Schleswig-Holsteinischer Landtag
Umdruck 19/5699

www.datenschutzzentrum.de

Landesbeauftragte für Datenschutz • Postfach 71 16 • 24171 Kiel

Schleswig-Holsteinischer Landtag
Innen- und Rechtsausschuss
Die Vorsitzende

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:
LD5-73.13/20.003

Kiel, 23. April 2021

Entwurf eines Gesetzes zur ambulanten Resozialisierung und zum Opferschutz in Schleswig-Holstein (ResOG SH), Drucksache 19/2681
Ihr Schreiben vom 1. März 2021

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

ich bedanke mich für die Übersendung des oben genannten Gesetzentwurfs und die Gelegenheit zur Stellungnahme.

Zunächst begrüße ich, dass durch den vorliegenden Entwurf klare und bestimmte sowie möglichst einheitliche Regelungen für die Datenverarbeitung der verschiedenen Adressaten getroffen werden. Dies dient der Verständlichkeit und Klarheit und damit auch der Rechtssicherheit für die Anwender. Meine Erfahrung zeigt, dass es häufig an Unkenntnis über die Datenschutzvorschriften oder an Unsicherheiten über deren Auslegung liegt, wenn diese von den Verantwortlichen nicht eingehalten werden. Die unterschiedlichen Regelungsebenen (EU-Recht, allgemeines Datenschutzrecht im Bundes- und im Landesrecht sowie bereichsspezifische Regelungen ebenfalls im Bundes- und im Landesrecht) machen die Materie für die Rechtsanwender kompliziert und schwer durchschaubar. Daher begrüße ich es, wenn der Landesgesetzgeber seinen verbliebenen Regelungsspielraum nutzt und das Datenschutzrecht für die Verantwortlichen klar und verständlich regelt.

Dabei fällt als erstes ins Auge, dass der Gesetzentwurf Klarheit darüber schafft, welches datenschutzrechtliche Rechtsregime für den Adressatenkreis gilt. Nach meiner Einschätzung ist es nicht eindeutig, ob die Tätigkeiten der jeweiligen Adressaten dem Bereich der Strafverfolgung und damit der Richtlinie (EU) 2016/680 (im Folgenden: JI-Richtlinie) zuzuordnen sind oder in den Anwendungsbereich der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung – DSGVO) fallen. Eine gesetzliche Festlegung ist daher im Interesse der Rechtssicherheit zu begrüßen.

Doch gerade weil die Zuordnung der Tätigkeiten zur Strafverfolgung im Sinne der Richtlinie nicht klar auf der Hand liegt, stellt sich die Frage, warum nicht im Interesse des Grundrechtsschutzes für die betroffenen Personen die Datenschutz-Grundverordnung angewendet wird. Diese verleiht den

betroffenen Personen im Allgemeinen weitergehende Rechte, sodass die Grundrechte durch die Anwendung der Datenschutz-Grundverordnung besser verwirklicht würden. Im Übrigen würde durch eine einheitliche Anwendung der Datenschutz-Grundverordnung auch ein Auseinanderfallen der Vorschriften für die öffentlichen Leistungserbringenden auf der einen und die nichtöffentlichen Leistungserbringenden auf der anderen Seite vermieden. Soweit die Leistungserbringenden dieselbe Tätigkeit ausüben, wäre ein unterschiedlicher Maßstab für die Datenverarbeitung schwer begründbar.

Die Datenschutz-Grundverordnung und die JI-Richtlinie schließen sich in ihrem Anwendungsbereich jeweils gegenseitig aus. Dabei wird der Anwendungsbereich ausschließlich sachlich nach den ausgeübten Tätigkeiten bestimmt, denen die Datenverarbeitung dient. Es erscheint daher widersprüchlich, wenn im vorliegenden Gesetzentwurf für die Ausübung der Tätigkeiten durch öffentliche Stellen die JI-Richtlinie und für die Ausübung durch nichtöffentliche Stellen die Datenschutz-Grundverordnung zu Grunde gelegt wird. Ich rege daher an **zu prüfen, ob die Tätigkeiten der Adressaten tatsächlich sämtlich zwingend dem Bereich der Strafverfolgung zuzuordnen** sind. Sofern auch eine **andere Zuordnung infrage kommt, sollte die Datenschutz-Grundverordnung angewendet** werden. Dies würde zudem zu einer Verschlankung der datenschutzrechtlichen Regelungen führen, da vielfach die Vorschriften aus der Datenschutz-Grundverordnung unmittelbar anzuwenden wären.

