THÜRINGER LANDTAG
5. Wahlperiode

Drucksache 5/6118
21.05.2013

G e s e t z e n t w u r f

der Landesregierung

Thüringer Gesetz zur Änderung des Polizeiaufgabengesetzes und des Ordnungsbehördengesetzes

A. Problem und Regelungsbedürfnis

Zum Polizeiaufgabengesetz

Die Koalitionsvereinbarung zwischen CDU und SPD sieht eine Novellierung des Polizeiaufgabengesetzes in der laufenden Legislaturperiode vor. Auf Seite 47 ist ausgeführt: "Das Polizeiaufgabengesetz wird novelliert, dabei wird insbesondere auf den unantastbaren Schutz des Kernbereichs geachtet. Gemeinsam mit Betroffenen sollen die Möglichkeiten eines besseren Schutzes von Berufsgeheimnisträgern besprochen und unter Berücksichtigung der Rechtsprechung überarbeitet werden."

Der Thüringer Verfassungsgerichtshof hat am 21. November 2012 das Urteil in der Verfassungsstreitsache 19/09 verkündet, die die Beschwerde dreier Rechtsanwälte gegen das Polizeiaufgabengesetz zum Gegenstand hatte. Die Beschwerde richtete sich gegen die im Jahr 2008 novellierten Normen der verdeckten Datenerhebung, der Überwachung der Telekommunikation und der Wohnraumüberwachung sowie gegen die Regelungen zum Schutz der Berufsgeheimnisträger vor polizeilicher Datenerhebung. Das Gericht hat Teile des Gesetzes für verfassungswidrig erklärt und dem Gesetzgeber eine Frist zur Änderung bis zum 30. September 2013 eingeräumt.

Weiterer Anpassungsbedarf ergibt sich aus dem Beschluss des Bundesverfassungsgerichts vom 24. Januar 2012, 1 BvR 1299/05 (Bestandsdatenspeicherung). Mit diesem Beschluss wurde die bisherige Ausgestaltung des Zugriffs der Sicherheitsbehörden auf Bestandsdaten nach § 113 des Telekommunikationsgesetzes für teilweise verfassungswidrig erklärt. Nach dem vom Bundesverfassungsgericht vorgegebenen "Doppeltürmodell" sind Anpassungen sowohl im Bundesrecht als auch im Landesrecht notwendig.

Darüber hinaus sollen mit dem Gesetz folgende europäische Beschlüsse auf Landesebene umgesetzt werden:

1. Beschluss 2008/615/JI des Rates vom 23. Juni 2008 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität (ABl. L 210 vom 6. August 2008, S. 1) - Ratsbeschluss Prüm,

Vorabdruck verteilt am: 21. Mai 2012

Druck: Thüringer Landtag, 19. Juni 2013

2. Rahmenbeschluss 2006/960/JI des Rates vom 18. Dezember 2006 über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union (ABl. L 386 vom 29. Dezember 2006, S. 89, L 75 vom 15. März 2007, S. 26) - Schwedische Initiative,
3. Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (ABl. L 350 vom 30. Dezember 2008, S. 60) - Rahmenbeschluss Datenschutz.

Zum Ordnungsbehördengesetz

Das Thüringer Oberverwaltungsgericht hat mit Urteil vom 21. Juni 2012, Az: 3 N 653/09, den § 8a Abs. 2 der Erfurter Stadtordnung für unwirksam erklärt. Durch diese im Jahre 2008 in die Stadtordnung eingefügte Bestimmung wird in Teilen der Erfurter Altstadt das mit dem Verzehr von Alkohol verbundene Lagern von Personengruppen oder längere Verweilen einzelner Personen untersagt. Nach Auffassung des Gerichts kann der Erlass einer solchen Verbotsregelung nicht auf § 27 Abs. 1 des Ordnungsbehördengesetzes (OBG) gestützt werden, denn durch das Trinken von Alkohol in der Öffentlichkeit entstehe keine allgemeine Gefahrenlage, die allein eine solche Regelung rechtfertigen könnte. Durch die Verordnung der Stadt Erfurt werde eine Maßnahme der Gefahrenvorsorge ergriffen, die durch die allgemeine Regelung des § 27 Abs. 1 OBG nicht erlaubt sei. Dafür bedürfe es einer speziellen landesgesetzlichen Regelung.

Wegen dieses Urteils besteht aus Sicht der Gemeinden ein dringender gesetzlicher Handlungsbedarf, denn für ihre Einwohner und Gäste stellt das alkoholbedingte Niederlassen und Verweilen von einzelnen Personen oder Personengruppen in öffentlichen Anlagen und auf öffentlichen Verkehrsflächen ein ständiges Ärgernis dar, wenn es dabei zu alkoholbedingten Straftaten und Ordnungswidrigkeiten, wie zum Beispiel Verunreinigungen und ruhestörendem Lärm, kommt.

B. Lösung

Unverzügliche Novellierung des Polizeiaufgabengesetzes

Nach § 27 OBG wird ein neuer § 27a eingefügt, der Ordnungsbehörden ermächtigt, den Aufenthalt zum Zwecke des Alkoholgenusses in bestimmten Bereichen der Gemeinden aus Gründen des Jugend- und Gesundheitsschutzes sowie zur Verhinderung von alkoholbedingten Straftaten und Ordnungswidrigkeiten zu verbieten.

C. Alternativen

keine

D. Kosten

Durch das Gesetz entsteht in geringfügigem Umfang ein nicht näher bezifferbarer Verwaltungsmehraufwand bei der Polizei und den Gerichten, da die Richtervorbehalte für verschiedene Maßnahmen ausgeweitet werden.

Im Übrigen entstehen keine Mehrkosten.

E. Zuständigkeit

Federführend ist das Innenministerium.

FREISTAAT THÜRINGEN
DIE MINISTERPRÄSIDENTIN

An die
Präsidentin des Thüringer Landtags
Frau Birgit Diezel
Jürgen-Fuchs-Straße 1

99096 Erfurt

Erfurt, den 21. Mai 2013

Sehr geehrte Frau Präsidentin,

hiermit überreiche ich den von der Landesregierung beschlossenen Entwurf des

> "Thüringer Gesetzes zur Änderung des Polizeiaufgabengesetzes und des Ordnungsbehördengesetzes"

mit der Bitte um Beratung durch den Landtag in den Plenarsitzungen am 24. Mai 2013.

Mit freundlichen Grüßen

Christine Lieberknecht

Thüringer Gesetz zur Änderung des Polizeiaufgabengesetzes und des Ordnungsbehördengesetzes

Der Landtag hat das folgende Gesetz beschlossen:

Artikel 1 Änderung des Polizeiaufgabengesetzes

Das Polizeiaufgabengesetz vom 4. Juni 1992 (GVBl. S. 199), zuletzt geändert durch Artikel 2 des Gesetzes vom 25. Oktober 2011 (GVBl. S. 268), wird wie folgt geändert:

1. § 5 wird wie folgt geändert:

   a) In der Überschrift werden das Komma nach dem Wort "Mittel" und das Wort "Beweisverbote" gestrichen.

   b) Die Absätze 3 bis 7 werden aufgehoben.

2. § 19 Abs. 1 Nr. 2 Buchst. c erhält folgende Fassung:

   "c) sie bereits in der Vergangenheit aus vergleichbarem Anlass bei der Begehung von Straftaten oder von Ordnungswidrigkeiten von erheblicher Bedeutung angetroffen worden ist und nach den Umständen eine Wiederholung dieser Verhaltensweise zu erwarten ist, oder"

3. § 31 Abs. 5 und 6 wird aufgehoben.

