Schleswig-Holsteinischer Landtag
Umdruck 19/4779

www.datenschutzzentrum.de

Landesbeauftragte für Datenschutz • Postfach 71 16 • 24171 Kiel

Schleswig-Holsteinischer Landtag
Innen- und Rechtsausschuss
Vorsitzende
Düsternbrooker Weg 70
24105 Kiel

per E-Mail:
innenausschuss@landtag.ltsh.de

Landesbeauftragte für Datenschutz
Holstenstraße 98
24103 Kiel
Tel.: 0431 988-1200
Fax: 0431 988-1223

Ansprechpartner/in:
Barbara Körffer
Durchwahl: 988-1216

Aktenzeichen:
LD5-73.13/20.001

Kiel, 4. November 2020

Entwurf eines Justizvollzugsmodernisierungsgesetz, LT-Drs. 19/2381
Schriftliche Anhörung; Ihr Schreiben vom 6. Oktober 2020

Sehr geehrte Frau Vorsitzende,
sehr geehrte Damen und Herren Abgeordnete,

ich bedanke mich für die Gelegenheit, zu dem oben genannten Gesetzentwurf Stellung zu nehmen.

Aufgrund des beträchtlichen Umfangs des Gesetzentwurfs kann ich nicht auf alle Aspekte des Entwurfs eingehen, die eventuell einen Bezug zum Datenschutz aufweisen können. Ich beschränke mich daher auf den für Datenschutz relevantesten Teil des Gesetzentwurfs, die Neufassung des Justizvollzugsdatenschutzgesetzes Schleswig-Holstein in Artikel 6 des Entwurfs.

Nach wie vor bin ich von dem Sinn einer gemeinsamen Datenschutzregelung für alle Vollzugsarten überzeugt und begrüße daher, dass das Justizvollzugsdatenschutzgesetz auch in Umsetzung der Richtlinie (EU) 2016/680 fortgeführt wird. Gerade durch die europäische Gesetzgebung sind die von den öffentlichen Stellen zu beachtenden Datenschutzvorschriften noch breiter verteilt, als dies bislang der Fall war. Im Interesse einer möglichst einfachen Handhabbarkeit für den Rechtsanwender begrüße ich alle Bemühungen des Gesetzgebers, Datenschutzvorschriften in einem oder wenigen Regelwerken zu konzentrieren und so die Anzahl zu beachtender Gesetze gering zu halten. Ebenso begrüße ich die Bestrebungen einer bundesweit einheitlichen Gesetzgebung, die auch dem vorliegenden Entwurf zu Grunde liegen.

Bei der Durchsicht des Entwurfs für das Justizvollzugsdatenschutzgesetz fällt auf, dass dieser zweierlei Arten von Änderungen enthält. Dies sind zum einen diejenigen Änderungen, die der Umsetzung der Richtlinie (EU) 2016/680 dienen. Zum anderen enthält der Entwurf aber auch Änderungen gegenüber dem geltenden Justizvollzugsdatenschutzgesetz, die nicht erkennbar durch die Umsetzung der EU-Richtlinie veranlasst sind. Hierbei handelt es sich fast durchweg um Einschränkungen für die Datenschutzrechte der betroffenen Personen, die überwiegend aus meiner Sicht nicht nachvollziehbar sind und datenschutzrechtlichen Bedenken begegnen.

Im Ergebnis sind aus datenschutzrechtlicher, verfassungsrechtlicher und europarechtlicher Sicht an einer Vielzahl von Stellen Änderungen der Formulierungen im Entwurf geboten.

Zu den Regelungen im Einzelnen:

Zu § 2 JVollzDSG-E – Begriffsbestimmungen

a) Nr. 8 Begriff der „Anonymisierung"

Die **Begriffsbestimmung zur „Anonymisierung"** steht **nicht im Einklang mit der Richtlinie (EU) 2016/680**: Danach wären Daten auch dann anonymisiert, wenn sie nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden könnten. Die Richtlinie (EU) 2016/680 enthält keine Definition des Begriffs „Anonymisierung". Sie kennt nur einerseits personenbezogene Daten und andererseits solche Daten, die keinen Personenbezug aufweisen. Letztere werden in Erwägungsgrund 21 der Richtlinie als „anonyme Informationen" bezeichnet. Sie sind vom Anwendungsbereich der Richtlinie nicht erfasst. Daraus ergibt sich, dass anonymisiert nur solche Daten sein können, die nicht oder nicht mehr personenbezogen sind. Daten, die mit unverhältnismäßig großem Aufwand einer Person zugeordnet werden können, sind hingegen personenbezogen. Dementsprechend kann der Anonymisierungsprozess im Sinne der Richtlinie auch nur zu solchen Daten führen, die einer Person absolut nicht mehr zugeordnet werden können.