Zu einzelnen Vorschriften:

Zu den Verarbeitungsbegriffen

Der Gesetzentwurf verwendet die Begrifflichkeiten aus dem Landesdatenschutzgesetz in der vor der EU-Datenschutzreform geltenden Fassung. Seit der EU-Datenschutzreform verwenden die Datenschutzgesetze durchgängig nur noch den Begriff der Verarbeitung personenbezogener Daten. Spezifische Regelungen werden allenfalls punktuell zur Konkretisierung spezifischer Anforderungen an einzelne Phasen der Verarbeitung, z. B. die Übermittlung, getroffen. Der Begriff der Verarbeitung ist dabei umfassend. Dadurch soll sichergestellt werden, dass jegliche Behandlung personenbezogener Daten vom Gesetz erfasst wird und keine Schutzlücken, aber auch keine Befugnislücken entstehen. Die hier verwendete Regelungstechnik mit Generalklauseln für die Verarbeitung in §§ 45 und 46 und der konkreten Ausformung der Anforderungen lediglich für die Phasen der Erhebung, Speicherung, Nutzung und Übermittlung birgt die Gefahr solcher Lücken. Verschärft wird die Problematik dadurch, dass die Begriffe seit der Anpassung des Landesdatenschutzgesetzes an die EU-Datenschutzreform nicht mehr legaldefiniert sind.

Eine **Regelungslücke** ist bereits absehbar im Hinblick auf den **Schutz besonderer Kategorien personenbezogener Daten**. Für diese Daten gelten nach Art. 10 der JI-Richtlinie besondere Bedingungen, die für alle Phasen der Verarbeitung vorzusehen sind. Im vorliegenden Entwurf werden diese besonderen Bedingungen jedoch nur für einzelne Phasen der Verarbeitung geregelt, nämlich für die Erhebung (§ 48 Abs. 2 ResOG SH-E), die Speicherung und Nutzung (§ 52 Abs. 1 Satz 2 ResOG SH-E) und die Übermittlung (§ 53 Abs. 1 Satz 2 ResOG SH-E, § 56 Abs. 1 Satz 4 ResOG SH-E). Der Umgang mit diesen Daten **sollte zusammengefasst im Unterabschnitt 1 für die gesamte Verarbeitung geregelt** werden. Dabei sollten auch die **Garantien für die Rechte und Freiheiten der betroffenen Personen** näher ausgestaltet werden, wie dies z.B. in § 24 Abs. 2 und 3 LDSG erfolgt ist.

§ 46 ResOG SH-E

Die hier als Umsetzung der JI-Richtlinie geregelte **Einwilligung** der betroffenen Person ist in der Richtlinie **ausdrücklich nicht als alleinige Rechtsgrundlage** für die Verarbeitung personenbezogener Daten vorgesehen. Erwägungsgrund 35 der JI-Richtlinie führt hierzu Folgendes aus:

„Die Verarbeitung personenbezogener Daten im Rahmen dieser Richtlinie sollte nur dann als rechtmäßig gelten, wenn sie zur Wahrnehmung einer Aufgabe erforderlich ist, die eine zuständige Behörde im öffentlichen Interesse auf Grundlage des Unionsrechts oder des Rechts der Mitgliedstaaten 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, ausführt. Diese Tätigkeiten sollten sich auf die Wahrung lebenswichtiger Interessen der betroffenen Person erstrecken. Bei der Wahrnehmung der ihnen als gesetzlich begründeter Institution übertragenen Aufgaben, Straftaten zu verhüten, zu ermitteln, aufzudecken und zu verfolgen, können die zuständigen Behörden natürliche Personen auffordern oder anweisen, ihren Anordnungen nachzukommen. ***In einem solchen Fall sollte die Einwilligung der betroffenen Person im Sinne der Verordnung (EU) 2016/679 keine rechtliche Grundlage für die Verarbeitung personenbezogener Daten durch die zuständigen Behörden darstellen.*** *Wird die betroffene Person aufgefordert, einer rechtlichen Verpflichtung nachzukommen, so hat sie keine echte Wahlfreiheit, weshalb ihre Reaktion nicht als freiwillig abgegebene Willensbekundung betrachtet werden kann. Dies sollte die Mitgliedstaaten nicht daran hindern, 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."*