4. Die §§ 34 bis 34 b erhalten folgende Fassung:

"§ 34
Besondere Mittel der Datenerhebung

(1) Die Polizei kann zur Abwehr einer Gefahr für den Bestand oder die Sicherheit der Bundesrepublik Deutschland oder eines Landes, für Leben, Gesundheit oder Freiheit einer Person oder zur Abwehr einer gemeinen Gefahr für Sachen
1. über die für die Gefahr Verantwortlichen oder
2. über Personen, bei denen Tatsachen die Annahme rechtfertigen, dass sie für die für die Gefahr Verantwortlichen bestimmte oder von diesen herrührende Mitteilungen entgegennehmen oder weitergeben,

Daten durch den Einsatz von besonderen Mitteln nach Absatz 2 erheben. Die Anordnung der Maßnahme ist unzulässig, wenn tatsächliche Anhaltspunkte für die Annahme vorliegen, dass durch die Maßnahme allein Kenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden. Die Anordnung der Maßnahme nach Satz 1 Nr. 2 ist unzulässig, wenn die Person das Recht zur Verweigerung der Aussage nach den §§ 53 oder 53a StPO hätte. Die Datenerhebung darf auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden.

(2) Besondere Mittel der Datenerhebung sind
1. die planmäßig angelegte Beobachtung einer Person, die durchgehend länger als 24 Stunden oder an mehr als zwei Tagen durchgeführt werden soll (längerfristige Observation),

2. der verdeckte Einsatz technischer Mittel
   a) zur Ermittlung des Aufenthaltsorts einer Person,
   b) zur Anfertigung von Bildaufzeichnungen,
   c) zum Abhören oder zur Aufzeichnung des nicht öffentlich gesprochenen Wortes,
3. der Einsatz von Polizeibeamten unter einer Legende (verdeckte Ermittler),
4. der Einsatz sonstiger nicht offen ermittelnder Polizeibeamter und
5. der Einsatz von Personen, deren Zusammenarbeit mit der Polizei Dritten nicht bekannt ist (Vertrauenspersonen).

(3) Wird im Verlauf einer Maßnahme nach Absatz 2 Nr. 1 oder 2 Buchst. b oder c erkennbar, dass Inhalte erfasst werden, die
1. dem Kernbereich privater Lebensgestaltung zuzuordnen sind,
2. einem Geistlichen oder seinem Berufshelfer in der Eigenschaft als Seelsorger anvertraut werden oder
3. einem Vertrauensverhältnis zu einem Berufsgeheimnisträger oder Berufshelfer (§§ 53 oder 53a StPO) zuzuordnen sind und kein unmittelbarer Bezug zu den in Absatz 1 genannten Gefahren besteht,

sind die unmittelbare Kenntnisnahme und die Aufzeichnungen unverzüglich und so lange wie erforderlich zu unterbrechen. Angefertigte Aufzeichnungen sind zu löschen. Bestehen über die Voraussetzungen einer Unterbrechung Zweifel, ist nur die unmittelbare Kenntnisnahme entsprechend Satz 1 zu unterbrechen. In diesem Fall ist nur die Fortsetzung automatisierter Aufzeichnungen zulässig. Diese sind unverzüglich dem Richter zur Entscheidung über die Verwendbarkeit oder Löschung der Daten vorzulegen. Ist die Aufzeichnung oder die unmittelbare Kenntnisnahme unterbrochen worden, so darf sie nur fortgesetzt werden, wenn aufgrund tatsächlicher Anhaltspunkte nicht mehr zu erwarten ist, dass der Kernbereich privater Lebensgestaltung oder ein geschütztes Vertrauensverhältnis verletzt wird. Die Tatsache der Erlangung und die Löschung der Daten sind zu protokollieren.

(4) Der Einsatz von besonderen Mitteln nach Absatz 2 Nr. 1, 2 Buchst. c und Nr. 3 darf nur auf Antrag des Leiters der Landespolizeidirektion oder des Leiters des Landeskriminalamts oder eines von diesen besonders beauftragten Beamten des höheren Polizeivollzugsdienstes durch den Richter angeordnet werden. Bei Gefahr im Verzug dürfen die in Satz 1 genannten Personen die Maßnahme anordnen; die richterliche Entscheidung ist in diesem Fall unverzüglich nachzuholen. Die Anordnung nach Satz 2 Halbsatz 1 tritt außer Kraft, wenn sie nicht binnen drei Werktagen durch den Richter bestätigt wird. Die Anordnung hat schriftlich unter Angabe der für sie maßgeblichen Gründe zu erfolgen und ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als drei weitere Monate ist zulässig, soweit die Voraussetzungen unter Berücksichtigung der gewonnenen Erkenntnisse fortbestehen.

(5) Der Einsatz von besonderen Mitteln nach Absatz 2 Nr. 2 Buchst. a und b sowie Nr. 4 und 5 darf nur durch den Leiter der Landespolizeidirektion oder den Leiter

des Landeskriminalamts oder einen von diesen besonders beauftragten Beamten des höheren Polizeivollzugsdienstes angeordnet werden. Absatz 4 Satz 4 und 5 gilt entsprechend.

(6) Soweit es für den Aufbau und zur Aufrechterhaltung der Legende eines verdeckten Ermittlers erforderlich ist, dürfen entsprechende Urkunden hergestellt, verändert oder gebraucht werden. Ein verdeckter Ermittler darf zur Erfüllung seines Auftrags unter der Legende am Rechtsverkehr teilnehmen. Er darf ferner unter der Legende mit Einverständnis des Berechtigten dessen Wohnung betreten. Im Übrigen richten sich die Befugnisse eines verdeckten Ermittlers nach den Bestimmungen dieses Gesetzes.

§ 34 a
Überwachung der Telekommunikation

(1) Die Polizei kann zur Abwehr einer Gefahr für den Bestand oder die Sicherheit der Bundesrepublik Deutschland oder eines Landes, für Leben, Gesundheit oder Freiheit einer Person oder zur Abwehr einer gemeinen Gefahr für Sachen die Telekommunikation
1. der für die Gefahr Verantwortlichen,
2. von Personen, bei denen Tatsachen die Annahme rechtfertigen, dass sie für die für die Gefahr Verantwortlichen bestimmte oder von diesen herrührende Mitteilungen entgegennehmen oder weitergeben oder
3. von Personen, soweit Tatsachen die Annahme rechtfertigen, dass die für die Gefahr Verantwortlichen ihre Kommunikationseinrichtungen benutzen werden,

überwachen und aufzeichnen und die innerhalb des Telekommunikationsnetzes in Datenspeichern abgelegten Inhalte erheben. Die Maßnahme ist nur zulässig, wenn die Abwehr der Gefahr auf andere Weise aussichtslos oder wesentlich erschwert wäre. Die Anordnung der Maßnahme ist unzulässig, wenn tatsächliche Anhaltspunkte für die Annahme vorliegen, dass durch die Maßnahme allein Kenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden. Die Anordnung der Maßnahme nach Satz 1 Nr. 2 und 3 ist unzulässig, wenn die Person das Recht zur Verweigerung des Zeugnisses nach den §§ 53 oder 53a StPO hätte. Die Maßnahme darf auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden.

(2) Die Überwachung und Aufzeichnung der Telekommunikation kann auch in der Weise erfolgen, dass mit informationstechnischen Programmen in vom Betroffenen genutzte informationstechnische Systeme eingegriffen wird, wenn
1. durch technische Maßnahmen sichergestellt ist, dass ausschließlich eine laufende Telekommunikation überwacht und aufgezeichnet wird und
2. der Eingriff in das informationstechnische System notwendig ist, um die Überwachung und Aufzeichnung der Telekommunikation in unverschlüsselter Form zu ermöglichen.

Ein Zugriff auf die auf dem System gespeicherten Daten sowie alle anderen auf dem informationstechnischen System integrierten technischen Systemkomponenten ist unzulässig.

(3) Bei einer Maßnahme nach Absatz 2 ist technisch sicherzustellen, dass
1. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Erfassung und Ausleitung von Sprachsignalen am Audiosystem unerlässlich sind und
2. die vorgenommenen Veränderungen bei Beendigung der Maßnahme, soweit technisch möglich, automatisiert rückgängig gemacht werden.