b) Nr. 20 Begriff der „anstaltsfremden Person"

Aus dem vorliegenden Wortlaut der **Begriffsbestimmung zur „anstaltsfremden Person"** ergibt sich, dass sämtliche Personen, die im Auftrag einer Behörde tätig sind, unabhängig von ihrer Tätigkeit nicht „anstaltsfremd" sind. Das kann nicht so gemeint sein; vielmehr sollte doch entscheidend sein, inwieweit eine Beziehung der Tätigkeiten oder Aufgaben zur Justizvollzugsbehörde besteht. Daher sollte die **Formulierung um Aufgaben bezüglich der Justizvollzugsbehörde ergänzt** werden.

Zu § 4 JVollzDSG-E – Zulässigkeit der Datenverarbeitung, Einwilligung

Nach § 4 Abs. 1 des Entwurfs soll die Datenverarbeitung unter anderem zulässig sein, wenn die betroffenen Personen eingewilligt haben und der Einwilligung ein gesetzliches Verbot nicht entgegensteht.

Es bestehen **erhebliche Zweifel, ob die Einwilligung als allgemeine Grundlage für die Verarbeitung personenbezogener Daten richtlinienkonform** ist. Im Gegensatz zur Verordnung (EU) 2016/679 (Artikel 6 Abs.1 Buchst. a DSGVO), in der die Einwilligung als Rechtsgrundlage konkret normiert ist, hat der Richtliniengeber in der Richtlinie (EU) 2016/680 die Einwilligung als alleinige Grundlage der Datenverarbeitung bewusst nicht vorgesehen.

Nach Artikel 8 Abs. 1 der Richtlinie ist eine Datenverarbeitung nur dann rechtmäßig, wenn sie zur Erfüllung einer Aufgabe der zuständigen Behörde erforderlich ist und auf der Grundlage des Unionsrechts oder des Rechts der Mitgliedstaaten erfolgt. Die Vorschrift muss nach Artikel 8 Abs. 2 der Richtlinie zumindest die Ziele der Verarbeitung, die personenbezogenen Daten, die verarbeitet werden sollen, und die Zwecke der Verarbeitung angeben.

Dass die Einwilligung als Verarbeitungsgrund nicht vollständig ausgeschlossen ist, legen zwar die Erwägungsgründe 35 und 37 der Richtlinie nahe. Dabei stellt Erwägungsgrund 35 jedoch heraus,

dass die Einwilligung als alleinige Rechtsgrundlage in der Regel nicht in Betracht kommt. Nach Erwägungsgrund 35 sollen die Mitgliedstaaten jedoch die Möglichkeit haben, „durch Rechtsvorschriften vorzusehen, dass die betroffene Person der Verarbeitung ihrer personenbezogenen Daten für die Zwecke dieser Richtlinie zustimmen kann, beispielsweise im Falle von DNA-Tests in strafrechtlichen Ermittlungen oder zur Überwachung ihres Aufenthaltsorts mittels elektronischer Fußfessel zur Strafvollstreckung."

Die Einwilligung ist also als allgemeine Grundlage für die Verarbeitung personenbezogener Daten gemäß der Richtlinie nicht vorgesehen, kann aber für Einzelfälle gesetzlich geregelt werden. Dieser Einzelfallcharakter schlägt sich auch in der allgemeinen Regel des § 27 LDSG nieder. Daraus wiederum eine Norm abzuleiten, die die Einwilligung als allgemeine Grundlage für die Verarbeitung personenbezogener Daten zum Zwecke der Gefahrenabwehr vorsieht, geht deutlich über die Vorgaben der Richtlinie hinaus.

Es bestehen daher **Bedenken**, ob § 4 Abs. 1 des Entwurfs **europarechtskonform** ist.

Zu § 6 JVollzDSG-E – Zulässigkeit der Datenerhebung

a) Begrifflichkeiten

Der Gesetzwurf behält die aus dem bisherigen Datenschutzrecht bekannten Begriffe der „Erhebung" (Abschnitt 2), „Speicherung" und „Nutzung" (Abschnitt 3) sowie „Übermittlung" (Abschnitt 4) bei. Anders als im bisherigen Recht sind diese **Begriffe nicht mehr definiert**. Dies kann **in der Anwendung zu Unsicherheiten** führen, da die jeweiligen Vorschriften des Entwurfs anders als die Richtlinie (EU) 2016/680 und das neue Landesdatenschutzgesetz nicht den gesamten Umgang mit personenbezogenen Daten regeln, sondern nur punktuell einzelne Formen der Verarbeitung personenbezogener Daten.

