Landesbeauftragte
für Datenschutz und Informationsfreiheit
Nordrhein-Westfalen

LANDTAG
NORDRHEIN-WESTFALEN
17. WAHLPERIODE

STELLUNGNAHME
17/696

A14

LDI NRW, Postfach 20 04 44, 40102 Düsseldorf
Der Präsident
des Landtags Nordrhein-Westfalen
Platz des Landtags 1
40221 Düsseldorf

per E-Mail an: anhoerung@landtag.nrw.de

Aktenzeichen
bei Antwort bitte angeben
207.1.2

Telefon 0211 38424-
Fax 0211 38424-10

Gesetzesentwurf der Landesregierung zur Umsetzung des bereichsspezifischen Datenschutzes im Bereich der Justiz (Justizdatenschutz-Anpassungsgesetz - JustDSAnpG)

Ihr Schreiben vom 24. Mai 2018, Ihr Zeichen: I.1

Sehr geehrter Herr Präsident,

sehr geehrte Damen und Herren Abgeordnete,

für die Gelegenheit zur Stellungnahme danke ich Ihnen.

Zunächst möchte ich mich ausdrücklich für die frühzeitige Information und Beteiligung durch das Ministerium der Justiz bedanken, das bereits im Vorfeld zur Einbringung dieses Entwurfs (d. E.) in den Landtag viele meiner datenschutzrechtlichen Hinweise aufgegriffen und umgesetzt hat. Insgesamt ist festzustellen, dass der Entwurf ersichtlich von dem Bestreben getragen ist, sowohl die Richtlinie (EU) 2016/680[1] (JI-RL) umzusetzen als auch die jüngste Rechtsprechung des Bundesverfassungsgerichts (BVerfG) zu berücksichtigen.

Die folgende Stellungnahme ist in erster Linie darauf gerichtet, die vorgesehenen Gesetzesnovellierungen aus datenschutzrechtlicher Sicht nachzuvollziehen und ggf. zu beurteilen. Sofern ich im Rahmen der datenschutzrechtlichen Prüfung in einzelnen Punkten darauf aufmerksam geworden bin, dass mit Blick auf die Richtlinie oder die Rechtsprechung

Dienstgebäude und Lieferanschrift:
Kavalleriestraße 2 - 4
40213 Düsseldorf
Telefon 0211 38424-0
Telefax 0211 38424-10
poststelle@ldi.nrw.de
www.ldi.nrw.de

Öffentliche Verkehrsmittel:
Rheinbahnlinien 704, 709, 719
Haltestelle Poststraße

[1] 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.

Handlungsbedarf besteht, werden diese Aspekte ebenfalls angesprochen.

I. Zu Artikel 1 d. E.

Gesetz zum Schutz personenbezogener Daten im Justizvollzug in Nordrhein-Westfalen (Justizvollzugsdatenschutzgesetz Nordrhein-Westfalen – JVollzDSG NRW)

A. Vorbemerkungen

Mit der grundsätzlichen Zielrichtung des Entwurfs stimme ich überein, für den Anwendungsbereich der Richtlinie im Justizvollzug einen möglichst einheitlichen Rechtsrahmen zu schaffen sowie dort, wo die Richtlinie Regelungsspielräume lässt, das bisherige Datenschutzniveau des Landes aufrechtzuerhalten. Ferner begrüße ich ausdrücklich die Entscheidung, die datenschutzrechtlichen Vorschriften für die verschiedenen Bereiche des Justizvollzugs in einem Gesetz zusammenzufassen. Dies dient der Transparenz und erleichtert die Rechtsanwendung.

Allerdings wird das selbst gesetzte Ziel der Aufrechterhaltung des bisherigen Datenschutzniveaus noch nicht umfassend erreicht. Hierauf gehe ich in den Anmerkungen zu den jeweiligen Vorschriften unter B. noch im Einzelnen ein. Einige Regelungen, die aus datenschutzrechtlicher Sicht besonders bedenklich erscheinen, möchte ich jedoch bereits an dieser Stelle ausdrücklich hervorheben.

Zur Videoüberwachung von Hafträumen zu Forschungszwecken bzw. Technikentwicklungen

Schwerwiegende datenschutzrechtliche Bedenken bestehen hinsichtlich der in § 24 Abs. 7 Satz 2 d. E. vorgesehenen Regelung, mit Videokameras gewonnene Bilder aus der Haftraumüberwachung zur Entwicklung eines Computerprogramms aufzuzeichnen und zu verwenden. Bereits die bloße Videobeobachtung eines Haftraums stellt einen massiven Eingriff in das Recht auf informationelle Selbstbestimmung dar, der verfassungsrechtlich nur im Einzelfall unter besonderen Voraussetzungen zu rechtfertigen ist. Die nun vorgesehene Regelung, die mittels eines solchen schwerwiegenden Grundrechtseingriffs erhobenen Daten dar-

über hinaus allein zu Forschungszwecken zu speichern und zu nutzen, missachtet die Grundrechte der Gefangenen, die in ihrer Situation dem Staat generell in besonderer Weise ausgeliefert sind. Auch wenn das Ziel, Suizide wirksam zu verhindern, als solches selbstverständlich nicht in Rede steht, dürfen die Einzelnen gerade in dieser besonderen Situation nicht zum Gegenstand und bloßen Objekt der staatlichen Forschung gemacht werden. Angesichts dieser grundlegenden Bedenken kann derzeit auch dahinstehen, ob und inwieweit der Einsatz sogenannter intelligenter Videoüberwachung in Zukunft überhaupt geeignet wäre, Suizidversuche selbständig sowie sicher zu erkennen und diese wirksam zu verhindern, was zumindest äußerst zweifelhaft erscheint.