Das eingesetzte Programm ist nach dem Stand der Wissenschaft und Technik gegen unbefugte Nutzung zu schützen. Die überwachte und aufgezeichnete Telekommunikation ist nach dem Stand der Wissenschaft und Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen. Zum Zwecke der Datenschutzkontrolle sind
1. die Bezeichnung der technischen Erfassungsanlage, der Ort und der Zeitpunkt des Einsatzes,
2. die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen,
3. die Angaben, die die Feststellung der erhobenen Daten ermöglichen und
4. die Organisationseinheit, die die Maßnahme durchführt,

zu protokollieren. Die Protokolldaten dürfen nur verwendet werden, um dem Betroffenen oder einer dazu befugten öffentlichen Stelle die Prüfung zu ermöglichen, ob die Maßnahme rechtmäßig durchgeführt worden ist. Sie sind bis zum Ablauf des auf die Speicherung folgenden Kalenderjahres aufzubewahren und sodann zu löschen, es sei denn, dass sie für den in Satz 5 genannten Zweck erforderlich sind.

(4) Erfolgt im Rahmen von Maßnahmen nach den Absätzen 1 oder 2 neben einer automatischen Aufzeichnung eine unmittelbare Kenntnisnahme und wird in deren Verlauf erkennbar, dass Inhalte erfasst werden, die
1. dem Kernbereich privater Lebensgestaltung zuzuordnen sind,
2. einem Geistlichen oder seinem Berufshelfer in der Eigenschaft als Seelsorger anvertraut werden oder
3. einem Vertrauensverhältnis zu einem Berufsgeheimnisträger oder Berufshelfer (§§ 53 oder 53a StPO) zuzuordnen sind und kein unmittelbarer Bezug zu den in Absatz 1 genannten Gefahren besteht,

ist die unmittelbare Kenntnisnahme unverzüglich und so lange wie erforderlich zu unterbrechen. Diesbezügliche Aufzeichnungen sind zu löschen. Bestehen über die Voraussetzungen einer Unterbrechung Zweifel, gilt Satz 1 entsprechend. Die vorhandenen Aufzeichnungen sind unverzüglich dem anordnenden Richter zur Entscheidung über die Verwendbarkeit oder Löschung der Daten vorzulegen. Ist die unmittelbare Kenntnisnahme unterbrochen worden, so darf sie nur fortgesetzt werden, wenn aufgrund tatsächlicher Anhaltspunkte nicht mehr zu erwarten ist, dass der Kernbereich privater Lebensgestaltung oder ein geschütztes Vertrauensverhältnis verletzt werden. Die Tatsache der Erlangung und die Löschung der Daten sind zu protokollieren.

(5) Maßnahmen nach den Absätzen 1 und 2 dürfen nur auf Antrag des Leiters der Landespolizeidirektion oder des Leiters des Landeskriminalamts oder eines beson-

ders beauftragten Beamten des höheren Polizeivollzugsdienstes durch den Richter angeordnet werden. Bei Gefahr im Verzug können die in Satz 1 genannten Behördenleiter oder bei deren jeweiliger Verhinderung ein besonders beauftragter Beamter des höheren Polizeivollzugsdienstes die Anordnung treffen; die richterliche Entscheidung ist in diesem Fall unverzüglich nachzuholen. Die Anordnung nach Satz 2 Halbsatz 1 tritt außer Kraft, wenn sie nicht binnen drei Werktagen durch den Richter bestätigt wird.

(6) Eine Anordnung nach Absatz 5 ergeht schriftlich. In ihr sind anzugeben:
1. die Person, gegen die sich die Maßnahme richtet, soweit möglich mit Name und Anschrift,
2. die Rufnummer oder eine andere Kennung des zu überwachenden Anschlusses oder des Endgeräts, sofern sich nicht aus bestimmten Tatsachen ergibt, dass diese zugleich einem anderen Endgerät zugeordnet ist,
3. die Art, der Umfang und die Dauer der Maßnahme unter Benennung des Endzeitpunktes und
4. im Fall des Absatzes 2 auch eine möglichst genaue Bezeichnung des informationstechnischen Systems, in das zur Datenerhebung eingegriffen werden soll.

Die Maßnahmen sind auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als drei weitere Monate ist zulässig, soweit die Voraussetzungen der Anordnung unter Berücksichtigung der gewonnenen Erkenntnisse fortbestehen. Liegen die Voraussetzungen der Anordnung nicht mehr vor, sind die aufgrund der Anordnung ergriffenen Maßnahmen unverzüglich zu beenden.

(7) Aufgrund der Anordnung hat jeder, der Telekommunikationsdienste erbringt oder daran mitwirkt (Diensteanbieter), der Polizei die Maßnahmen nach Absatz 1 zu ermöglichen und die erforderlichen Auskünfte unverzüglich zu erteilen. Ob und in welchem Umfang hierfür Vorkehrungen zu treffen sind, bestimmt sich nach dem Telekommunikationsgesetz (TKG) und der Telekommunikations-Überwachungsverordnung. Für die Entschädigung der in Anspruch genommenen Unternehmen ist § 23 des Justizvergütungs- und -entschädigungsgesetzes (JVEG) entsprechend anzuwenden.

§ 34 b
Erhebung von Telekommunikationsverkehrsdaten und Nutzungsdaten

(1) Die Polizei kann zur Abwehr einer Gefahr für den Bestand oder die Sicherheit der Bundesrepublik Deutschland oder eines Landes oder für Leben, Gesundheit oder Freiheit einer Person oder zur Abwehr einer gemeinen Gefahr für Sachen Verkehrsdaten (§ 96 Abs. 1 TKG)
1. der für die Gefahr Verantwortlichen,
2. von Personen, bei denen Tatsachen die Annahme rechtfertigen, dass sie für die für die Gefahr Verantwortlichen bestimmte oder von diesen herrührende Mitteilungen entgegennehmen oder weitergeben,

3. von Personen, soweit bestimmte Tatsachen die begründete Annahme rechtfertigen, dass die für die Gefahr Verantwortlichen ihre Kommunikationseinrichtungen benutzen werden, oder
4. von vermissten, suizidgefährdeten oder hilflosen Personen

erheben. Die Maßnahme ist nur zulässig, wenn die Abwehr der Gefahr auf andere Weise aussichtslos oder wesentlich erschwert wäre. Die Anordnung der Maßnahme nach Satz 1 Nr. 2 und 3 ist unzulässig, wenn die Person zu einer der in den §§ 53 oder 53a StPO genannten Berufsgruppen gehört. Die Maßnahme darf auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen sein werden.

(2) Unter den Voraussetzungen des Absatzes 1 kann die Polizei von denjenigen, die geschäftsmäßig eigene oder fremde Telemedien zur Nutzung bereithalten oder den Zugang zur Nutzung vermitteln, Auskunft über Nutzungsdaten (§ 15 Abs. 1 des Telemediengesetzes) verlangen. Die Auskunft kann auch über zukünftige Nutzungsdaten angeordnet werden.

(3) Für die Anordnung der Maßnahme gilt § 34 a Abs. 5 und 6 entsprechend. Abweichend von § 34 a Abs. 6 Nr. 2 genügt eine räumlich und zeitlich hinreichende Bezeichnung der Telekommunikation, sofern anderenfalls die Erreichung des Zwecks der Maßnahme aussichtslos oder wesentlich erschwert wäre.

(4) Für die Entschädigung der in Anspruch genommenen Unternehmen ist § 23 JVEG entsprechend anzuwenden."

5. Nach § 34 b werden folgende §§ 34 c bis 34 e eingefügt:

"§ 34 c
Identifizierung und Lokalisierung von Mobilfunkkarten und -endgeräten

(1) Die Polizei kann, wenn dies zur Abwehr einer Gefahr für den Bestand oder die Sicherheit der Bundesrepublik Deutschland oder eines Landes oder für Leben, Gesundheit oder Freiheit einer Person oder zur Abwehr einer gemeinen Gefahr für Sachen zwingend erforderlich ist und die Abwehr der Gefahr auf andere Weise aussichtslos oder wesentlich erschwert wäre, durch technische Mittel

1. die Gerätenummer eines Mobilfunkendgeräts und die Kartennummer der darin verwendeten Karte sowie
2. den Standort eines Mobilfunkendgeräts

der für die Gefahr Verantwortlichen ermitteln.