Auch **Regelungslücken** sind nicht auszuschließen, da die Erlaubnisse nur für bestimmte Arten der Verarbeitung, **nicht aber für alle Verarbeitungen personenbezogener Daten geregelt** werden, wie dies zu erwarten wäre.

b) Zweckbestimmung

Die Zweckbestimmung der „vollzuglichen Zwecke" ist sehr vage und unbestimmt. Klarer und bestimmter ist dagegen die Regelung im geltenden Justizvollzugsdatenschutzgesetz, die nicht allgemein auf vollzugliche Zwecke abstellt, sondern konkret auf die **„Aufgaben des Vollzugs"**. Dies entspricht auch der Richtlinie, die in Artikel 8 Abs. 1 für die Rechtmäßigkeit der Verarbeitung ebenfalls nicht auf die Zwecke im Allgemeinen, sondern im Rahmen dieser Zwecke auf die konkrete Aufgabe der Verantwortlichen abstellt. Ein Grund für die hier gewählte davon abweichende Regelung ist nicht erkennbar. Es sollte daher die Formulierung aus dem geltenden Justizvollzugsdatenschutzgesetz beibehalten werden oder eine ähnliche auf die jeweiligen Aufgaben bezogene Formulierung gewählt werden. Der Begriff der „vollzuglichen Zwecke" sollte **durchgängig im Gesetz durch diese Formulierung ersetzt** werden.

c) Anforderung an die Verarbeitung besonderer Kategorien

aa) Erforderlichkeit

Der Entwurf verwendet für die von der Richtlinie geforderte gesteigerte Erforderlichkeit den **Begriff „unbedingt erforderlich"**, wie er auch in Artikel 10 der Richtlinie und im Bundesdatenschutzgesetz

verwendet wird. Das Landesdatenschutzgesetz verwendet dagegen, z. B. in § 24 Abs. 1 Nr. 1, den **Begriff „zwingend erforderlich“**. Ich rege an zu prüfen, ob eine **Vereinheitlichung** mit den übrigen Landesregelungen sinnvoll ist **oder** ob eine **Angleichung** an die Vorschriften im Bundesrecht als sinnvoller erachtet wird.

Im Übrigen weise ich darauf hin, dass der Begriff der gesteigerten Erforderlichkeit, unabhängig davon ob als unbedingt oder zwingend erforderlich bezeichnet, inhaltlich eigentlich keinen höheren Schutz der Daten gewährleisten kann. Denn bereits die „einfache“ Erforderlichkeit ist im Sinne einer „conditio sine qua non“ zu verstehen, sodass die Erreichung des Zwecks ohne die Verarbeitung der Daten nicht möglich sein darf. Eine Steigerung ist denklogisch nicht möglich. Dass der Gesetzgeber nun eine weitere Stufe der Erforderlichkeit einführt, birgt die Gefahr, dass die Voraussetzungen der „einfachen“ Erforderlichkeit abgewertet werden. Dies ist aber bereits in der EU-Richtlinie angelegt und kann durch den nationalen Gesetzgeber nicht beeinflusst werden. **Bei der Anwendung des Gesetzes ist aber darauf zu achten, dass auch die „einfache“ Erforderlichkeit im Sinne einer zwingenden Bedingung für die Erreichung des Zwecks ausgelegt wird.**

bb) Geeignete Garantien

Die Richtlinie (EU) 2016/680 verlangt in Artikel 10 nicht nur ein erhöhtes Maß an Erforderlichkeit. Ebenfalls verlangt sie **geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen**. Da es denklogisch eine Steigerung der Erforderlichkeit nicht geben kann, kommt den Garantien für die Datenverarbeitung eine besondere Bedeutung zu. Hierzu enthalten die **Zulässigkeitsnormen der §§ 6, 10 und 12 des Entwurfs keine Regelungen**. Voraussetzungen für die geeigneten Garantien müssten nach Artikel 10 bei allen diesen Regelungen aufgenommen werden. Sie können auch zusammengefasst geregelt werden, wie dies etwa in § 24 Abs. 2 LDSG der Fall ist. Besonders wichtig ist dies bei der nach § 12 Abs. 6 des Entwurfs zugelassenen Übermittlung an nichtöffentliche Stellen. Für die Justizvollzugsbehörden können Garantien für die Verarbeitung besonderer Arten von Daten auch an anderer Stelle in diesem Gesetz geregelt werden. Bei anderen öffentlichen und erst recht bei anderen nichtöffentlichen Stellen kann der Gesetzgeber sich nicht darauf verlassen, dass dort geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen im Sinne gegeben sind. Der Gesetzgeber muss daher die Empfänger verpflichten, bestimmte von ihm vorgegebene Garantien zu erfüllen.