Bezüglich der **Regelung der Möglichkeit einer Einwilligung** als alleinige Rechtsgrundlage für die Verarbeitung personenbezogener Daten sollte der Gesetzentwurf **geändert** werden, um die Anforderungen des europäischen Datenschutzrechts umzusetzen. Würde dagegen meine Empfehlung aufgegriffen, die Datenschutz-Grundverordnung für alle Adressaten anzuwenden, wäre damit auch die Frage der Einwilligung gelöst. Die Datenschutz-Grundverordnung sieht die Einwilligung der betroffenen Person als Grundlage für die Verarbeitung personenbezogener Daten vor.

§ 51 ResOG SH-E

Absatz 1 sollte sprachlich überarbeitet werden. Aus der Begründung ergibt sich, dass die Daten über andere Personen als Verletzte oder Probandinnen und Probanden bei den Probandinnen und Probanden erhoben werden dürfen. Um dies deutlicher zum Ausdruck zu bringen, sollte in Absatz 1 anstelle der Formulierung „bei diesen selbst" die **Formulierung „bei den Probandinnen und Probanden und den Verletzten" verwendet werden, sofern dies gemeint ist**.

§ 52 ResOG SH-E

Hier gelten die obigen Ausführungen zu den Begrifflichkeiten der Verarbeitung, Speicherung und Nutzung. Ich weise darauf hin, dass an dieser Stelle **Regelungslücken vor allem im Hinblick auf die Befugnisse der Leistungserbringenden** entstehen können. Ihnen werden durch § 52 ResOG SH-E Befugnisse, unter anderem zur zweckändernden Speicherung und Nutzung personenbezogener Daten, eingeräumt. Auf andere Phasen der Verarbeitung beziehen sich diese Befugnisse ausdrücklich nicht.

§ 52 Absatz 6 ResOG SH-E erlaubt die Nutzung von Protokolldaten unter anderem für die Verfolgung von Straftaten von erheblicher Bedeutung. Der ursprüngliche Zweck der Protokolldatenerhebung besteht in der Durchführung von Aufsichts- und Kontrollaufgaben sowie zur Gewährleistung der Datensicherheit und Datenintegrität. Diese Zwecke dienen internen Abläufen. **Die Ausweitung der Verarbeitung von Protokolldaten auch für andere Zwecke ist im Hinblick auf die Verhältnismäßigkeit des damit verbundenen Grundrechtseingriffs bedenklich.** Eine dem Grundsatz der Verhältnismäßigkeit entsprechende Verarbeitung für Strafverfahren kann allenfalls darin bestehen, dass die **Protokolldaten für die Verfolgung von Straftaten verwendet** werden, **für die sie auch**

erhoben worden sind. Dies kann beispielsweise die Verfolgung von missbräuchlichen Verarbeitungen personenbezogener Daten sein, die mit den Protokolldaten festgestellt und nachgewiesen werden kann. Dies sollte im Gesetz oder zumindest in der Begründung klargestellt werden.

§ 53 ResOG SH-E

Absatz 2

Absatz 2 ResOG SH-E regelt die Zulässigkeit von Übermittlungen für den Zweck, zu dem die Daten erhoben worden sind. Nummer 2 erlaubt in diesem Zusammenhang die Übermittlung von Daten, wenn der Empfänger ein rechtliches Interesse an der Kenntnis der Daten hat. Es ist **fraglich, ob das Interesse des Empfängers überhaupt noch unter den Zweck fallen kann, zu dem die Daten erhoben** worden sind. Denn offensichtlich benötigt die empfangende nichtöffentliche Stelle die Daten für eigene Interessen. Bei einer Übermittlung für den ursprünglichen Zweck müsste man eigentlich davon ausgehen können, dass die Übermittlung (zumindest auch) für die übermittelnde Stelle erforderlich ist, um ihre Aufgaben zu erfüllen. Dieser Fall ist bereits nach Nummer 1 erlaubt. Es sollte **daher geprüft werden, ob Nummer 2 zu streichen ist**.