Aus datenschutzrechtlicher Sicht ist es deshalb unerlässlich, in § 27 Abs. 2 Satz 2 d. E. zumindest die Worte *„Entwicklung und“* ersatzlos zu streichen.

Zu Fallkonferenzen

Neue und nicht unerhebliche datenschutzrechtliche Eingriffe sind ferner im Rahmen der Durchführung sogenannter Fallkonferenzen in § 28 d. E. vorgesehen. Die besondere datenschutzrechtliche Brisanz ergibt sich daraus, dass – wie in der Begründung des Entwurfs zutreffend ausgeführt wird – Fallkonferenzen über eine punktuelle Datenübermittlung aufgrund anderer Vorschriften hinausgehen (vgl. S. 172 d. E.). Bei diesen Konferenzen werden letztlich wesentlich mehr Daten an wesentlich mehr Stellen übermittelt, als dies auf der Grundlage anderer Datenschutzvorschriften zulässig wäre. Es handelt sich dabei um eine Übermittlung „auf Vorrat“, die zudem im Wesentlichen auf einer Prognose beruht. Wie die Gesetzesbegründung darlegt sind Fallkonferenzen in bestimmten Fällen zur Gefahrenabwehr unerlässlich. Auch wenn die Argumentation grundsätzlich nachvollziehbar erscheint, ist damit allein die datenschutzrechtliche Besorgnis nicht ausgeräumt. Vielmehr muss aus Sicht des Datenschutzes auf jeden Fall sichergestellt werden, dass diese Konferenzen auf wichtige Einzelfälle beschränkte und besondere Ausnahmen bleiben, ihre Durchführung umfassend dokumentiert und das Instrument der Fallkonferenz nach einem angemessenen Zeitraum evaluiert wird. Diesbezüglich gibt es noch Handlungsbedarf (vgl. im Einzelnen unten).

Zum Grundsatz der Direkterhebung

Eine deutliche Absenkung des bisherigen Datenschutzniveaus droht etwa durch die in § 9 d. E. vorgesehene Vorschrift „*Erhebung bei betroffenen Personen und öffentlichen Stellen*“. Anders als es die Begründung vermuten lässt kann von der Aufrechterhaltung des bisherigen Grundsatzes der Direkterhebung bei der betroffenen Person im Hinblick auf den Gesetzeswortlaut nicht die Rede sein, da nunmehr die gleichrangige Möglichkeit geschaffen werden soll, die in Rede stehenden Daten auch bei einer öffentlichen Stelle zu erheben, also eine Dritterhebung durchzuführen. Zwar können einige der in der Begründung genannten Argumente für Ausnahmen vom Direkterhebungsgrundsatz sprechen, wie sie die aktuelle Regelung aber auch bisher zulässt; eine Rechtfertigung für die Schaffung einer grundsätzlichen Befugnis zur Erhebung bei öffentlichen Stellen kann daraus jedoch keinesfalls abgeleitet werden.

B. Zu den einzelnen Vorschriften

Zu § 3 d. E.

Absatz 3 sollte um folgenden Satz aus der Begründung ergänzt werden: *„Die Daten sind entsprechend ihrer Kategorie zu kennzeichnen, soweit sich nicht bereits aus den Daten selbst ergibt, welcher Kategorie sie zuzuordnen sind.“*

Zu § 4 d. E.

Absatz 2 sollte noch um die Regelungen ergänzt werden, dass die betroffene Person vor der Erklärung der Einwilligung umfassend über den gesamten geplanten Prozess der Datenverarbeitung sowie auch die hierfür verantwortlichen Stellen/Personen zu informieren ist. Am Ende des Absatzes sollte es heißen, dass die betroffene Person stets über die Folgen einer Verweigerung der Einwilligung zu informieren ist. Dies sind (weitere) wichtige Voraussetzungen dafür, dass die Einwilligung in informierter Weise im Sinne des § 2 Nr. 18 d. E. (sogenannte „informierte Einwilligung“) erfolgt. Aus den Erfahrungen meiner Beratungspraxis kann ich versichern, dass die Beachtung dieser Teilaspekte keineswegs selbstverständlich ist.

Zu § 5 d. E.

Der Vorentwurf sah in Absatz 3 Satz 3 noch folgende Regelung vor: *„Die Vollzugsbehörden haben den Nachweis für den offenkundig unbegründeten Antrag oder exzessiven Charakter eines Antrags zu erbringen."* Mit der Überarbeitung des Texts in Absatz 3 ist diese Nachweispflicht der Vollzugsbehörde entfallen. Auch in der Begründung erfolgt keine Klarstellung. Im Hinblick auf Art. 12 Abs. 4 Satz 3 JI-RL sollte die Nachweispflicht der Vollzugsbehörde wieder in den Entwurf aufgenommen werden.

Zu § 9 d. E.