Im Ergebnis sind die **geeigneten Garantien für die Verarbeitung besonderer Arten von Daten sowohl für die Justizvollzugsbehörden als auch für die Empfänger der Daten zu regeln**. Hier besteht Ergänzungsbedarf.

Zu § 10 JVollzDSG-E – Speicherung und Nutzung

Absatz 1 enthält den Grundsatz der Zweckbindung. Dieser ist **unpräzise** und damit zu weitgehend formuliert. Nach dem Datenschutzrecht ist die weitere Verarbeitung personenbezogener Daten nur zu dem konkreten Zweck zulässig, zu dem die Daten erhoben wurden. Es reicht also nicht aus, wie im Entwurf auf die allgemeine Zweckbestimmung der Erhebung – zu vollzuglichen Zwecken – abzustellen. Vielmehr müsste die Regelung lauten:

„Die Justizvollzugsbehörden dürfen personenbezogene Daten, die sie zulässig erhoben haben, speichern und nutzen, soweit dies für den Zweck, für den sie erhoben wurden, erforderlich ist.“

Zu § 12 – Übermittlung an öffentliche und nichtöffentliche Stellen

In Absatz 8 Satz 2 muss es anstelle von „berechtigten Interesse“ **„schutzwürdiges Interesse“** heißen.

Zu §§ 13-15 JVollzG-E – Überprüfung Gefangener und anstaltsfremder Personen

Mit diesen Vorschriften wird eine Befugnis zur Überprüfung Gefangener durch Einholung von Auskünften bei Justiz- und Sicherheitsbehörden eingeführt. Die Anfragebefugnis ist auf Fälle beschränkt, in denen tatsächliche Anhaltspunkte für eine dem Gefangenen zurechenbare Gefahr für die Sicherheit der Anstalt drohen. Hier wird der **Begriff der „drohenden Gefahr“** eingeführt, der bislang im schleswig-holsteinischen Landesrecht noch nicht bekannt ist. Die Figur der drohenden Gefahr hat bei ihrer Einführung in anderen Landesgesetzen viel Kritik erfahren; es wurden vielfach **Zweifel an der Verfassungsmäßigkeit** geäußert. Diese Bedenken gelten auch für die Regelung im vorliegenden Entwurf.

Fraglich ist zudem, ob der Begriff der sicherheitsrelevanten Erkenntnisse **in § 13 Abs. 2** des Entwurfs den Anforderungen an die Bestimmtheit genügt. Der Begriff ist laut Begründung bewusst nicht abschließend definiert. So sollen etwa auch psychische Auffälligkeiten, die im Gesetz nicht genannt sind, nach der Begründung als sicherheitsrelevant in Betracht kommen. Durch die **unbestimmte Regelung** besteht das Risiko, dass die angefragten Behörden Informationen mitteilen, die für den jeweiligen Zweck nicht erforderlich sind. Dieses Risiko sollte **durch konkretisierende Regelungen der sicherheitsrelevanten Erkenntnisse im Gesetz** begrenzt werden. Gleiches gilt für sicherheitsrelevante Erkenntnisse in Bezug auf anstaltsfremde Personen nach **§ 15** des Entwurfs.

Zu § 16 JVollzG-E – Fallkonferenzen

§ 16 regelt besondere Befugnisse für den Datenaustausch zwischen Justizvollzugsbehörden und den in § 16 des Entwurfs genannten Behörden, die nur im Rahmen von Fallkonferenzen gelten sollen. Warum die Befugnisse zum Datenaustausch zwischen den in § 16 des Entwurfs genannten Behörden nicht auch außerhalb von Fallkonferenzen gelten sollen – beispielsweise bei bilateralen Anfragen von Behörden -, erschließt sich nicht. Die Fallkonferenz bekommt dadurch eine herausgehobene Bedeutung. Vor diesem Hintergrund verwundert es, dass der **Begriff der Fallkonferenz nicht im Gesetz definiert** wird. Weder das genaue **Ziel** der Fallkonferenz noch die **Teilnehmenden** werden beschrieben. In den einzelnen Absätzen des § 16 werden offenbar teilweise die Anlässe einer Fallkonferenz und teilweise die Voraussetzungen der Übermittlung personenbezogener Daten geregelt. Ein Anlass für eine Fallkonferenz ist beschrieben in Absatz 1 Satz 2 („Fallkonferenzen dürfen auch zur Vorbereitung von Ausführungen [...] stattfinden“) und in Absatz 3 Satz 1 („Fallkonferenzen dürfen zwischen [...] stattfinden, sofern [...]“). Die Voraussetzungen für die Übermittlung personenbezogener Daten sind beschrieben für die Fallkonferenzen nach Absatz 1 Satz 1 und nach Absatz 2. Die **Systematik** sollte **vereinheitlicht** werden und **es sollten für jede Art von Fallkonferenz deren Anlass, die Teilnehmer und die Voraussetzungen für die Übermittlung personenbezogener Daten geregelt werden.**

