BREMISCHE BÜRGERSCHAFT
Landtag
21. Wahlperiode

Drucksache 21/1646
(Änderungsantrag zu Drs. 21/1616)
23. Februar 2026

Änderungsantrag der Fraktion der FDP

Änderungsantrag der Fraktion der FDP zur „Änderung des Bremischen Polizeigesetzes (BremPolG) und weiterer Gesetze (Drucksache 21/1616 Landtag).

Beschlussempfehlung:

Der Landtag möge beschließen: Das Gesetz zur Änderung polizei- und vollstreckungsrechtlicher Vorschriften“ wird wie folgt geändert:

Artikel 1 Änderung des Bremischen Polizeigesetzes wird wie folgt geändert:

1. Änderung des Inhaltsverzeichnisses

   a. Es wird eine neue Änderung b) eingeführt

      § 11 a Elektronische Aufenthaltsüberwachung

   b. Die bisherige Änderung zu b) „Nach der Angabe zu § 12 werden die folgenden Angaben eingefügt:“ wird zu Änderung c) (neu), die weiteren Änderungen verschieben sich entsprechend bis zu Änderung h (alt) / i (neu)

   c. Nach Änderung i (neu) wird eine neue Änderung j eingeführt
      „§ 51a Training und Testung von lernenden IT-Systemen“

   d. Die bisherige Änderung zu i (alt) wird zu Änderung k (neu), die weiteren Änderungen verschieben sich entsprechend bis zu Änderung u (alt) / v (neu)

2. § 9 wird wie folgt geändert:
   a. § 9 Abs. 2 wird gestrichen.
   b. § 9 Abs. 3 wird gestrichen.
   c. § 9 Abs. 4 Hs. 2 wird gestrichen.

3. Nach § 11 wird § 11 a neu eingefügt:

   § 11 a Elektronische Aufenthaltsüberwachung

   (1) Die Polizeibehörden können zur Verhütung von terroristischen Straftaten oder zur Gefahrenabwehr eine Person dazu verpflichten, ein technisches Mittel, mit dem der Aufenthaltsort dieser Person elektronisch überwacht werden kann, ständig in betriebsbereitem Zustand am Körper bei sich zu führen und dessen Funktionsfähigkeit nicht zu beeinträchtigen, wenn
   1. bestimmte Tatsachen die Annahme rechtfertigen, dass diese Person innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine terroristische Straftat begehen wird, oder

2. deren individuelles Verhalten eine konkrete Wahrscheinlichkeit dafür begründet, dass sie innerhalb eines übersehbaren Zeitraums eine terroristische Straftat begehen wird, oder
3. im Einzelfall bestimmte Tatsachen die Annahme rechtfertigen, dass diese Person innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise Leben, Leib oder Freiheit einer Person erheblich gefährden oder eine Straftat gegen die sexuelle Selbstbestimmung, die im Mindestmaß mit wenigstens drei Monaten Freiheitsstrafe bedroht ist, begehen wird,
4. die Person, der gegenüber die Anordnung nach Absatz 1 getroffen werden soll, nach polizeilichen Erkenntnissen bereits eine Straftat nach § 238 des Strafgesetzbuchs begangen hat und bestimmte Tatsachen die Annahme rechtfertigen, dass sie weitere Straftaten nach § 238 des Strafgesetzbuchs begehen wird, um diese Person durch die Überwachung und die Datenverarbeitung von der Begehung terroristischer Straftaten abzuhalten oder die Effektivität der Gefahrenabwehr zu steigern. Die Verpflichtung nach Satz 1 umfasst auch die Verpflichtung, ein zur Verfügung gestelltes Mobiltelefon ständig in betriebsbereitem Zustand bei sich zu führen und dessen Funktionsfähigkeit nicht zu beeinträchtigen.

(2) Die Polizeibehörden können der Person, deren Aufenthaltsort nach Abs. 1 elektronisch überwacht werden darf, aufgeben,
1. einen bestimmten Bereich nicht ohne Erlaubnis der Polizeibehörde zu verlassen,
2. sich nicht an bestimmten Orten aufzuhalten, die ihr Gelegenheit oder Anreiz zu Straftatenbieten können,
3. den Kontakt mit bestimmten Personen oder Personen einer bestimmten Gruppe zu unterlassen.
Die Maßnahmen nach Satz 1 sind zeitlich und örtlich auf den zur Verhütung der Straftat erforderlichen Umfang zu beschränken und sind auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils bis zu drei Monate ist möglich, soweit die Voraussetzungen der Maßnahme fortbestehen. Die Vorschriften des Versammlungsrechts bleiben unberührt.