§ 9 d. E. sollte unbedingt überarbeitet werden. Wie unter A. bereits ausgeführt ist in Absatz 1 in der vorgelegten Fassung gerade nicht die Aufrechterhaltung des Direkterhebungsgrundsatzes normiert, sondern dieser wird vielmehr unterlaufen. Die Erhebung bei der betroffenen Person und bei öffentlichen Stellen wird als gleichwertig geregelt und in eine „Oder-Alternative" gestellt. Damit wird der Direkterhebungsgrundsatz gegenüber der bisherigen Form[2] konterkariert. So werden die gesetzgeberischen Ziele zu gewährleisten, dass Gefangene über ihre Daten weitestgehend selbst bestimmen können sollen (vgl. S. 149, Pkt. 3 d. E.), und das bisherige Datenschutzniveau aufrechtzuerhalten gleichermaßen verfehlt. Die Regelung entspricht auch nicht der Einleitung der Gesetzesbegründung (vgl. S. 150 d. E.), wonach der Grundsatz der Direkterhebung wie im bisherigen Recht weitergelten soll, die erforderlichen Daten also beim Gefangenen selbst und nur im Ausnahmefall bei Dritten zu erheben. Die für die Gefangenen möglicherweise unangenehmen Fälle der wiederholten Erhebung von Daten sind zwar eventuell verständliche Ausnahmefälle, und ich kann das in der Begründung zu § 9 d. E. genannte Argument, dass in solchen Fällen die Mitwirkungsbereitschaft der Gefangenen leiden kann, nachvollziehen. Allerdings könnten diese Fälle auch entsprechend als Ausnahme vom Direkterhebungsgrundsatz geregelt werden. Beispielsweise könnte normiert werden, dass die Daten dann bei einer öffentlichen Stelle erhoben werden dürfen, wenn die betroffene Person die Angabe von Daten, zu der sie verpflichtet ist, verweigert. Für den Fall, dass es den Gefangenen lieber ist,

[2] Vgl. § 108 Abs. 2 StVollzG NRW i. V. m. § 12 Abs. 1 DSG NRW a. F.

die Daten ggf. auch zum wiederholten Male selbst bereitzustellen, wäre es – entgegen der Begründung – nicht in ihrem Sinne, die Daten bei einer öffentlichen Stelle zu erheben.

Die genannten Bedenken werden auch nicht dadurch ausgeräumt, dass in der Begründung ausgeführt wird, der Direkterhebung von Daten bei den Gefangenen würde aufgrund des Grundsatzes der Richtigkeit, Vollständigkeit und Aktualität der Daten in der Praxis nach wie vor vielfach der Vorrang vor einer direkten Erhebung bei öffentlichen Stellen eingeräumt werden (vgl. S. 160 d. E.). Solange dieser Gedanke zum einen so abstrakt bleibt, und zum anderen keinen Niederschlag im Gesetzestext selbst findet, ist zu besorgen, dass der Direkterhebungsgrundsatz in der Anwendungspraxis keine Beachtung findet.

Zu § 12 d. E.

Das Bundesverfassungsgericht (BVerfG) hat in seinem Urteil zum Bundeskriminalamtgesetz[3] (BKAG-Urteil) umfangreich ausgeführt, wann eine Zweckänderung vorliegt und unter welchen Voraussetzungen eine zweckändernde Verarbeitung personenbezogener Daten zulässig ist. Diese Rechtsprechung ist auch im Bereich des Justizvollzuges zu berücksichtigen. Eine Zweckänderung liegt nach der Rechtsprechung des BVerfG immer dann vor, wenn personenbezogene Daten durch eine andere Behörde oder durch dieselbe Behörde jedoch zur Erfüllung einer anderen Aufgabe oder zum Schutz anderer Rechtsgüter verarbeitet werden, als der Erhebung zu Grunde lagen.[4] In diesem Zusammenhang ist darauf hinzuweisen, dass die in § 1 Abs. 3 d. E. genannten vollzuglichen Zwecke in diesem Sinne als ein und derselbe Zweck anzusehen sind. In § 12 Abs. 1 d. E. wird dementsprechend zutreffend davon ausgegangen, dass keine Zweckänderung vorliegt, wenn personenbezogene Daten, die von einer Vollzugsbehörde zu einem der vollzuglichen Zwecke nach § 1 Abs. 3 d. E. erhoben wurden, von der derselben Behörde zu einen anderen vollzuglichen Zweck i. S. d. § 1 Abs. 3 d. E. verarbeitet werden. Im Umkehrschluss bedeutet dies jedoch, dass wann immer dieselbe Vollzugsbehörde personenbezogene Daten, die zu einem vollzuglichen Zweck erhoben wurden, zu einem nicht-vollzuglichen Zweck verarbeitet oder an eine andere Behörde übermittelt, eine Zweckänderung gegeben ist.

[3] Urteil vom 20. April 2016 (1 BvR 966/09 und 1 BvR 1140/06).
[4] BVerfG, BKAG-Urteil, Rn. 282.