Zu § 17 JVollzG-E – Weitere Zulässigkeitsvoraussetzungen für die Datenverarbeitung mit den Sicherheitsbehörden

Die Regelung soll ausweislich der Begründung vor allem die Anforderungen aus der Entscheidung des BVerfG vom 20.04.2016 zum BKAG, hauptsächlich diejenigen der hypothetischen Datenneuerhebung, umsetzen.

In Absatz 1 wird demzufolge für eine Übermittlung personenbezogener Daten an Sicherheitsbehörden in erster Linie auf die vergleichbaren Rechtsgüter oder Straftaten abgestellt. Andere **Voraussetzungen, insbesondere die Erforderlichkeit der Übermittlung für einen bestimmten Zweck, fehlen** hingegen. Dies kann auch nicht durch die in Absatz 1 Nr. 1 recht unbestimmt formulierte Voraussetzung „sich im Einzelfall konkrete Ansätze ergeben" ersetzt werden. Die Entwurfsfassung würde die Anforderungen aus der **bundesverfassungsgerichtlichen Entscheidung** nicht korrekt umsetzen; es besteht Nachbesserungsbedarf.

Zu § 25 JVollzG-E – Datenverarbeitung bei Übertragung von Vollzugsaufgaben

Mit dieser Vorschrift soll die Datenverarbeitung durch andere Stellen geregelt werden, die im Wege der so genannten Funktionsübertragung Daten verarbeiten. In Abgrenzung zur gesetzlich geregelten Datenverarbeitung im Auftrag handelt es sich bei der Funktionsübertragung um dritte Stellen, die die Aufgaben in eigener Verantwortung ausüben und hierfür auch in eigener Verantwortung personenbezogene Daten verarbeiten. Dass für die Auswahl solcher Stellen und die Art und Weise der Übertragung der Datenverarbeitung Regeln getroffen werden, ist grundsätzlich zu begrüßen.

Ich rege an, zu **prüfen**, ob die hier gewählten **Begriffe des „Auftrags" und dementsprechend des „Auftragnehmers" und des „Auftraggebers" zutreffend** sind. In datenschutzrechtlicher Hinsicht sind diese Begriffe eng mit dem Begriff des „Auftragsverarbeiters" verknüpft, der gerade nicht in eigener datenschutzrechtlicher Verantwortlichkeit handelt.

Zu § 26 JVollzDSG – Gemeinsame Verantwortung der Justizvollzugsbehörden

Anders als die vorliegende Regelung enthält § 39 Abs. 3 LDSG den Zusatz, dass eine **Vereinbarung zwischen den gemeinsam Verantwortlichen die betroffene Person nicht hindert, ihre Rechte gegenüber jedem der gemeinsam Verantwortlichen geltend zu machen**. Dies sollte auch hier aufgenommen werden, auch wenn es nach Artikel 21 der Richtlinie (EU) 2016/680 nicht zwingend vorgeschrieben ist. Die Vereinbarung zwischen den Verantwortlichen muss nicht zwingend und nicht in vollem Umfang Außenwirkung entfalten. Es käme auch eine Vereinbarung in Betracht, die ausschließlich Binnenwirkung erzeugt. Für die betroffene Person ist dann nicht erkennbar, wie die Verantwortung intern aufgeteilt wurde und an welche Stelle sie sich für welche Rechte bzw. welche Verarbeitung wenden muss. Daher erleichtert eine nach Artikel 21 Abs. 2 der Richtlinie (EU) 2016/680 mögliche Regelung, nach der die betroffene Person ihre Rechte bei und gegenüber jedem einzelnen der Verantwortlichen geltend machen kann, die Rechtewahrnehmung erheblich und ist daher **zu empfehlen**.