(2) Personenbezogene Daten Dritter dürfen bei einer Maßnahme nach Absatz 1 nur erhoben werden, wenn dies aus technischen Gründen unvermeidbar ist. Über den Datenabgleich zur Ermittlung der gesuchten Geräte- und Kartennummer hinaus dürfen sie nicht verwendet werden und sind nach Beendigung der Maßnahme unverzüglich zu löschen.

(3) Für die Anordnung der Maßnahme gilt § 34 a Abs. 5 und 6 entsprechend.

(4) Aufgrund der Anordnung einer Maßnahme nach Absatz 1 Nr. 2 hat jeder, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, der Polizei die für die Ermittlung des Standorts des Mobilfunkendgeräts erforderliche Geräte- und Kartennummer unverzüglich mitzuteilen. Für die Entschädigung der in Anspruch genommenen Unternehmen ist § 23 JVEG entsprechend anzuwenden.

§ 34 d
Unterbrechung und Verhinderung von Telekommunikation

(1) Die Polizei kann, wenn dies zur Abwehr einer gegenwärtigen Gefahr für den Bestand oder die Sicherheit der Bundesrepublik Deutschland oder eines Landes oder für Leben, Gesundheit oder Freiheit einer Person zwingend erforderlich ist, durch den Einsatz technischer Mittel Kommunikationsverbindungen der für die Gefahr Verantwortlichen unterbrechen oder verhindern. Kommunikationsverbindungen Dritter dürfen nur unterbrochen oder verhindert werden, wenn die Gefahr durch andere Mittel nicht abgewehrt werden kann.

(2) Maßnahmen nach Absatz 1 dürfen nur durch den Leiter der Landespolizeidirektion oder den Leiter des Landeskriminalamts oder durch einen von diesen besonders beauftragten Beamten des höheren Polizeivollzugsdienstes angeordnet werden. Die Anordnung hat schriftlich unter Angabe der für sie maßgeblichen Gründe zu erfolgen und ist auf höchstens drei Tage zu befristen.

§ 34 e
Erhebung von Bestandsdaten

(1) Soweit dies zur Abwehr einer Gefahr erforderlich ist, darf die Polizei von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, Auskunft über die nach den §§ 95 und 111 TKG erhobenen Daten verlangen (§ 113 Abs. 1 Satz 1 TKG). Bezieht sich das Auskunftsverlangen nach Satz 1 auf Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird (§ 113 Abs. 1 Satz 2 TKG), darf die Auskunft nur

1. zur Überwachung der Telekommunikation nach § 34 a oder
2. zur Sicherstellung von nicht mehr dem Schutz des Artikels 10 des Grundgesetzes unterliegenden in Endeinrichtungen oder auf Speichereinrichtungen abgelegten Daten nach § 27

verlangt werden, wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen.

(2) Die Auskunft nach Absatz 1 darf auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse verlangt werden (§ 113 Abs. 1 Satz 3 TKG).

(3) Auskunftsverlangen nach Absatz 1 Satz 2 dürfen nur auf Antrag des Leiters der Landespolizeidirektion oder des Leiters des Landeskriminalamts oder eines besonders beauftragten Beamten des höheren Polizeivollzugsdienstes durch den Richter angeordnet werden.

Bei Gefahr im Verzug können die in Satz 1 genannten Behördenleiter oder, bei deren jeweiliger Verhinderung, ein besonders beauftragter Beamter des höheren Polizeivollzugsdienstes die Anordnung treffen; die richterliche Entscheidung ist in diesem Fall unverzüglich nachzuholen. Die Anordnung nach Satz 2 tritt außer Kraft, wenn sie nicht binnen drei Werktagen durch den Richter bestätigt wird. Die Sätze 1 bis 3 finden keine Anwendung, wenn der Betroffene vom Auskunftsverlangen bereits Kenntnis hat oder haben muss oder wenn die Nutzung der Daten bereits durch eine gerichtliche Entscheidung gestattet wird. Das Vorliegen der Voraussetzungen nach Satz 4 ist aktenkundig zu machen.

(4) Für die Entschädigung der in Anspruch genommenen Unternehmen ist § 23 JVEG entsprechend anzuwenden."

6. Die §§ 35 und 36 erhalten folgende Fassung:

"§ 35
Wohnraumüberwachung

(1) Die Polizei kann durch den verdeckten Einsatz technischer Mittel in oder aus Wohnungen (§ 25 Abs. 1 Satz 2) personenbezogene Daten erheben, wenn dies zur Abwehr einer dringenden Gefahr für die öffentliche Sicherheit, insbesondere einer gemeinen Gefahr oder einer Lebensgefahr, erforderlich ist und die Abwehr der Gefahr auf andere Weise unverhältnismäßig erschwert oder aussichtslos wäre.

(2) Die Maßnahme nach Absatz 1 darf nur angeordnet werden, soweit nicht aufgrund tatsächlicher Anhaltspunkte, insbesondere beruhend auf der Art der zu überwachenden Räumlichkeiten oder dem Verhältnis der zu überwachenden Personen zueinander, anzunehmen ist, dass durch die Überwachung Daten aus dem Kernbereich privater Lebensgestaltung oder aus einem Vertrauensverhältnis mit Berufsgeheimnisträgern oder deren Berufshelfern (§§ 53 oder 53a StPO) erlangt würden.

(3) Die Maßnahme darf sich nur gegen die für die Gefahr verantwortlichen Personen richten und nur in deren Wohnung durchgeführt werden. Hierzu kann die Polizei deren Wohnungen betreten, wenn dies erforderlich ist, um die technischen Voraussetzungen des Einsatzes besonderer Mittel zu schaffen.

(4) Maßnahmen nach Absatz 1 dürfen nur auf Antrag des Leiters der Landespolizeidirektion oder des Leiters des Landeskriminalamts oder eines besonders beauftragten Beamten des höheren Polizeivollzugsdienstes durch den Richter angeordnet werden. Bei Gefahr im Verzug können die in Satz 1 genannten Behördenleiter oder, bei deren jeweiliger Verhinderung, ein besonders beauftragter Beamter des höheren Polizeivollzugsdienstes die Anordnung treffen. Die richterliche Entscheidung ist unverzüglich nachzuholen. Die Anordnung nach Satz 2 tritt außer Kraft, wenn sie nicht binnen drei Werktagen durch den Richter bestätigt wird.

(5) Eine Anordnung nach Absatz 4 ergeht schriftlich. Sie enthält
1. soweit bekannt, den Namen und die Anschrift der Person, gegen die sich die Maßnahme richtet,
2. die zu überwachende Wohnung oder die zu überwachenden Wohnräume,
3. die Art, den Umfang und die Dauer der Maßnahme und
4. die wesentlichen Gründe.

Die Maßnahme ist auf höchstens einen Monat zu befristen. Verlängerungen um jeweils nicht mehr als einen weiteren Monat sind auf Antrag zulässig, soweit die Voraussetzungen unter Berücksichtigung der gewonnenen Erkenntnisse für die Anordnung fortbestehen. Bestehen die Voraussetzungen der Anordnung nicht mehr fort, so ist die Maßnahme unverzüglich zu beenden. Die Beendigung ist dem Richter unverzüglich mitzuteilen.

(6) Das Abhören und Beobachten nach Absatz 1 ist unverzüglich und so lange wie erforderlich zu unterbrechen, soweit während der Überwachung erkennbar wird, dass Inhalte erfasst werden, die
1. dem Kernbereich privater Lebensgestaltung zuzuordnen sind,
2. einem Geistlichen oder seinem Berufshelfer in der Eigenschaft als Seelsorger anvertraut werden oder
3. einem Vertrauensverhältnis zu einem Berufsgeheimnisträger oder Berufshelfer (§§ 53 oder 53a StPO) zuzuordnen sind und kein unmittelbarer Bezug zu den in Absatz 1 genannten Gefahren besteht.