Wenn eine Zweckänderung vorliegt, muss nach der Rechtsprechung des BVerfG der geänderte Zweck in einem angemessenen Verhältnis zur Art der personenbezogenen Daten und zur Art und Eingriffsintensität des Mittels stehen, mit dem die Daten erhoben wurden.[5] Informationen, die durch besonders eingriffsintensive Maßnahmen (beispielsweise erkennungsdienstliche Behandlung) erlangt wurden, dürfen somit auch nur zu besonders gewichtigen Zwecken (beispielsweise Abwehr einer Gefahr für die öffentliche Sicherheit) genutzt werden. Zwischen beiden muss ein angemessenes Verhältnis bestehen. Da die vollzuglichen Zwecke des § 1 Abs. 3 d. E. in einem gleichrangigen Verhältnis zueinander stehen, ist diese Angemessenheit bei der Übermittlung personenbezogener Daten an andere Behörden zu vollzuglichen Zwecken gegeben. Daher stellt § 13 Abs. 3 d. E. folgerichtig nur für den Fall, in dem personenbezogene Daten von Vollzugsbehörden zu nichtvollzuglichen Zwecken an andere öffentliche Stellen übermittelt werden, besondere Vorgaben auf.

Da § 13 Abs. 3 d. E. jedoch in den Fällen des § 12 Abs. 2 d. E. die Angemessenheit regelmäßig bejaht, ist sicherzustellen, dass § 12 Abs. 2 d. E. auch nur solche gewichtigen Zwecke enthält, die dies rechtfertigen können. Dies gilt für § 12 Abs. 2 Nr. 4 d. E. bisher nicht. Dessen Zusatz *„durch welche die Sicherheit oder Ordnung der Anstalt gefährdet wird“* gilt ausweislich der Begründung allein für die Variante *„Verhinderung oder Verfolgung von Ordnungswidrigkeiten“*. Daher wäre eine Zweckänderung für jegliche Form von Straftaten – also auch für Bagatelldelikte – zulässig. Statt *„Straftaten“* sollte es daher mindestens *„erhebliche Straftaten“* heißen.

Zu § 13 d. E.

Dass Absatz 3 – wie bereits angesprochen – zur Umsetzung der Rechtsprechung des BVerfG bereits eine Regelung zur Abwägung der Zulässigkeit einer zweckändernden Nutzung personenbezogener Daten enthält, ist ausdrücklich zu begrüßen.

Da § 13 Abs. 7 Satz 2 d. E. mit der Möglichkeit der Übermittlung zu ausländerrechtlichen Maßnahmen einen weiteren Fall der Übermittlung zu vollzugsfremden Zwecken an andere öffentliche Stellen regelt, muss sich Absatz 3 jedoch auch auf diesen Fall beziehen. Es ist nicht ersicht-

[5] Sog. „hypothetische Datenneuerhebung“.

lich, dass jeder Fall der Verarbeitung zu ausländerrechtlichen Maßnahmen in einem angemessenen Verhältnis zur Art und Weise der Erhebungsform sowie der Art der erhobenen Daten steht. Immerhin lässt der Entwurf gegenüber Dritten teils auch eingriffsintensive Maßnahmen wie erkennungsdienstliche Behandlungen zu, mit denen zudem besondere Kategorien personenbezogener Daten erhoben werden. Weder im Gesetzestext selbst noch in der Begründung wird hierzu etwas ausgeführt. Eine Klarstellung könnte erfolgen, indem § 13 Abs. 7 Satz 2 d. E. zu § 13 Abs. 2 Satz 2 würde. Dann wären diese Fälle klar vom nachfolgenden Absatz 3 erfasst.

Zu § 14 d. E.

Soweit in Absatz 1 Satz 4 eine Verbunddatei gemeint ist, in der die Gefangenendaten jederzeit vorgehalten werden und auf die von allen Justizvollzugsanstalten (JVA) jederzeit zugegriffen werden kann, bestehen erhebliche datenschutzrechtliche Bedenken. Diese ergeben sich schon daraus, dass die abgebenden JVA die Daten regelmäßig zu löschen haben. Somit dürfte jeweils immer nur eine JVA Zugriff auf die jeweiligen Datensätze haben. Der regelmäßigen Vorteile einer Verbunddatei, gerade den gleichzeitigen Zugriff mehrerer Stellen zu ermöglichen, bedarf es in diesen Fällen somit nicht. Das zusätzliche Risiko für personenbezogene Daten, welches Verbunddateien mit sich bringen, ist deshalb nicht in Kauf zu nehmen. Sollte lediglich eine technische Plattform gemeint sein, auf der die Daten zu den Gefangenen zwischen den JVA im Bedarfsfall übermittelt werden können, ist dies im Gesetzestext klarzustellen.

Zu § 15 d. E.

In Absatz 1 ist unbedingt auf die Erforderlichkeit bzw. unbedingte Erforderlichkeit der Datenübermittlung zu diesen Zwecken abzustellen. Anderenfalls gäbe es außer der Zweckbindung kaum Begrenzungen für Datenübermittlungen an nicht-öffentliche Stellen.

Zu § 18 d. E.

In Absatz 2 findet sich eine Übermittlungsregelung für die besondere Situation, dass personenbezogene Daten mit weiteren Daten derselben

oder einer dritten Person in Akten so verbunden sind, dass eine Trennung etc. nicht möglich ist. Damit es in der Regel gar nicht zu dieser Situation kommt, sollte an geeigneter Stelle noch die Regelung des § 4 Abs. 6 Satz 1 DSG NRW a. F. in den Entwurf aufgenommen werden: *„Die Datenverarbeitung soll so organisiert sein, dass bei der Verarbeitung, insbesondere bei der Übermittlung, die Kenntnisnahme im Rahmen der Aufgabenerfüllung und der Einsichtnahme, die Trennung der Daten nach den jeweils verfolgten Zwecken und nach unterschiedlichen Betroffenen möglich ist."* Zwar wird in der Begründung zu § 34 Abs. 2 d. E. ausgeführt, dass die Regelung des § 4 Abs. 6 Satz 1 DSG NRW a. F. in § 34 Abs. 2 Satz 4 d. E. übernommen wurde. § 34 Abs. 2 d. E. enthält jedoch keinen vierten Satz, und die Regelung findet sich im Übrigen weder in § 18 d. E. noch in § 34 d. E. oder an einer anderen Stelle des Entwurfs.