Zu § 32 JVollzDSG-E – Optisch-elektronische Einrichtungen innerhalb von Hafträumen und Zimmern

Die Regelung entspricht weitgehend dem geltenden Recht. Eine wesentliche Ausweitung erfährt die Videoüberwachung jedoch insofern, als sie nach Absatz 2 Satz 1 nicht mehr wie im geltenden Recht auf die Abwehr von Gefahren für Leib und Leben der betroffenen Gefangenen beschränkt ist. Die Videoüberwachung könnte daher grundsätzlich auch zum Schutz anderer Personen eingesetzt werden. Laut Begründung des Gesetzentwurfs soll die Überwachung zwar nur zum Schutz der Gefangenen zum Einsatz kommen. Der Gesetzeswortlaut enthält diese Einschränkung jedoch nicht.

Für den Einsatz der Videoüberwachung zum Schutz anderer Personen kann ich die Eignung und damit die Verhältnismäßigkeit des Grundrechtseingriffs nicht feststellen. Hierzu fehlen mir Erkenntnisse, um die fachliche Erforderlichkeit beurteilen zu können. Bislang ist mir nur die Fallkonstellation bekannt, dass ein Gefangener allein in einem besonders gesicherten Raum untergebracht ist und aufgrund der Annahme, dass er sich selbst verletzen könnte, beobachtet werden soll. In diesen Fällen erfolgt die Videobeobachtung anstelle der Sitzwache. Wie eine Videobeobachtung andere Personen vor einer Gefährdung durch den betroffenen Gefangenen ausreichend schützen soll, ist mir nicht bekannt und im Entwurf auch nicht dargelegt.

Es sollte daher im Gesetz durch die Einfügung der **Formulierung „der betroffenen Gefangenen" in § 32 Abs. 2 Satz 1 hinter den Wörtern „für Leib und Leben" klargestellt werden, dass die Videoüberwachung weiterhin nur zu deren Schutz zulässig ist**.

Zu § 40 JVollzDSG-E – Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

a) Vermengung von Artikel 20 und 29 der Richtlinie (EU) 2016/680

Problematisch ist, dass in dieser Regelung die Anforderungen an die Gewährleistung des angemessenen Schutzniveaus für die Verarbeitung personenbezogener Daten (Sicherheit der Verarbeitung) durch technische und organisatorische Maßnahmen nach Artikel 29 der Richtlinie (EU) 2016/680 mit dem Grundsatz des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen nach Artikel 20 der Richtlinie zusammengefasst werden. Dies wird dem unterschiedlichen Charakter beider Regelungen nicht gerecht. **Artikel 20 und 29 der Richtlinie sollten daher in getrennten Vorschriften umgesetzt werden.**

b) Vollständige Umsetzung des Artikels 20 der Richtlinie (EU) 2016/680 erforderlich

Artikel 20 der Richtlinie muss vollständig umgesetzt werden. In der vorliegenden Vorschrift finden sich nur Regelungen zur Umsetzung des Artikels 20 Abs. 2 der Richtlinie (Datenschutz durch datenschutzfreundliche Voreinstellungen – Data Protection by Default), die in Absatz 4 vorgesehen sind. **Regelungen zur Umsetzung des Artikels 20 Abs. 1 der Richtlinie (Datenschutz durch Technikgestaltung – Data Protection by Design) fehlen** hingegen. Die Richtlinie dürfte damit nicht vollständig umgesetzt sein, sodass der Gesetzentwurf insoweit **nicht europarechtskonform** sein dürfte.

c) Begriffe der „Gefahr" und der „Rechtsgüter"

In § 40 des Entwurfs sollte anstelle des Begriffs der „Gefahr für die Rechtsgüter" der betroffenen Personen der **Begriff des „Risikos für „Rechte und Freiheiten" der betroffenen Personen** verwendet werden. Der Begriff des Risikos in Artikel 29 der EU-Richtlinie ist nicht gleichbedeutend mit dem Begriff der „Gefahr" im nationalen Recht, der hauptsächlich aus dem Polizeirecht bekannt ist. Der Begriff des Risikos geht darüber hinaus und soll gerade auch die Möglichkeit solcher Schäden mit in die Betrachtung einfließen lassen, die eher fernliegend sind und deren Eintritt wenig wahrscheinlich ist. Der Begriff der „Rechte und Freiheiten der betroffenen Personen" nimmt Bezug auf die nach der Richtlinie (EU) 2016/680 maßgeblichen Rechte aus der Grundrechtecharta der EU. Um **Schutzlücken** zu **vermeiden**, sollte hier ebenfalls dieser Begriff verwendet werden.

Dies gilt **auch für die nachfolgenden Vorschriften**. Diese verwenden im Übrigen beide Begriffe nebeneinander (so etwa „Risiko" in der Überschrift des § 41 und „Gefahr" in § 41 Abs. 1 des Entwurfs), was ohnehin vermieden werden sollte.