(3) Die Maßnahme nach Abs. 1 und die Verlängerung der Maßnahmen nach Abs. 2 dürfen nur aufgrund richterlicher Anordnung auf Antrag der Behördenleitung getroffen werden. Bei Gefahr im Verzug kann die Anordnung nach Satz 1 durch eine von der Behördenleitung beauftragte Person getroffen werden. In diesem Fall ist die richterliche Anordnung unverzüglich nachzuholen. Die Anordnung ist auf höchstens vier Monate zu befristen. Eine Verlängerung um jeweils bis zu vier Monate ist möglich, soweit die Anordnungsvoraussetzungen fortbestehen. Liegen die Voraussetzungen nicht mehr vor, ist die Maßnahme unverzüglich zu beenden. Zuständig ist das Amtsgericht, in dessen Bezirk die Polizeibehörde ihren Sitz hat. Für das Verfahren gelten die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend.

(4) Die Anordnung nach Abs. 3 ergeht schriftlich. In ihr sind anzugeben
1. die Person, gegen die sich die Maßnahme richtet mit Name und Anschrift,
2. Art, Umfang und Dauer der Maßnahme,
3. im Falle der Aufenthaltsvorgabe nach Abs. 2 Satz 1 Nr. 1 oder 2 die Bezeichnung der Orte, von denen sich die Person ohne Erlaubnis der Polizeibehörde nicht entfernen oder an denen sich die Person ohne Erlaubnis der Polizeibehörde nicht aufhalten darf,
4. im Falle des Kontaktverbots nach Abs. 2 Satz 1 Nr. 3 die Personen oder die Gruppe, mit denen oder mit der der betroffenen Person der Kontakt untersagt ist, soweit möglich, mit Name und Anschrift,
5. die wesentlichen Gründe.

(5) Die Polizeibehörden können mithilfe der von der betroffenen Person mitgeführten technischen Mittel automatisiert Daten über deren Aufenthaltsort sowie über etwaige Beeinträchtigungen der Datenerhebung verarbeiten. Soweit dies zur Erfüllung des

Überwachungszwecks erforderlich ist, dürfen die erhobenen Daten aufgrund richterlicher Anordnung zu einem Bewegungsbild verbunden werden. Durch Rechtsverordnung des Senators für Inneres und Sport kann bestimmt werden, dass eine andere öffentliche Stelle als die Polizeibehörde die in Satz 1 genannten Daten verarbeitet. Die Polizeibehörden können mit Einwilligung einer Person, zu deren Schutz gegenüber der betroffenen Person eine Anordnung nach Abs. 2 oder § 1 des Gewaltschutzgesetzes besteht, Daten über deren Aufenthaltsort durch ein von dieser mitzuführendes technisches Mittel automatisiert verarbeiten und mit den nach Abs. 1 Satz 1 erhobenen Daten automatisiert abgleichen. Soweit es technisch möglich ist, ist sicherzustellen, dass innerhalb der Wohnung der Person keine über den Umstand ihrer Anwesenheit hinausgehenden Aufenthaltsdaten erhoben werden. Die Daten dürfen ohne Einwilligung der betroffenen Person nur verarbeitet werden, soweit dies erforderlich ist für folgende Zwecke:
1. zur Verhütung zu erwartender Straftaten sowie zur Verfolgung von Straftaten im Sinne des Abs. 1 Satz 1 Nr. 1 und 2,
2. zur Abwehr einer Gefahr für Leib, Leben, Freiheit oder sexuelle Selbstbestimmung einer Person im Sinne des Abs. 1 Satz 1 Nr. 3,
3. zur Feststellung von Verstößen gegen Maßnahmen nach Abs. 2 oder § 1 des Gewaltschutzgesetzes,
4. zur Abwehr einer erheblichen gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer dritten Person oder
5. zur Aufrechterhaltung der Funktionsfähigkeit der technischen Mittel. Zur Einhaltung der Zweckbindung nach Satz 4 hat die Verarbeitung der Daten automatisiert zu erfolgen und es sind die Daten gegen unbefugte Kenntnisnahme besonders zu sichern. Die in Satz 1 genannten Daten sind spätestens zwei Monate nach ihrer Erhebung zu löschen,
soweit sie nicht für die in Satz 4 genannten Zwecke verarbeitet werden. Jeder Abruf der Daten ist zu protokollieren. Die Protokolldaten sind nach zwölf Monaten zu löschen. Werden innerhalb der Wohnung der betroffenen Person über den Umstand ihrer Anwesenheit hinausgehende Aufenthaltsdaten erhoben, dürfen diese nicht verwendet werden und sind unverzüglich nach Kenntnisnahme zu löschen. Die Tatsache ihrer Kenntnisnahme und Löschung ist zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist nach Abschluss der Datenschutzkontrolle zu löschen.