Angefertigte Aufzeichnungen und Aufnahmen sind unverzüglich zu löschen. Bestehen über die Voraussetzungen einer Unterbrechung Zweifel, gilt Satz 1 entsprechend. In diesem Fall sind nur automatisierte Aufzeichnungen zulässig. Diese sind unverzüglich dem anordnenden Richter zur Entscheidung über die Verwendbarkeit oder Löschung der Daten vorzulegen. Ist die Aufnahme, die Aufzeichnung oder die unmittelbare Kenntnisnahme unterbrochen worden, so darf sie nur fortgesetzt werden, wenn aufgrund tatsächlicher Anhaltspunkte nicht mehr zu erwarten ist, dass der Kernbereich privater Lebensgestaltung oder ein geschütztes Vertrauensverhältnis verletzt wird. Die Tatsache der Erlangung und die Löschung der Daten sind zu protokollieren.

(7) Die Anordnung eines verdeckten Einsatzes technischer Mittel in oder aus Wohnungen ausschließlich zum Schutz der bei einem polizeilichen Einsatz tätigen Personen treffen die in Absatz 4 Satz 1 genannten Behördenleiter oder, bei deren jeweiliger Verhinderung, ein besonders beauftragter Beamter des höheren Polizeivollzugsdienstes. Eine anderweitige Nutzung der hierbei erlangten Erkenntnisse zu Zwecken der Abwehr einer dringenden Gefahr ist nur zulässig, wenn zuvor die Rechtmäßigkeit der Maßnahme richterlich festgestellt ist; bei Gefahr im Verzug ist die richterliche Entscheidung unverzüglich nachzuholen. Absatz 6 findet entsprechende Anwendung. Aufzeichnungen aus einem solchen Einsatz sind unverzüglich nach Beendigung des Einsatzes zu löschen, soweit sie nicht zur Gefahrenabwehr benötigt werden; die Löschung ist zu protokollieren.

§ 36
Gemeinsame Verfahrensbestimmungen für
Maßnahmen der verdeckten Datenerhebung

(1) Die durch eine Maßnahme nach den §§ 34 bis 34 c sowie den §§ 34 e und 35 erlangten Daten sind besonders zu kennzeichnen. Für den Fall der Übermittlung ist die Kennzeichnung durch den Empfänger aufrechtzuerhalten. Die Daten dürfen grundsätzlich nur zur Abwehr der Gefahr, die zur Anordnung der Überwachungsmaßnahme geführt hat, verwendet werden. Eine Verwendung in einem anderen Verfahren ist nur zulässig, wenn die Datenerhebung auch in diesem Verfahren hätte angeordnet werden dürfen; die Zweckänderung ist zu dokumentieren.

(2) Daten, bei denen sich nach der Auswertung herausstellt, dass sie Inhalte betreffen,
1. die dem Kernbereich privater Lebensgestaltung zuzuordnen sind,
2. über die das Zeugnis als Geistlicher oder als Berufshelfer eines Geistlichen verweigert werden könnte oder
3. über die das Zeugnis nach den §§ 53 oder 53a StPO verweigert werden könnte und bei denen kein unmittelbarer Bezug zu den Gefahren besteht, die zur Anordnung der Maßnahme geführt haben,

dürfen nicht verwendet werden und sind unverzüglich zu löschen. Eine Verwendung ist ausnahmsweise zulässig, wenn dies zur Abwehr einer gegenwärtigen Gefahr für Leben oder Freiheit einer Person zwingend erforderlich ist. Vor einer Verwendung der Daten ist über deren Zulässigkeit eine richterliche Entscheidung herbeizuführen. Bei Gefahr im Verzug kann die Entscheidung auch der Leiter der Landespolizeidirektion, der Leiter des Landeskriminalamtes oder ein von diesen besonders beauftragter Beamter des höheren Polizeivollzugsdienstes treffen; in diesem Fall ist eine richterliche Entscheidung unverzüglich nachzuholen. Die Tatsache der Erlangung und die Löschung der Daten sind zu protokollieren. Satz 1 findet keine Anwendung, wenn ein Berufsgeheimnisträger betroffen ist, der selbst für die Gefahr verantwortlich ist.

(3) Von Maßnahmen nach den §§ 34 bis 34 c sowie den §§ 34 e und 35 sind zu benachrichtigen im Fall
1. des § 34 Abs. 2 Nr. 1 und 2 (längerfristige Observation, technische Observationsmittel, Bildaufzeichnungen, Aufzeichnung des nicht öffentlich gesprochenen Wortes) die Zielperson sowie die erheblich mitbetroffenen Personen,
2. des § 34 Abs. 2 Nr. 3 bis 5 (verdeckt handelnde Personen):
   a) die Zielperson,
   b) die erheblich mitbetroffenen Personen,
   c) die Personen, deren nicht allgemein zugängliche Wohnung die verdeckt handelnde Person betreten hat,
3. des § 34 a (Telekommunikationsüberwachung) die Beteiligten der überwachten Telekommunikation,
4. des § 34 b Abs. 1 (Erhebung von Verkehrsdaten) die Beteiligten der betroffenen Telekommunikation,
5. des § 34 b Abs. 2 (Erhebung von Nutzungsdaten) der Nutzer,
6. des § 34 c (IMSI-Catcher) die Zielperson,

7. des § 34 e Abs. 1 Satz 2 (Erhebung von Zugangssicherungscodes) der Nutzer,
8. des § 34 e Abs. 2 (Auskunft über den Nutzer einer Internetprotokoll-Adresse) der Nutzer,
9. des § 35 (Wohnraumüberwachung):
   a) die Person, gegen die sich die Maßnahme richtete,
   b) sonstige überwachte Personen,
   c) Personen, die die überwachte Wohnung zur Zeit der Durchführung der Maßnahme innehatten oder bewohnten.

Die Benachrichtigung unterbleibt, wenn ihr überwiegende schutzwürdige Belange einer betroffenen Person entgegenstehen. Zudem kann die Benachrichtigung einer in Satz 1 Nr. 3 und 4 bezeichneten Person, gegen die sich die Maßnahme nicht gerichtet hat, unterbleiben, wenn diese von der Maßnahme nur unerheblich betroffen gewesen ist und anzunehmen ist, dass sie kein Interesse an einer Benachrichtigung hat. Nachforschungen zur Feststellung der Identität einer in Satz 1 bezeichneten Person sind nur vorzunehmen, wenn dies unter Berücksichtigung der Eingriffsintensität der Maßnahme gegenüber dieser Person, des Aufwands für die Feststellung ihrer Identität sowie der daraus für diese oder andere Personen folgenden Beeinträchtigungen geboten ist.

(4) Die Benachrichtigung erfolgt, sobald dies ohne Gefährdung des Zwecks der Maßnahme, des Bestands des Staates oder von Gesundheit, Leben oder Freiheit einer Person möglich ist. Im Fall des Absatzes 3 Satz 1 Nr. 2 kann die Benachrichtigung zudem auch zurückgestellt werden, wenn die Möglichkeit der weiteren Verwendung der verdeckt handelnden Personen durch die Benachrichtigung gefährdet wäre und unter Berücksichtigung der Eingriffsintensität der Maßnahme gegenüber den Betroffenen das öffentliche Interesse an der Weiterverwendung überwiegt. Ist wegen desselben Sachverhalts ein strafrechtliches Ermittlungsverfahren gegen den Betroffenen eingeleitet worden, ist die Benachrichtigung in Abstimmung mit der Staatsanwaltschaft vorzunehmen, sobald dies der Stand des Ermittlungsverfahrens zulässt. Wird die Benachrichtigung aus einem der vorgenannten Gründe zurückgestellt, ist dies zu dokumentieren.