Zur Umsetzung des Artikels 28 der Richtlinie (EU) 2016/680

Eine Regelung zur Umsetzung des Artikels 28 der Richtlinie (EU) 2016/680 (**Vorherige Konsultation der Aufsichtsbehörde**) fehlt im vorliegenden Entwurf. Hierfür wird auf das LDSG Bezug genommen. Dies ist zur Umsetzung der Richtlinie sicherlich ausreichend. In der Praxis wirft dies jedoch voraussichtlich Probleme auf, weil diese zusätzlichen Regelungen zur Datenschutz-Folgenabschätzung von den Rechtsanwendern leicht übersehen werden könnten. Ich rate daher **zu prüfen, ob im Interesse einer einfacheren Handhabbarkeit des Gesetzes für die Rechtsanwender hier auch die Regelung des § 45 LDSG eingefügt** werden sollte.

Zu § 42 JVollzDSG-E – Protokollierung

Es ist zweifelhaft, ob Absatz 2 Satz 2 die Anforderung aus Artikel 25 Abs. 1 Satz 2 der Richtlinie ausreichend umsetzt. Danach müssen die Protokolle über Abfragen und Offenlegungen es ermöglichen, die **Begründung für den Abruf oder die Offenlegung festzustellen**. Der vorliegende Entwurf sieht vor, dass sich die Begründung hierfür aus der Identität der Person ableiten lassen muss. Ob die Identität der abfragenden Person ausreicht, um eine Begründung für den Abruf oder die Offenlegung nachträglich festzustellen, halte ich für äußerst fraglich. Eine Befragung der Person wird zur Ermittlung der Begründung in vielen Fällen nicht ausreichen. Aufgrund der Aufbewahrungsdauer der Protokolldaten für zwei Jahre kann der Zeitpunkt des Abrufs im Fall einer nachträglichen Kontrolle weit zurückliegen, sodass Erinnerungslücken bestehen können. Ein allgemeiner, abstrakter Rückschluss von der Identität der abrufenden Person auf die Begründung für den Abruf kommt ebenfalls nicht infrage. Dies würde bedeuten, dass bloße Annahmen ausreichen würden. Sofern Personen Daten abgerufen haben, die nicht für die Bearbeitung damit verbundener Vorgänge zuständig sind, hätten diese Personen anhand der Protokolldaten keine Möglichkeit, sich bei im Raum stehenden Missbrauchsvorwürfen zu entlasten. **Für eine rechtssichere Umsetzung des Artikels 25 Abs. 1 Satz 2 der Richtlinie (EU) 2016/680 sollte daher die tatsächliche Begründung für den Abruf erfasst und protokolliert werden.**

Zu den Transparenzpflichten in Abschnitt 8

Nach § 53 Abs. 1 des Entwurfs werden den betroffenen Personen bei einer Benachrichtigung über eine ohne ihre Kenntnis vorgenommene Datenverarbeitung **Angaben zur Rechtsgrundlage der Verarbeitung, zur Speicherdauer und zu den Empfängern der personenbezogenen Daten mitgeteilt**. Es erschließt sich nicht, warum diese Angaben nicht auch denjenigen Personen mitgeteilt werden, bei denen personenbezogene Daten direkt und mit deren Kenntnis erhoben werden. Diese sollen nur die eher abstrakten Informationen nach § 51 und § 52 des Entwurfs erhalten. Informationen über die Rechtsgrundlage, die Speicherdauer und die möglichen Empfänger wären in den Fällen der Direkterhebung jedoch ebenso relevant für die betroffenen Personen wie in den Fällen des § 53 des Entwurfs. Sie sind auch nach Artikel 13 Abs. 3 der Richtlinie (EU) 2016/680 für besondere Fälle vorgesehen. Diese Informationen sollten daher **zusätzlich in die Aufklärungspflicht nach § 52 des Entwurfs aufgenommen** werden.

Zu § 54 JVollzDSG-E – Auskunftsrecht der betroffenen Person

In Absatz 2 der Vorschrift wird die grundsätzlich nach der Richtlinie bestehende Auskunftspflicht ausgeschlossen, wenn die Daten aufgrund gesetzlicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder sie ausschließlich zu Zwecken der Datensicherung oder der Datenschutzkontrolle verarbeitet werden, die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde und die Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist.

Diese Vorschrift begegnet **Bedenken im Hinblick auf die Reichweite des Ausschlusses des grundrechtlich garantierten Auskunftsrechts**. Weiterhin ergeben sich terminologische **Unklarheiten**. So ist z. B. nicht klar, was Daten sein sollen, die nur zum Zwecke der Datenschutzkontrolle verarbeitet werden. Obwohl der Begriff auch im geltenden BDSG verwendet wird, findet sich einschlägigen Kommentaren keine Erläuterung dazu.

