen Daten (Personen mit besonderen Kenntnissen für die Gefahrenabwehr, Anlagenverantwortliche, Veranstaltungsverantwortliche) nur bei Vorliegen einer datenschutzrechtlichen Einwilligung stattfinden darf. Hier stellt sich wie generell für den Einwilligungstatbestand im Polizeirecht die Frage nach der Freiwilligkeit der Einwilligung, und damit zwangsläufig auch für die Möglichkeit einer Nachweisbarkeit durch die Polizeibehörde.

22. § 32 Abs. 3

Für die rechtliche Beurteilung des Einsatzes der Body-Cam wird auf die von mir getätigte ausführliche Stellungnahme zur Anhörung des Ausschusses für Inneres und Sport am 21. April 2016 zum Gesetzentwurf zur Änderung des Saarländischen Polizeigesetzes vom 10. März 2016, Drs. 15/1734, verwiesen, da auch beim gegenwärtig gewählten Regelungsvorschlag nach wie vor rechtliche Bedenken bestehen. Diese betreffen die generelle Tonaufzeichnung, die dargelegten Schutzziele, die angelegte Gefahrenschwelle, und den Einsatz in privaten Wohnräumen. Positiv anzumerken ist, dass in Abs. 5 nunmehr ausdrücklich datenschutzfreundliche Rahmenregelungen für den Kameraeinsatz vorgesehen sind.

23. § 45 S. 2

§ 45 hat die Übermittlung von personenbezogenen Daten an Behörden, öffentliche oder sonstige Stellen zum Gegenstand. Im Speziellen regelt S. 2 die Datenübermittlung der Polizei u.a. an außerhalb des öffentlichen Bereichs liegende Stellen. Im Hinblick hierauf ist die Regelung der Nr. 2 kritikwürdig, da sie festlegt, dass eine Datenübermittlung dann zulässig ist, soweit sie unter Beachtung des §

23 erfolgt und zur Erfüllung der polizeilichen Aufgaben nach diesem Gesetz erforderlich ist. Der Verweis auf den § 23 ist an dieser Stelle zu pauschal und bietet keine konkreten Anhaltspunkte für eine auf diesen speziellen Fall zugeschnittene Zulässigkeitsprüfung der Datenübermittlung, dies gilt ebenso für den pauschalen Verweis auf „Aufgaben nach diesem Gesetz“. Gerade wenn personenbezogene Daten, die für Gefahrenabwehr oder Strafverfolgung relevant sind, an nicht-öffentliche Stellen übermittelt werden, von denen unter Umständen nicht dasselbe Maß an Vertraulichkeit und Sicherheit ohne Weiteres erwartet werden kann, müssen die Voraussetzungen der Datenübermittlung enger gefasst werden.

24. § 46

Im Generellen sollten, da automatisierte Abrufverfahren erhöhte Gefahren für die Datensicherheit bergen können, an dieser Stelle technisch-organisatorische Sicherheitsmaßnahmen Eingang in den Gesetzeswortlaut finden.

II. Artikel 4: Einschränkung von Grundrechten

Die verfassungsgerichtliche Rechtsprechung zieht für den Eingriff in die Integrität eines informationstechnischen Systems weite Grenzen. Im Gesetzentwurf werden technische Maßnahmen vorgeschlagen, die geeignet sind, die Integrität eines IT-Systems über die konkrete Maßnahme hinaus im Ganzen zu beeinträchtigen. Fraglich ist deshalb, warum an dieser Stelle in der Aufzählung nur das Grundrecht auf informationelle Selbstbestimmung und das Fernmeldegeheimnis genannt werden. Ergänzt werden sollte hier konkret das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (IT- bzw. Computer-Grundrecht).

Bremen, den 29. April 2020

(Dr. Dennis-Kenji Kipker)