Absatz 3

Mit der Einführung dieser Regelung ist eine gesetzgeberische **Entscheidung von erheblicher Tragweite** verbunden. Es soll erstmalig eine Übermittlung von Daten durch die Leistungserbringenden an andere Stellen für andere Zwecke zugelassen werden. Zu den Empfängern der Daten sollen unter anderem die Polizei und die Verfassungsschutzbehörden gehören. Nach geltendem Recht, § 12 Abs. 1 BGG, dürfen Bewährungshelferinnen und Bewährungshelfer personenbezogene Daten grundsätzlich nur zu dem Zweck verarbeiten, zu dem sie erhoben worden sind. Andere Verarbeitungen sind nur mit Einwilligung der betroffenen Personen zugelassen. Der Grund dieser sehr engen Regelung liegt darin, dass Bewährungshelferinnen und Bewährungshelfer in der Regel Berufsgeheimnisträger sind. Für eine erfolgreiche Arbeit mit den Probandinnen und Probanden sind sie auf ein Vertrauensverhältnis zu diesen angewiesen, das die Grundlage dafür schafft, die für Resozialisierungsmaßnahmen erforderlichen Informationen zu erhalten.

Die **Übermittlung von Daten der Probandinnen und Probanden durch Leistungserbringende für andere Zwecke an andere Stellen** gehört daher seit Jahren zu den **umstrittensten Fragen des Datenschutzes in der Bewährungshilfe**. Auf Bundesebene gab es in der Vergangenheit viele Gesetzesinitiativen zur Schaffung von gesetzlichen Grundlagen für solche Übermittlungen, die aufgrund von Befürchtungen für negative Auswirkungen auf das Vertrauensverhältnis zu den Probandinnen und Probanden gescheitert sind. Im Jahr 2017 sind nun jedoch mit § 481 Absatz 1 Satz 3 und § 487 Absatz 1 Satz 3 StPO zwei ausdrückliche Übermittlungsbefugnisse für Bewährungshelferinnen und Bewährungshelfer und Führungsaufsichtsstellen geregelt worden. Danach dürfen diese Stellen personenbezogene Daten zum Zweck der Gefahrenabwehr an die Polizei (§ 481 Abs. 1 Satz 3 StPO) und für vollzugliche Zwecke an die Einrichtungen des Justiz- und Maßregelvollzug (§ 487 Absatz 1 Satz 3 StPO) weitergeben.

Mit Einführung der neuen Regelung im vorliegenden Entwurf würden **die zweckändernden Übermittlungen durch die Leistungserbringenden nochmals erheblich ausgeweitet**. Übermittlungen sind nach Absatz 3 Nummer 2 z. B. an folgende Empfänger vorgesehen:

- an die Jugendämter
- an Ausländerbehörden
- an Sozialleistungsträger
- an Verfassungsschutzbehörden
- an Gefahrenabwehrbehörden

- an Strafverfolgungsbehörden zur Verhinderung oder Verfolgung von Straftaten
- an Strafvollstreckungsbehörden

Aus welchem Grund diese Übermittlungen erforderlich sind, geht aus dem Entwurf nicht hervor. Die oben genannten Änderungen im Bundesrecht waren politisch umstritten und können als Ergebnis eines jahrelangen Prozesses angesehen werden, in dem über das **Erfordernis der Übermittlung einerseits und die Vertraulichkeitserwartung an den Leistungserbringenden als Grundlage für seine Tätigkeit anderseits** öffentlich diskutiert wurde. Der vorliegende Gesetzentwurf, der den Kreis der Empfängerbehörden nun erheblich erweitert, ohne die Erforderlichkeit für solche Übermittlungen auch nur im Ansatz zu begründen, kann für den Gesetzgeber keine Grundlage sein, solche Grundrechtseingriffe vorzunehmen. Daher rege an, **von der datenschutzrechtlich problematischen Erweiterung des Empfängerkreises Abstand zu nehmen** und diese Regelungen zu **streichen**.