Der **Ausschluss der Auskunft nach Absatz 3 ist zu weitgehend** gefasst. Für die Interessen der Justizvollzugsbehörden dürfte es ausreichend sein, ein Absehen von der Auskunftserteilung in den hier genannten Fällen zu erlauben und die **Regelung wie in § 33 Abs. 3 LDSG als „Kann-Regelung" auszugestalten**.

Zu § 56 JVollzDSG-E – Auskunft und Akteneinsicht in Gesundheitsakten

Es ist **fraglich**, ob die **Verarbeitung von Daten in Gesundheitsakten** in dem auf die Richtlinie (EU) 2016/680 gestützten Justizvollzugsdatenschutzgesetz geregelt werden kann. Soweit Gesundheitsakten von Ärzten oder anderen Angehörigen von Gesundheitsberufen geführt werden, dürften diese auch für die Datenverarbeitung selbst verantwortlich sein. Solche Personen dürften kaum dem Begriff der Justizvollzugsbehörde in § 1 Abs. 2 des Entwurfs unterfallen und wären damit nicht Adressat dieses Gesetzes. Liegt der Gesundheitsakte eine ärztliche oder sonstige medizinische Behandlung zu Grunde, dürfte es sich dabei auch nicht um „vollzugliche Zwecke" im Sinne des § 2 Abs. 2 Nr. 2 des Entwurfs und auch nicht um Zwecke handeln, die vom Anwendungsbereich der Richtlinie (EU) 2016/680 erfasst sind. Vielmehr wäre dann die Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung – DSGVO) anwendbar. Es würde dann unmittelbar Artikel 15 DSGVO gelten. Eine wiederholende nationale Regelung wäre grundsätzlich ausgeschlossen. **Die hier getroffene Regelung wiederholt nicht den Regelungsgehalt des Artikels 15 DSGVO, sondern widerspricht ihm sogar.** So sieht beispielsweise Artikel 15 Abs. 3 DSGVO einen Anspruch der betroffenen Person auf eine kostenlose Kopie der personenbezogenen Daten vor.

Soweit meine Annahme zutrifft, dass für die hier geregelten Gesundheitsakten die DSGVO anwendbar ist, bestehen gegen die Regelung **erhebliche europarechtliche Bedenken**. Sie sollte in diesem Fall **ersatzlos gestrichen** werden.

Zu § 57 JVollzDSG-E – Sperrvermerke

Ein Vergleich zum geltenden Recht zeigt, dass die in Absatz 1 Nr. 3 vorgesehene weitere Voraussetzung für einen Sperrvermerk nach § 42 JVollzDSG nicht nur für die Nummer 3, sondern für alle Nummern gilt.

Zudem gibt es im geltenden Recht in § 42 Abs. 3 eine Regelung über eine Auskunft an die Gefangenen, die ohne ersichtlichen Grund im vorliegenden Entwurf fehlt. Da für eine weitergehende Einschränkung des Auskunftsanspruchs im Vergleich zum geltenden Recht kein Grund erkennbar ist,

sind diese **Einschränkungen nicht nachvollziehbar**. Es sollte daher **die bisherige Regelung des § 42 JVollzDSG fortgelten**.

Zu § 65 JVollzDSG – Anwendung weiterer Vorschriften des allgemeinen Datenschutzrechts

Es ist nicht nachvollziehbar, warum in § 65 des Entwurfs die **„entsprechende Anwendung“** von Vorschriften des Abschnitts 3 des LDSG angeordnet wird. Ich gehe davon aus, dass diese **Vorschriften unmittelbar anwendbar** sind. Dies ist in der Formulierung **klarzustellen**.

Zum Begriff des Unabhängigen Landeszentrums für Datenschutz

An einigen Stellen verwendet der Entwurf den Begriff des Unabhängigen Landeszentrums für Datenschutz als Bezeichnung der Datenschutzaufsichtsbehörde (z.B. § 54 Abs. 1 Nr. 7 und 8, Abs. 6, Überschrift zu Abschnitt 10 und § 64 JVollzDSG-E). Im Einklang mit dem LDSG sollte für die **Datenschutzaufsichtsbehörde** durchgängig die **Bezeichnung „Landesbeauftragte oder Landesbeauftragter für Datenschutz“** verwendet werden.

Für Rückfragen und für weitere Auskünfte stehe ich Ihnen mit meinem Team gern zur Verfügung.

Mit freundlichen Grüßen

gez. Marit Hansen
Landesbeauftragte für Datenschutz