(5) Erfolgt die Benachrichtigung nicht binnen sechs Monaten nach Beendigung der Maßnahme, bedarf die weitere Zurückstellung der richterlichen Zustimmung. Die richterliche Entscheidung ist vorbehaltlich einer anderen richterlichen Fristsetzung jeweils nach einem Jahr erneut einzuholen. Eine Benachrichtigung kann mit richterlicher Zustimmung auf Dauer unterbleiben, wenn die Gründe nach Absatz 4 mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft fortbestehen werden. Die Entscheidung nach Satz 3 darf frühestens fünf Jahre nach Beendigung der Maßnahme getroffen werden. Sind mehrere Maßnahmen im selben Sachzusammenhang durchgeführt worden, ist die Beendigung der letzten Maßnahme für die Berechnung der Fristen maßgeblich.

(6) Zuständig für richterliche Entscheidungen nach den Absätzen 2 und 5 sowie nach den §§ 34 bis 34 c sowie den §§ 34 e und 35 ist das Amtsgericht, in des-

sen Bezirk die beantragende Polizeibehörde ihren Sitz hat. Für das Verfahren gelten die Bestimmungen des Buches 1 des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend. Diese Entscheidungen des Gerichts ergehen ohne vorherige Anhörung der Betroffenen; sie bedürfen zu ihrer Wirksamkeit nicht der Bekanntmachung an die Betroffenen. Gegen die Ablehnung des Antrags der Polizeibehörde auf Zustimmung zur Zurückstellung oder zum dauerhaften Unterbleiben einer Benachrichtigung findet die Beschwerde statt. Die Beschwerde ist binnen einer Frist von zwei Wochen einzulegen. Für dieses Beschwerdeverfahren gilt Satz 3 entsprechend. Die Benachrichtigung darf bis zur Rechtskraft der richterlichen Entscheidung vorläufig unterbleiben.

(7) Die Landesregierung unterrichtet den Landtag jährlich über die durchgeführten Maßnahmen nach den §§ 34 a bis 34 c und 35."

7. § 37 wird wie folgt geändert:

   a) Die Absätze 1 und 2 erhalten folgende Fassung:

      "(1) Die Polizei kann personenbezogene Daten, insbesondere die Personalien einer Person sowie das amtliche Kennzeichen des von ihr benutzten Fahrzeugs, zur Mitteilung über das Antreffen (polizeiliche Beobachtung) oder zur gezielten Kontrolle ausschreiben, wenn die Gesamtwürdigung der Person und ihrer bisher begangenen Straftaten erwarten lässt, dass sie auch künftig Straftaten von erheblicher Bedeutung begehen wird und die polizeiliche Beobachtung zur vorbeugenden Bekämpfung dieser Straftaten erforderlich ist.

      (2) Im Fall eines Antreffens der Person oder des Fahrzeugs können Erkenntnisse über das Antreffen sowie über etwaige Begleiter und mitgeführte Sachen an die ausschreibende Polizeidienststelle übermittelt werden."

   b) Folgender Absatz 5 wird angefügt:

      "(5) Nach Abschluss der Maßnahmen sind die ausgeschriebene Person und die Personen, deren personenbezogene Daten infolge der Ausschreibung gemeldet wurden, zu benachrichtigen. § 36 Abs. 3 bis 6 gilt entsprechend."

8. § 41 Abs. 1 Satz 2 wird aufgehoben.

9. Nach § 41 werden folgende §§ 41 a bis 41 d eingefügt:

"§ 41 a
Datenübermittlung zum Zwecke einer Zuverlässigkeitsüberprüfung

Zum Zwecke der Gefahrenabwehr bei besonders gefährdeten Veranstaltungen kann die Polizei personenbezogene Daten an öffentliche und nichtöffentliche Stellen übermitteln, wenn es

1. für eine Zuverlässigkeitsüberprüfung erforderlich ist,

2. mit schriftlicher Einwilligung des Betroffenen erfolgt und
3. im Hinblick auf den Anlass dieser Überprüfung, insbesondere den Zugang des Betroffenen zu der Veranstaltung, sowie wegen der Art und des Umfangs der Erkenntnisse über ihn und mit Rücksicht auf das berechtigte Sicherheitsinteresse des Datenempfängers angemessen ist.

Die Rückmeldung an eine nichtöffentliche Stelle beschränkt sich auf die Auskunft zum Vorliegen von Zuverlässigkeitsbedenken. Die Übermittlung der personenbezogenen Daten ist zu dokumentieren. Der Empfänger darf die übermittelten Daten nur für den Zweck der Zuverlässigkeitsüberprüfung verarbeiten. Die Polizei hat den Empfänger schriftlich zu verpflichten, diese Zweckbestimmung einzuhalten und eine Löschung der Daten spätestens nach Beendigung der Veranstaltung vorzunehmen. Der Betroffene ist über den Inhalt der Übermittlung zu informieren, soweit dies nicht bereits auf andere Weise sichergestellt ist.

§ 41 b
Übermittlung personenbezogener Daten an Mitgliedstaaten der Europäischen Union aufgrund des Rahmenbeschlusses 2006/960/JI

(1) Auf ein Ersuchen einer Polizeibehörde oder einer sonstigen für die Verhütung und Verfolgung von Straftaten zuständigen öffentlichen Stelle eines Mitgliedstaats der Europäischen Union kann die Polizei personenbezogene Daten zum Zwecke der Verhütung von Straftaten übermitteln. Für die Übermittlung dieser Daten gelten die Vorschriften über die Datenübermittlung im innerstaatlichen Bereich entsprechend.

(2) Die Übermittlung personenbezogener Daten nach Absatz 1 ist nur zulässig, wenn das Ersuchen mindestens folgende Angaben enthält:
1. die Bezeichnung und die Anschrift der ersuchenden Behörde,
2. die Bezeichnung der Straftat, zu deren Verhütung die Daten benötigt werden,
3. die Beschreibung des Sachverhalts, der dem Ersuchen zugrunde liegt,
4. die Benennung des Zwecks, zu dem die Daten erbeten werden,
5. den Zusammenhang zwischen dem Zweck, zu dem die Informationen oder Erkenntnisse erbeten werden, und der Person, auf die sich diese Informationen beziehen,
6. Einzelheiten zur Identität der betroffenen Person, soweit sich das Ersuchen auf eine bekannte Person bezieht, und
7. Gründe für die Annahme, dass sachdienliche Informationen und Erkenntnisse im Inland vorliegen.

(3) Die Polizei kann auch ohne Ersuchen personenbezogene Daten an eine Polizeibehörde oder eine sonstige für die Verhütung oder Verfolgung von Straftaten zuständige öffentliche Stelle eines Mitgliedstaates der Europäischen Union übermitteln, wenn Tatsachen die Annahme rechtfertigen, dass eine Straftat im Sinne des Artikels 2 Abs. 2 des Rahmenbeschlusses 2002/584/JI des Rates vom 13. Juni 2002 über den Europäischen Haftbefehl und die Übergabeverfahren zwischen den

Mitgliedstaaten (ABl. L 190 vom 18. Juli 2002, S. 1) begangen werden soll und konkrete Anhaltspunkte dafür vorliegen, dass die Übermittlung dieser personenbezogenen Daten dazu beitragen könnte, eine solche Straftat zu verhindern. Für die Übermittlung dieser Daten gelten die Vorschriften über die Datenübermittlung im innerstaatlichen Bereich entsprechend.

(4) Die Datenübermittlungen nach den Absätzen 1 bis 3 sind zu dokumentieren. Bei der Übermittlung sind besondere Verwendungsbeschränkungen und geltende Sperr- oder Löschfristen mitzuteilen.

(5) Die Zulässigkeit der Übermittlung personenbezogener Daten an eine Polizeibehörde oder eine sonstige für die Verhütung und Verfolgung von Straftaten zuständige öffentliche Stelle eines Mitgliedstaates der Europäischen Union auf Grundlage des § 41 Abs. 4 bleibt unberührt.