Zu § 20 d. E.

In Absatz 1 sollte grundsätzlich auf die Erforderlichkeit – und im Fall von besonderen Kategorien personenbezogener Daten auf die unbedingte Erforderlichkeit – der Erhebung der genannten personenbezogenen Daten abgestellt werden.

Ich empfehle, Absatz 3 Satz 2 dahingehend umzuformulieren, dass „*eine Übermittlung der Fingerabdruckdaten an das Landeskriminalamt*" nur dann erfolgt, *„wenn Nr. 1 die Identität einer oder eines Gefangenen nicht bereits anderweitig gesichert ist, Nr. 2 ein Abgleich der Fingerabdruckdaten mit den dem Justizvollzug vorliegenden Daten nicht möglich ist oder Nr. 3 eine Gefährdung der Sicherheit der Anstalt nicht ausgeschlossen werden kann."* Im Übrigen geht die Regelung des Absatz 3 Satz 10, wonach die angefragten Behörden die ihnen übermittelten personenbezogenen Daten löschen, soweit diese nicht zur Dokumentation erforderlich sind, ins Leere, wenn es sich dabei um Bundesbehörden handelt, die nicht durch Landesgesetz verpflichtet werden können.

Absatz 4 regelt mit dem Verweis auf die Zwecke des § 12 Abs. 2 Nr. 4 d. E. einen Fall der Zweckänderung. Die nach § 20 d. E. erhobenen Daten sollen zu vollzugsfremden Zwecken (Strafverfolgung) an andere öffentliche Stellen übermittelt werden können. Zunächst muss die Übermittlung zu diesen Zwecken (unbedingt) erforderlich sein. Eine entsprechende Ergänzung des Entwurfs ist erforderlich, da Absatz 4 allein auf die Zwecke des § 12 Abs. 2 d. E. verweist, nicht jedoch auf dessen sonstige

Voraussetzungen. Daneben nehme ich auf die obigen Ausführungen zu § 12 Abs. 2 Nr. 4 d. E. Bezug. Darüber hinaus ist – wie zuvor bei § 13 Abs. 7 Satz 2 d. E. – auch hier deutlich zu machen, dass § 13 Abs. 3 d. E. auch in diesem Kontext zu beachten ist. Dies könnte beispielsweise erfolgen, indem hinter *„dürfen“* die Worte *„unbeschadet des § 13 Abs. 3“* eingefügt werden.

Zu § 21 d. E.

Absatz 12 enthält mit der Übermittlungsmöglichkeit an öffentliche Stellen für Maßnahmen des ambulanten Sozialen Dienstes der Justiz und der Jugendgerichtshilfe sowie zu Zwecken des § 12 Abs. 2 Nr. 1 bis 3 d. E. Regelungen zur Zweckänderung. Zumindest mit dem Verweis auf § 12 d. E. sollen damit auch die Übermittlungen an sonstige öffentliche Stellen zu vollzugsfremden Zwecken – also Fälle des § 13 Abs. 3 d. E. – möglich sein. Es ist somit klarzustellen, dass § 13 Abs. 3 d. E. auch in diesem Kontext zu beachten ist. Dies könnte beispielsweise erfolgen, indem hinter *„erfolgt“* die Worte *„unbeschadet des § 13 Abs. 3“* eingefügt werden.

Zu § 23 d. E.

Im Vorentwurf war in Absatz 2 Satz 3 noch geregelt, dass jede Auslesung des Gefangenenausweises nur mit bewusster Zustimmung der betroffenen Person erfolgen darf, wobei die Zustimmung auch durch schlüssiges Handeln erteilt werden kann. Diese Regelung ist ersatzlos entfallen. Aus datenschutzrechtlicher Sicht sollte eine Auslesung zumindest nicht ohne Kenntnis des Gefangenen erfolgen dürfen.

Zu § 24 d. E.

In Bezug auf die Regelungen in § 24 d. E. besteht zum Teil noch dringender Überarbeitungsbedarf.

Obwohl es sich bei der Überwachung mit Videokameras um einen besonderen Eingriff in das Recht der Betroffenen auf informationelle Selbstbestimmung handelt, legt die Regelung in Absatz 1 zunächst nahe, dass eine solche Überwachung zu den genannten Zwecken uneingeschränkt zulässig ist. Erst in Absatz 3 finden sich im Zusammenhang mit der Planung einer solchen optisch-elektronischen Überwachung ge-

wisse Einschränkungen. Ich empfehle, diese Einschränkungen bereits in die Rechtsgrundlage des Absatzes 1 aufzunehmen und somit ausdrücklich klarzustellen, dass die Videoüberwachung nur unter diesen einschränkenden Voraussetzungen zulässig ist.