4. § 18 Abs. 3 wird wie folgt geändert:

   a. 1. Satz 1 wird wie folgt geändert:
   Betrifft die Durchsuchung ein elektronisches Speichermedium, können in den Fällen des § 17 Absatz 1 Satz 1 Nummer 1 bis 3 auch vom Durchsuchungsobjekt räumlich getrennte Speichermedien durchsucht werden, soweit die von der Durchsuchung betroffene Person von diesem aus auf sie zugreifen kann, eine konkrete Gefahr vorliegt und wenn dies im Hinblick auf den Zweck der Durchsuchung erforderlich und angemessen ist.

   b. Es wird ein neuer Satz 6 eingefügt:
   „Für die Durchsuchung von Speichermedien, die sich örtlich innerhalb von Wohnungen befinden, sind die Voraussetzungen der §§ 19 und 20bBremPolG entsprechend zu erfüklken.

5. § 27 wird wie folgt geändert:

   Abs. 1 Satz 2 wird gestrichen

6. § 44 wird wie folgt geändert:

a. Absatz 1 Satz 1 wird durch den folgenden Satz ersetzt:
„Der Polizeivollzugsdienst darf Auskunft verlangen über
1. Bestandsdaten gemäß § 3 Nummer 6 des Telekommunikationsgesetzes und über die nach § 172 des Telekommunikationsgesetzes erhobenen Daten von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, und
2. Bestandsdaten gemäß § 2 Absatz 2 Nummer 2 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes von demjenigen, der geschäftsmäßig eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt.“

b. Die Maßnahme darf nur durch das Gericht oder, soweit die zu erhebenden Daten zur Abwehr einer Gefahr für die öffentliche Sicherheit im Einzelfall erforderlich sind, durch den Behördenleiter oder die Behördenleiterin oder die jeweilige Vertretung angeordnet werden; in diesem Fall ist unverzüglich eine richterliche Bestätigung einzuholen.

c. In Absatz 2 Satz 2 wird die Angabe „des Telekommunikation-Telemedien- Datenschutz-Gesetz“ durch die Angabe „des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes“ ersetzt.

d. In Absatz 3 Satz 2 wird die Angabe „des Telekommunikation-Telemedien- Datenschutz-Gesetzes“ durch die Angabe „des Telekommunikation- Digitale-Dienste-Datenschutz-Gesetzes“ ersetzt.

7. § 49 Absatz 3 Satz 1 wird durch den folgenden Satz ersetzt:

„Eine Maßnahme nach Absatz 1 darf nur durch ein Gericht oder, soweit die es zur Abwehr einer Gefahr für die öffentliche Sicherheit im Einzelfall erforderlich ist, durch die Behördenleitung mit Zustimmung der Senatorin oder des Senators für Inneres und Sport angeordnet werden.“

8. Es wird ein neuer § 51a eingeführt:

§ 51a Training und Testung von lernenden IT-Systemen

(1) Die Polizei darf zum Trainieren und Testen von lernenden IT-Systemen, die die Polizei für die eigene Aufgabenwahrnehmung entwickelt oder nutzt, soweit erforderlich bei ihr vorhandene personenbezogene Daten nach Maßgabe der Absätze 2 bis 5 weiterverarbeiten und dafür auch an Dritte oder Auftragsverarbeiter übermitteln. Es ist dabei sicherzustellen, dass diskriminierende Algorithmen weder herausgebildet noch verwendet werden. Soweit wie technisch möglich muss die Nachvollziehbarkeit des verwendeten Verfahrens sichergestellt werden. Die Weiterverarbeitung von personenbezogenen Daten, die durch einen verdeckten Einsatz technischer Mittel in oder aus Wohnungen, durch Überwachung und Aufzeichnung von Telekommunikation oder durch den verdeckten Einsatz technischer Mittel aus vom Betroffenen genutzten informationstechnischen Systeme n erhoben wurden, ist unzulässig.