(6) Die Datenübermittlung nach den Absätzen 1 und 3 unterbleibt über die in § 41 Abs. 4 Satz 4 genannten Gründe hinaus auch dann, wenn
1. hierdurch wesentliche Sicherheitsinteressen der Bundesrepublik Deutschland oder eines Landes beeinträchtigt würden,
2. hierdurch der Erfolg laufender Ermittlungen oder Leib, Leben oder Freiheit einer Person gefährdet würde,
3. die Übermittlung der Daten zu den in Artikel 6 des Vertrages über die Europäische Union enthaltenen Grundsätzen in Widerspruch stünde,
4. die zu übermittelnden Daten bei der ersuchten Behörde nicht vorhanden sind und nur durch das Ergreifen von Zwangsmaßnahmen erlangt werden können oder
5. die Übermittlung der Daten unverhältnismäßig wäre oder die Daten für die Zwecke, für die sie übermittelt werden sollen, nicht erforderlich ist.

(7) Die Datenübermittlung nach den Absätzen 1 und 3 kann darüber hinaus auch unterbleiben, wenn
1. die zu übermittelnden Daten bei der ersuchten Stelle nicht vorhanden sind, jedoch ohne das Ergreifen von Zwangsmaßnahmen erlangt werden können oder
2. die Tat, zu deren Verhütung die Daten übermittelt werden sollen, nach deutschem Recht mit einer Freiheitsstrafe von im Höchstmaß einem Jahr oder weniger bedroht ist.

(8) Als Polizeibehörde oder sonstige für die Verhütung und Verfolgung von Straftaten zuständige öffentliche Stelle eines Mitgliedstaats der Europäischen Union im Sinne der Absätze 1 und 3 gilt jede Stelle, die von diesem Staat gemäß Artikel 2 Buchst. a des Rahmenbeschlusses 2006/960/JI des Rates vom 18. Dezember 2006 über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union (ABl. L 386 vom 29. Dezember 2006, S. 89, L 75 vom 15. März 2007, S. 26) benannt wurde.

(9) Die Absätze 1 bis 8 finden auch Anwendung auf die Übermittlung von personenbezogenen Daten an Poli-

zeibehörden oder sonstige für die Verhütung und Verfolgung von Straftaten zuständige öffentliche Stellen eines Staats, der die Bestimmungen des Schengen-Besitzstandes aufgrund eines Assoziierungsübereinkommens mit der Europäischen Union über die Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstandes anwendet (Schengen-assoziierter Staat).

§ 41 c
Verarbeitung von Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union übermittelt worden sind

(1) Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union an die Polizei übermittelt worden sind, dürfen ohne Zustimmung der übermittelnden Stelle oder Einwilligung der betroffenen Person nur

1. für die Zwecke, für die sie übermittelt wurden,
2. zur Verhütung von Straftaten, zur Strafverfolgung oder zur Strafvollstreckung,
3. für andere justizielle und verwaltungsbehördliche Verfahren, die mit der Verhütung von Straftaten, der Strafverfolgung oder der Strafvollstreckung unmittelbar zusammenhängen oder
4. zur Abwehr einer gegenwärtigen und erheblichen Gefahr für die öffentliche Sicherheit

verarbeitet werden.

(2) Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union nach dem Rahmenbeschluss 2006/960/JI an die Polizei übermittelt worden sind, dürfen nur für die Zwecke, für die sie übermittelt wurden, oder zur Abwehr einer gegenwärtigen und erheblichen Gefahr für die öffentliche Sicherheit verarbeitet werden. Für einen anderen Zweck dürfen sie nur verarbeitet werden, wenn die übermittelnde Stelle zugestimmt hat.

(3) Die übermittelten Daten sind zu kennzeichnen. Die empfangende Stelle hat von der übermittelnden Stelle mitgeteilte Bedingungen und besondere Verarbeitungsbeschränkungen zu beachten, insbesondere Fristen, nach deren Ablauf die Daten zu löschen, zu sperren oder auf die Erforderlichkeit ihrer fortgesetzten Speicherung zu prüfen sind. Hat die übermittelnde Stelle eine nach ihrem innerstaatlichen Recht geltende Sperr- oder Löschfrist mitgeteilt, dürfen die Daten nach Ablauf dieser Frist nur noch für laufende Strafverfolgungs- oder Strafvollstreckungsverfahren verarbeitet werden. Hat die übermittelnde Stelle mitgeteilt, dass unrichtige Daten oder Daten unrechtmäßig übermittelt wurden, sind diese unverzüglich zu berichtigen, zu löschen oder zu sperren. Der übermittelnden Stelle ist auf deren Ersuchen zu Zwecken der Datenschutzkontrolle Auskunft darüber zu erteilen, wie die übermittelten Daten verarbeitet wurden.

(4) Die übermittelten Daten dürfen mit Zustimmung der übermittelnden Stelle an andere öffentliche Stellen außerhalb des Anwendungsbereichs des Rahmenbeschlusses 2008/977/JI des Rates vom 27. November

2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (ABl. L 350 vom 30. Dezember 2008, S. 60) oder an internationale Einrichtungen weiterübermittelt werden, soweit dies zur Verhütung von Straftaten, zur Strafverfolgung oder zur Strafvollstreckung erforderlich ist und

1. der Empfänger ein angemessenes Datenschutzniveau gewährleistet,
2. die Weiterübermittlung aufgrund überwiegender Interessen der betroffenen Person oder überwiegender öffentlicher Interessen erforderlich ist oder
3. die empfangende Stelle im Einzelfall angemessene Garantien bietet.

Ohne Zustimmung ist eine Weiterübermittlung nur zulässig, soweit dies zur Wahrung wesentlicher Interessen eines Mitgliedstaats oder zur Abwehr einer gegenwärtigen und erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist und die Zustimmung nicht rechtzeitig eingeholt werden kann. Die für die Erteilung der Zustimmung zuständige Stelle des übermittelnden Mitgliedstaats ist hiervon unverzüglich zu unterrichten.

(5) Die übermittelten Daten dürfen innerhalb der Europäischen Union an Stellen außerhalb des öffentlichen Bereichs nur mit Zustimmung der übermittelnden Stelle weiterübermittelt werden, soweit dies

1. zur Verhütung von Straftaten,
2. zur Strafverfolgung,
3. zur Strafvollstreckung,
4. zur Abwehr einer gegenwärtigen und erheblichen Gefahr für die öffentliche Sicherheit oder
5. zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte Einzelner

erforderlich ist und überwiegende schutzwürdige Interessen des Betroffenen nicht entgegenstehen.

(6) Die Absätze 1 bis 5 gelten entsprechend für Schengen-assoziierte Staaten sowie Behörden und Informationssysteme, die aufgrund des Vertrages über die Europäische Union oder des Vertrages zur Gründung der Europäischen Gemeinschaft errichtet worden sind.

§ 41 d
Übermittlung und Verarbeitung personenbezogener Daten an Mitgliedstaaten der Europäischen Union aufgrund des Ratsbeschlusses 2008/615/JI

Die Bestimmungen des Beschlusses 2008/615/JI des Rates vom 23. Juni 2008 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität (ABl. L 210 vom 6. August 2008, S. 1) sind bei der polizeilichen Zusammenarbeit mit den Mitgliedstaaten der Europäischen Union anwendbar."

10. In § 43 Abs. 1 Satz 1 werden nach dem Wort "Personen" die Worte "sowie von Personen, die sie an einem der in § 14 Abs. 1 Nr. 2 bis 4 genannten Orte angetroffen hat," eingefügt.