In Bezug auf Absatz 6 ist mir nicht ersichtlich, warum quasi für den Regelfall eine Aufbewahrungsdauer von zwei Wochen vorgesehen wird. Grundsätzlich sind personenbezogene Daten zu löschen, sobald ihre weitere Speicherung zur Aufgabenerfüllung nicht mehr erforderlich ist, und dies dürfte bei vielen der Bildaufnahmen nach deutlich kürzerer Zeit der Fall sein. Mit dieser Ergänzung wäre dann auch der Zusatz hinnehmbar, dass die Löschung spätestens nach zwei Wochen zu erfolgen hat.

Absatz 7 Satz 2 und Absatz 8 sind aus den unter A. bereits dargelegten Gründen zumindest in der dort beschriebenen Form zu überarbeiten.

Zu § 25 d. E.

Der Entwurf schreibt zu Recht fest, dass jede Videoüberwachung im konkreten Einzelfall erforderlich bzw. unbedingt erforderlich sein muss. Vorsorglich möchte ich in diesem Zusammenhang darauf hinweisen, dass eine Videoüberwachung im Außenbereich der Anstalt zur Abwehr von Drohnenabwürfen regelmäßig weder geeignet noch erforderlich sein dürfte. Zum einen ist sie nicht in jedem Fall geeignet, derartige Vorkommnisse zu verhindern, da Drohnen sogar ohne Sichtkontakt gesteuert werden können. Zum anderen stehen zumindest dort, wo im unmittelbaren Anstaltsumfeld regelmäßig unbeteiligte Dritte (Anwohner etc.) durch die Videoüberwachung beeinträchtigt würden, in der Regel die schutzwürdigen Belange dieser Personen einer Videoüberwachung entgegen. Auch dürften regelmäßig mildere, weniger eingriffsintensive Maßnahmen als eine Videoüberwachung möglich sein. In Betracht kommen beispielsweise das Überspannen der jeweiligen JVA-Flächen mit Netzen oder die Nutzung von Störsendern.

Zu § 27 d. E.

Die mit § 53 Abs. 4 StVollzG NRW geschaffene Möglichkeit der elektronischen Aufenthaltsüberwachung (EAÜ) habe ich bei dessen Einführung mit meiner Stellungnahme vom 07. Oktober 2016 bereits wie folgt kritisiert:

„Mit seinem Urteil vom 17. Dezember 2009 (NJW 2010, 2495) hatte der Europäische Gerichtshof für Menschenrechte (EGMR) die nachträgliche Sicherungsverwahrung für unvereinbar mit der Konvention zum Schutz der Menschenrechte und Grundfreiheiten (EMRK) erklärt. Vor diesem Hintergrund hat der Bundesgesetzgeber im Rahmen der Führungsaufsicht die Möglichkeit einer neuen strafbewehrten und von der Einwilligung des Verurteilten unabhängigen Weisung geschaffen, mit der einer verurteilten Person aufgegeben werden kann, die für eine elektronische Überwachung ihres Aufenthaltsortes erforderlichen technischen Mittel ständig bei sich zu führen und deren Funktionsfähigkeit nicht zu beeinträchtigen (vgl. § 68b Absatz 1 Satz 1 Nr. 12 Strafgesetzbuch - StGB). Diese Regelung soll vor allem spezialpräventiv wirken, da sie eine bessere Überwachung der Einhaltung von aufenthaltsbezogenen Weisungen ermöglichen und somit ein erhöhtes Entdeckungsrisiko im Falle einer erneuten schweren Straftat begründen soll. Zudem soll es den Behörden erleichtert werden, im Falle einer von dem Straftäter ausgehenden gegenwärtigen erheblichen Gefahr für Leib oder Leben einzuschreiten (vgl. BT-Drs. 17/3403). Dies vorausgeschickt ist derzeit aus datenschutzrechtlicher Sicht die Erforderlichkeit der Überwachung von Gefangenen mittels eines elektronischen Überwachungssystems bei Ausführungen zur Erhaltung der Lebenstüchtigkeit und bei Ausführungen aus wichtigem Anlass nicht zu bejahen. Der Zweck einer solchen elektronischen Aufenthaltsüberwachung beschränkt sich allein darauf, dass Entweichungen entgegengewirkt werden soll. Dieser Zweck wird aber bereits dadurch erreicht, dass bei der Ausführung von Gefangenen eine ständige und unmittelbare Aufsicht durch Bedienstete gewährleistet ist und ggf. zusätzlich der Gefangene auf herkömmliche Weise gefesselt ist. Eine Vergleichbarkeit ist insoweit schon nicht gegeben.“

Diese Kritik hat weiterhin Bestand. Da § 53 Abs. 4 StVollzG NRW offensichtlich dennoch beibehalten werden soll, sollte § 27 d. E., der die datenschutzrechtlichen Rahmenbedingungen für die mittels EAÜ erhobenen Daten regelt, hilfsweise wenigstens wie folgt überarbeitet werden: Es sollte ergänzend geregelt werden, dass die durch das Überwachungsgerät erhobenen Daten über die Speicherung hinaus bis zu deren Löschung in keiner Weise verarbeitet werden dürfen, solange der Alarmfall im Sinne des Absatzes 8 nicht ausgelöst wird oder innerhalb der Speicherfrist eine Ausnahme nach Absatz 7 Satz 2 eintritt. Der Zugriff auf die Daten ist vielmehr bis zum Eintritt eines der genannten Fälle zu sperren, das heißt die Verarbeitung ist einzuschränken. Dies bedeu-

tet, dass ohne Alarmfall oder das Eintreten einer Ausnahme nach Absatz 7 Satz 2 lediglich die Erhebung und Löschung dieser Daten erfolgen.