§ 56 ResOG SH-E

Diese Vorschrift regelt die **Zulässigkeit von Fallkonferenzen** und den Austausch personenbezogener Daten zwischen den beteiligten Stellen im Rahmen solcher Konferenzen. Im Gegensatz zu § 53 Absatz 3 ResOG SH-E ist diese Regelung **ausführlich begründet**. Auch sind die Voraussetzungen für eine Übermittlung personenbezogener Daten hier wesentlich bestimmter und enger gefasst. Die zu § 53 Absatz 3 ResOG SH-E geäußerten Bedenken gelten daher hier nicht in gleicher Weise.

In **Absatz 2 Nummer 1** sollte die Voraussetzung der „Gefährlichkeit für die Allgemeinheit" präzisiert werden. Sie erscheint **zu unbestimmt und weit, um die Verhältnismäßigkeit der Eingriffe in die Vertraulichkeit des Berufsgeheimnisses zu garantieren**. Soweit ersichtlich wird eine ähnliche Formulierung in den Vorschriften des Strafgesetzbuchs über die Sicherungsverwahrung verwendet. In § 66 Absatz 1 Nummer 4 StGB wird der Begriff der Gefährlichkeit für die Allgemeinheit jedoch wie folgt näher ausgeformt:

> *„4. die Gesamtwürdigung des Täters und seiner Taten ergibt, dass er infolge eines Hanges zu erheblichen Straftaten, namentlich zu solchen, durch welche die Opfer seelisch oder körperlich schwer geschädigt werden, zum Zeitpunkt der Verurteilung für die Allgemeinheit gefährlich ist."*

Eine ähnliche **Einschränkung fehlt** im vorliegenden Entwurf. Dies wäre zu ergänzen.

Hinsichtlich des Datenaustauschs mit den Verfassungsschutzbehörden in **Absatz 3** stellt sich die Frage, inwieweit eine Datenübermittlung durch den Leistungserbringenden an die Verfassungsschutzbehörden geeignet sein kann, Gefahren für die Resozialisierung der Probandin oder des Probanden abzuwehren. **Die Unterstützung von konkreten Maßnahmen der Gefahrenabwehr oder der Resozialisierung gehört nicht zu den Aufgaben der Verfassungsschutzbehörden**. Möglicherweise soll die Datenübermittlung an die Verfassungsschutzbehörden nur dazu dienen, Anfragen an diese Behörden zu stellen und dort vorhandene **Erkenntnisse abzufragen**. In diesem Fall sollte dies im Gesetz **klargestellt** werden.

§ 62 ResOG SH-E

Artikel 13 der JI-Richtlinie sieht vor, dass die in § 62 Abs. 1 ResOG SH-E genannten Informationen den betroffenen Personen in jedem Fall zur Verfügung zu stellen sind. In besonderen Fällen sieht Artikel 13 Abs. 2 der JI-Richtlinie vor, dass den betroffenen Personen weitergehende Informationen zur Verfügung zu stellen sind, u. a. die Rechtsgrundlage der Verarbeitung, die Dauer der Speicherung und Kategorien von Empfängern der Daten. Diese Informationen sind im vorliegenden Entwurf nach § 62 Abs. 2 ResOG SH-E ebenfalls für besondere Fälle vorgesehen. Nach meiner Auffassung dürfte es sich

bei den Fällen, die der vorliegende Entwurf regelt, in der Regel um besondere Fälle handeln. Die Verarbeitung hat in der Regel einen **sensiblen Lebenshintergrund**, und häufig dürfte sie auch **sensible Informationen über die betroffenen Personen** zum Gegenstand haben. Daher rege ich an, die Informationen nach Absatz 2 in den Katalog des Absatzes 1 zu integrieren, so dass sie **stets zur Verfügung gestellt werden** müssen.

Hierfür spricht auch der **Gedanke der Gleichbehandlung** mit nichtöffentlichen Leistungserbringenden. Denn diese sind nach Artikel 13 DSGVO stets und ohne Ausnahme verpflichtet, diese Informationen zur Verfügung zu stellen.

§ 63 ResOG SH-E

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 betroffenen Stellen 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**.

Für eine Erörterung meiner Stellungnahme und weitere Fragen stehen mein Team und ich gern zur Verfügung.

Mit freundlichen Grüßen

gez. Marit Hansen
Landesbeauftragte für Datenschutz