(2) Personenbezogene Daten sind für die Verwendung zu Test- oder Trainingszwecken zu anonymisieren. Kann der Zweck des Tests oder Trainings mit anonymisierten Daten nicht erreicht werden oder ist die Anonymisierung nur mit unverhältnismäßigem Aufwand möglich, sind sie zu pseudonymisieren. Kann der Zweck des Tests oder Trainings mit pseudonymisierten Daten nicht erreicht werden oder ist die Pseudonymisierung nur mit unverhältnismäßigem Aufwand möglich, dürfen personenbezogene Daten zum Zweck des Tests oder Trainings verarbeitet werden. Besondere Kategorien personenbezogener Daten nach Artikel 10 der Richtlinie (EU) 2016/680 oder Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 dürfen unter Gewährleistung von Garantien im Sinne des § 4 Absatz 2 zum Zweck des Tests oder Trainings verwendet werden.

(3) Personenbezogene Daten dürfen zum Testen und Trainieren von lernenden Systemen nur an Auftragsverarbeiter übermittelt werden, wenn eine Verarbeitung bei der Polizei selber nur mit unverhältnismäßigem Aufwand möglich ist. An Dritte dürfen die Daten nur übermittelt werden, wenn eine Verarbeitung durch die Polizei auch unter Zuhilfenahme eines Auftragsverarbeiters nur mit unverhältnismäßigem Aufwand möglich ist. Sofern personenbezogene Daten zum Testen oder Trainieren von lernenden IT-Systemen an Dritte oder im Wege der Auftragsverarbeitung übermittelt werden, ist die Übermittlung von personenbezogenen Daten, die durch einen verdeckten Einsatz technischer Mittel in oder aus Wohnungen nach durch Überwachung und Aufzeichnung von Telekommunikation oder durch den verdeckten Einsatz technischer Mittel aus vom Betroffenen genutzten informationstechnischen Systemen erhoben wurden, unzulässig. Personenbezogene Daten dürfen nur an solche Personen übermittelt werden, die Amtsträger oder für den öffentlichen Dienst besonders Verpflichtete sind oder die zur Geheimhaltung verpflichtet worden sind. § 1 Absätze 2 und 3 sowie Absatz 4 Nummer 2 des Verpflichtungsgesetzes vom 2. März 1974 (BGBl. I S. 469, 547), geändert am 15. August 1974 (BGBl. I S. 1942), ist auf die Verpflichtung zur Geheimhaltung entsprechend anzuwenden. Durch organisatorische und technische Maßnahmen ist zu gewährleisten, dass die Daten gegen unbefugte Kenntnisnahme geschützt sind.

(4) Auftrags- und Drittverarbeiter dürfen die übermittelten Daten nur im Rahmen des jeweiligen Trainings und der jeweiligen Tests verarbeiten. Sie sind verpflichtet, die Daten nach Abschluss von Training und Testung des lernenden Systems wieder zu löschen. Sie dürfen die trainierten Modelle für eigene Zwecke weiternutzen, wenn die Polizei dies genehmigt und sichergestellt werden kann, dass aus den trainierten Modellen keine Trainingsdaten abgeleitet werden können.

(5) Für das Testen oder Trainieren von lernenden IT-Systemen wird in einer nach Anhörung durch den Beauftragten für Datenschutz und Informationsfreiheit zu veröffentlichenden und erlassenden Verwaltungsvorschrift das Nähere zu dem Verfahren, den Sicherungsmaßnahmen zur Verhinderung unbefugter Datenzugriffe sowie zu Art und Umfang der verarbeitenden Daten bestimmt. In der Verwaltungsvorschrift nach Satz 1 ist insbesondere zu bestimmen:

1. die Art der zu verarbeitenden Daten,
2. der Personenkreis, der von der Verarbeitung betroffen ist,
3. die Entscheidungsträger und das Verfahren, die die Einhaltung der maßgeblichen fachlichen und rechtlichen Anforderungen an das Training und die Testung von lernenden IT-Systemen sicherstellen,
4. Sicherungsmaßnahmen zur Datenaktualität und -qualität,
5. die Mindeststandards zur technischen Durchführung der Anonymisierung und Pseudonymisierung von Daten sowie die Beschreibung eines etwaigen unverhältnismäßigen Aufwands im Sinne von Absatz 2 Sätze 2 und 3 und Absatz 3 Sätze 1 und 2,
6. die Lösch- und Protokollierungspflichten.

9. § 150 wird wie folgt geändert:

   In § 150 Abs 1 S. 1 wird der Passus „sowie zur Anwendung des § 27 Absatz 1 Satz 2“ gestrichen.

Dr. Marcel Schröder, Thore Schäck und FDP-Fraktion