Sofern Absatz 7 die Fortspeicherung für spätere Übermittlungen zu vollzugsfremden Zwecken an öffentliche Stellen zulässt (beispielsweise *„für die Verfolgung von Straftaten")* ist eine mit § 13 Abs. 3 d. E. vergleichbare Abwägung vorzusehen.

Zu § 28 d. E.

Die besondere datenschutzrechtliche Brisanz der neu eingeführten *„Fallkonferenzen*" ist bereits unter A. (s.o.) dargelegt worden. Wie oben ausgeführt muss aus Gründen des Datenschutzes auf jeden Fall sichergestellt werden, dass diese Konferenzen auf wichtige Einzelfälle beschränkte und besondere Ausnahmen bleiben, ihre Durchführung umfassend dokumentiert und das Instrument der Fallkonferenz nach einem angemessenen Zeitraum evaluiert wird.

§ 28 d. E. nebst Begründung hat im Vorfeld der Einbringung des Entwurfs in den Landtag mehrfach so grundlegende Änderungen erfahren, dass es schwierig ist, diese noch in allen Punkten nachzuvollziehen und darauf zu achten, dass der Datenaustausch hinreichend beschränkt bleibt.

Dass die Vollzugsbehörde in Absatz 1 schon *„aus Anlass"* von Fallkonferenzen personenbezogene Daten verarbeiten darf ist auf jeden Fall zu weitgehend. Eine Datenverarbeitung im Rahmen von Fallkonferenzen kann nur dann zulässig sein, wenn sie zur Durchführung der Konferenz einschließlich Vor- und Nachbereitung und unter den weiterhin normierten Voraussetzungen erforderlich ist. Der bloße „Anlass" einer solchen Konferenz genügt nicht.

Auch in Absatz 2 muss der Austausch personenbezogener Daten unter die Voraussetzung der Erforderlichkeit gestellt werden. Dies ist bisher nicht der Fall. Soweit auch personenbezogene Daten besonderer Kategorien nach § 28 d. E. verarbeitet werden, ist (auch in Absatz 1 und 3) auf die unbedingte Erforderlichkeit abzustellen.

Das Erforderlichkeitsprinzip muss ferner auch in Absatz 4 und Absatz 5 festgeschrieben werden, und in Absatz 5 genügt ebenfalls der bloße „Anlass" einer Fallkonferenz nicht, um eine Verarbeitung personenbezogener Daten zu rechtfertigen.

Zudem stellt die Übermittlung personenbezogener Daten an Dritte – wie grundsätzlich jede Datenübermittlung (s.o.) – auch innerhalb von Fallkonferenzen eine Zweckänderung dar. Die obigen Ausführungen – insbesondere in Bezug auf § 13 Abs. 3 d. E. – gelten entsprechend.

Ob das Instrument der Fallkonferenz insgesamt tatsächlich auf die notwendigen Fälle beschränkt oder uferlos eingesetzt wird, wird sich zuverlässig vermutlich erst im Nachhinein auf der Grundlage einer soliden Datenbasis im Rahmen einer Evaluation feststellen lassen. Daher sollte dieses Instrument nach einer angemessenen Erprobungszeit unbedingt einer Evaluation unterzogen und dies ausdrücklich gesetzlich verankert werden. Die allgemeine Berichtspflicht des § 47 Abs. 3 d. E. ist hierfür nicht ausreichend.

Zu § 30 d. E.

Diesbezüglich nehme ich auf meine Ausführungen zu § 14 d. E. Bezug.

Zu § 32 d. E.

§ 32 d. E. regelt, dass personenbezogene Daten, die mittels besonders eingriffsintensiver Methoden erhoben wurden, nur zu besonderen Zwecken weiterverarbeitet werden dürfen. Nach den Ausführungen in der Gesetzesbegründung stellt § 32 d. E. selbst keine Ermächtigungsgrundlage für Datenverarbeitungen dar, sondern stellt lediglich besondere Schutzanforderungen auf. Mindestens § 32 Nr. 1 d. E. umfasst jedoch Fälle der Zweckänderung. Um klarzustellen, dass § 32 d. E. die Weiterverarbeitung in diesen Fällen nicht etwa erlauben, sondern allein auf diese Fälle beschränken möchte, sollte ein Satz 2 angefügt werden, wonach die Vorschriften zu Zweckänderungen (insbesondere §§ 12 und 13 d. E.) unberührt bleiben.

Zu § 34 d. E.

Die Regelungen der Absätze 3 bis 6, insbesondere auch die Pflicht zur Erstellung eines Sicherheitskonzeptes, sind aus datenschutzrechtlicher Sicht sehr zu begrüßen. Bezüglich des Verweises auf § 56 DSG NRW

gilt meine hierzu erfolgte Stellungnahme vom 12. April 2018[6] entsprechend. In Absatz 3 Nr. 7 sollte statt „Nicht-Verkettbarkeit“ der Begriff „Nichtverkettung“ verwendet werden.

Zu § 35 d. E.

Die Protokollierung dient der Abmilderung des Grundrechtseingriffs und stellt in automatisierten Verarbeitungsprozessen auch praktisch keine Schwierigkeit dar. Daher sollten in automatisierten Verarbeitungsprozessen sämtliche Verarbeitungsschritte protokolliert werden. Die Vorgaben des Art. 25 JI-RL sind insoweit nicht als abschließende Vollregelung zu verstehen.

Zu § 40 d. E.

In Bezug auf die Regelung in Absatz 1 gelten meine obigen Ausführungen zu § 18 d. E. entsprechend.

Zu § 42 d. E.

In Absatz 1 sollte eine Löschpflicht auch für den Fall aufgenommen werden, dass die weitere Speicherung der personenbezogenen Daten *„für vollzugliche oder andere nach diesem Gesetz oder den Vollzugsgesetzen anerkannte Zwecke nicht mehr erforderlich“* ist. In Absatz 2 sollte aufgenommen werden, dass die Löschung *„spätestens“* nach den dort vorgesehenen Zeiträumen zu erfolgen hat. Weiterhin sollte aufgenommen werden, dass das weitere Vorliegen der Speicherungsvoraussetzungen jährlich zu überprüfen ist. Alle drei Aspekte fanden sich bereits in einem Vorentwurf. Warum sie ersatzlos gestrichen wurden ist nicht ersichtlich. Dass diese Regelungen entfallen sind, ist datenschutzrechtlich bedenklich.

Bezüglich der Regelung in Absatz 4 gelten wiederum meine obigen Ausführungen zu § 18 d. E. entsprechend.

Absatz 7 sollte dahingehend ergänzt werden, dass die empfangenden Stellen bei der Übermittlung auf die Löschungspflicht hinzuweisen sind.

---

[6] MMST 17/508, abzurufen unter: https://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument?Id=MMST17/508.

Im Übrigen rege ich an zu erwägen, im Rahmen der Löschungsvorschrift auch eine Regelung zur vorrangigen Anbietung von Daten an die öffentlichen Archive aufzunehmen.

Zu § 43 d. E.

Absatz 1 Satz 1 Nr. 5 ist hinsichtlich der Variante *„Datenschutzkontrolle“* nachvollziehbar. Der Sinn bezüglich der Variante „*Datensicherung*“ erschließt sich jedoch nicht. Wenn Daten zu löschen sind, sind auch die entsprechenden Datensicherungen zu löschen. Wenn gemeint ist, dass alle Daten, die nur zur Datensicherung weiter gespeichert sind, in der Verarbeitung einzuschränken sind, passt dies nicht zum Anfang des Absatzes, wonach § 43 Abs. 1 d. E. nur statt einer gebotenen Löschung gilt.

Die Ausnahme in Absatz 1 Satz 1 Nr. 6 ist zu unbestimmt. Hier sollte mindestens das Schutzniveau von § 10 Abs. 10 DSG NRW erhalten bleiben, indem die Ausnahme auf die nicht automatisierte Verarbeitung beschränkt ist und sich ferner nicht auf die unrechtmäßige Verarbeitung erstreckt.

Die Ausnahme in Absatz 2 Satz 2 „*zur Verfolgung von Straftaten*“ ist zu unbestimmt. Die obigen Ausführungen zu Zweckänderungen gelten entsprechend.

Zu § 44 d. E.

In Absatz 4 sollten entsprechend der Ausführungen zu § 39 Abs. 5 d. E. die Ausnahmen jeweils nur gelten, „*soweit*“ sie zu den genannten Zwecken erforderlich sind.

Zu § 45 d. E.

Soweit in § 45 d. E. generell auf das DSG NRW und insbesondere die Regelungen zur LDI NRW und deren Befugnisse inklusive Rechtschutz- und Sanktionsmöglichkeiten, zu Datenübermittlungen in Drittstaaten sowie straf- und ordnungsrechtliche Bestimmungen Bezug genommen wird, verweise ich grundsätzlich auf meine diesbezügliche Stellungnah-

me vom 12. April 2018[7]. Einige der dort genannten Kritikpunkte möchte ich an dieser Stelle jedoch noch einmal besonders hervorheben:

- Vollstreckungsmöglichkeiten der LDI NRW zur Durchsetzung ihrer Anordnungen gegenüber öffentlichen Stellen
- Recht der Aufsichtsbehörden, den Justizbehörden Verstöße gegen nach der JI-RL erlassene Vorschriften zur Kenntnis zu bringen und gerichtliche Verfahren – auch gegen öffentliche Stellen – einleiten zu können
- Datenübermittlungen ins Ausland

Zu § 46 d. E.

Das Gesetz greift zumindest mit § 25 d. E. auch in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ein. § 46 d. E. sollte entsprechend ergänzt werden.

II. Zu Artikel 2 bis 6 d. E.

Gegen die Änderungen bestehen keine datenschutzrechtlichen Bedenken. Ausweislich der Begründung enthalten die Artikel – mit Ausnahme von Artikel 6 – lediglich Folgeänderungen, die sich aus der zentralen Regelung der Datenschutzvorschriften im Vollzugsbereich im in Artikel 1 vorgesehenen JVollzDSG NRW ergeben. Die übrigen in Artikel 6 vorgesehenen Änderungen sind nicht von primär datenschutzrechtlicher Relevanz.

Mit freundlichen Grüßen

(Block)

Helga Block

[7] Vgl. Fußnote 6.