11. § 44 wird wie folgt geändert:

    a) Absatz 1 erhält folgende Fassung:

    "(1) Die Polizei kann von öffentlichen oder nichtöffentlichen Stellen die Übermittlung von personenbezogenen Daten bestimmter Personengruppen aus Dateien zum Zweck des automatisierten Abgleichs mit anderen Datenbeständen verlangen, wenn dies zur Abwehr einer Gefahr für den Bestand oder die Sicherheit der Bundesrepublik Deutschland oder eines Landes oder für Leib, Leben oder Freiheit einer Person oder zur Abwehr einer gemeinen Gefahr für Sachen erforderlich ist."

    b) Nach Absatz 4 wird folgender neuer Absatz 5 angefügt:

    "(5) Nach Abschluss der Maßnahme sind die Personen, gegen die nach Auswertung der Daten weitere Ermittlungen geführt wurden, zu benachrichtigen. § 36 Abs. 3 bis 6 gilt entsprechend."

12. § 45 Abs. 2 wird wie folgt geändert:

    a) In Satz 1 Nr. 2 wird der Klammerzusatz "(§ 46 Abs. 1 Satz 1 Nr. 8)" gestrichen.

    b) In Satz 2 wird der Klammerzusatz "(§ 46 Abs. 1 Satz 1 Nr. 8 in Verbindung mit § 38 und § 40 Abs. 2)" gestrichen.

13. Die Inhaltsübersicht wird den vorstehenden Änderungen angepasst.

Artikel 2
Änderung des Ordnungsbehördengesetzes

Das Ordnungsbehördengesetz vom 18. Juni 1993 (GVBl. S. 323), zuletzt geändert durch Gesetz vom 9. September 2010 (GVBl. S. 291), wird wie folgt geändert:

1. Nach § 27 wird folgender § 27 a eingefügt:

"§ 27 a
Örtliche Alkoholkonsumverbote

(1) Die Gemeinden, Verwaltungsgemeinschaften oder erfüllenden Gemeinden können zum Zwecke des Kinder- und Jugendschutzes sowie des allgemeinen Gesundheitsschutzes durch ordnungsbehördliche Verordnung den Konsum von Alkohol in öffentlichen Anlagen und auf öffentlichen Verkehrsflächen, die sich in räumlicher Nähe von Einrichtungen, die ihrer Art nach oder tatsächlich vorwiegend von Kindern und Jugendlichen aufgesucht werden oder in der Nähe von Suchtberatungsstellen oder vergleichbaren sozialen Einrichtungen befinden, verbieten. Das Verbot gilt nur außerhalb zugelassener Freischankflächen und darf sich höchstens auf einen Radius von 200 Metern um die Einrichtung erstrecken. Es sollte sich zeitlich an den üblichen Öffnungs- und Betriebszeiten der Einrichtung orientieren.

(2) Die Gemeinden, Verwaltungsgemeinschaften oder erfüllenden Gemeinden können durch ordnungsbehördliche Verordnung den Konsum von Alkohol in öffentlichen Anlagen und auf bestimmten öffentlichen Verkehrsflächen verbieten, wenn sich die Belastung dieser Anlagen und Verkehrsflächen durch Ausmaß und Häufigkeit alkoholbedingter Straftaten oder Ordnungswidrigkeiten von der des übrigen Gemeindegebietes deutlich abhebt und Tatsachen die Annahme rechtfertigen, dass dort auch zukünftig mit der Begehung alkoholbedingter Straftaten oder Ordnungswidrigkeiten zu rechnen ist. Das Verbot gilt nur außerhalb zugelassener Freischankflächen. Es kann zeitlich befristet oder unbefristet erlassen werden. Der Verordnungsgeber ist gehalten, alle fünf Jahre zu überprüfen, ob die Voraussetzungen für die ordnungsbehördliche Verordnung noch vorliegen.

(3) Die Verbotsbereiche sind durch Hinweisschilder kenntlich zu machen."

2. Die Inhaltsübersicht wird der vorstehenden Änderung angepasst.

Artikel 3
Einschränkung von Grundrechten

Aufgrund dieses Gesetzes können die Grundrechte auf Freiheit der Person (Artikel 2 Abs. 2 Satz 2 des Grundgesetzes, Artikel 3 Abs. 1 Satz 2 der Verfassung des Freistaats Thüringen), Wahrung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10 des Grundgesetzes, Artikel 7 der Verfassung des Freistaats Thüringen), Schutz der personenbezogenen Daten (Artikel 6 Abs. 2 der Verfassung des Freistaats Thüringen) und auf Unverletzlichkeit der Wohnung (Artikel 13 des Grundgesetzes, Artikel 8 der Verfassung des Freistaats Thüringen) eingeschränkt werden.

Artikel 4
Inkrafttreten

Dieses Gesetz tritt am Tage nach der Verkündung in Kraft.

Begründung:

A. Allgemeines

1.
Durch den Thüringer Verfassungsgerichtshof wurden mit Urteil vom 21. November 2012, Az.: VerfGH 19/09, verschiedene Bestimmungen des Polizeiaufgabengesetzes (PAG) für verfassungswidrig erklärt:

- § 5 Abs. 3 bis 6, der den Schutz der Berufsgeheimnisträger zum Gegenstand hat, verstößt gegen den Grundsatz der Normenklarheit.
- Durch die weit vorgezogene Stellung der Schutzregelungen zugunsten der Berufsgeheimnisträger im Gesetz wird zudem ein weit über den Bereich der verdeckten Datenerhebung hinausreichendes generelles Verbot von Maßnahmen gegen Geistliche, Strafverteidiger und Abgeordnete statuiert, selbst wenn diese für eine Gefahr verantwortlich sind. Dies stellt einen Verstoß gegen die Schutzpflicht des Staats gegenüber seinen Bürgern dar.
- Die gesetzliche Definition des Kernbereichs privater Lebensgestaltung in § 5 Abs. 7 engt diesen zu weit ein und stellt daher einen Verstoß gegen die Menschenwürde dar.
- § 34 Abs. 3 Nr. 2 und 3, § 34 a Abs. 3 Satz 1 Nr. 2 und 3 sowie § 35 Abs. 1 Satz 1 Nr. 2 sind für verfassungswidrig erklärt worden, weil sie auf den Straftatenkatalog in § 31 Abs. 5 Bezug nehmen. Die alleinige Bezugnahme auf Strafrechtsnormen ohne zusätzliche Bestimmung der Gefahrenschwelle wurde vom Verfassungsgerichtshof in Übereinstimmung mit dem Bundesverfassungsgericht als ungeeignete Regelungstechnik für gefahrenabwehrende Normen angesehen, die zu erheblichen Grundrechtseingriffen ermächtigen.
- Die Regelungen zur nachträglichen Benachrichtigung der von verdeckten Datenerhebungen Betroffenen in § 34 Abs. 9 und 10 wurden durch den Verfassungsgerichtshof für verfassungswidrig erklärt, weil sie bei den Ausnahmegründen keine Differenzierung nach den von den Ausgangsmaßnahmen eingeschränkten Grundrechten erkennen lassen und zudem wesentliche Entscheidungen durch den Gesetzgeber in das Ermessen der Verwaltung gelegt wurden, ohne eine Absicherung durch richterliche Entscheidung vorzusehen.

In Umsetzung des Urteils sind zum Teil gravierende Anpassungen des Polizeiaufgabengesetzes vorzunehmen. Die Aufgabe der Bezugnahme auf Straftatenkataloge (§ 31 Abs. 5) als Tatbestandsmerkmal wirkt sich nicht nur auf die durch das Gericht betrachteten Normen der Datenerhebung mit besonderen Mitteln (§ 34), der Telekommunikationsüberwachung (§ 34 a) und der Wohnraumüberwachung (§ 35) aus, sondern zwingt darüber hinaus zu Anpassungen auch der Bestimmungen zur Gewahrsamnahme (§ 19), zur polizeilichen Beobachtung (§ 37) und zur Rasterfahndung (§ 44). Die aus den vorgenannten Gründen ohnehin erforderliche Überarbeitung der Bestimmung zur präventiven Telekommunikationsüberwachung soll darüber hinaus zu einer generellen Neugestaltung mit dem Ziel der besseren Verständlichkeit und Lesbarkeit genutzt werden.

Bei der Neukonzeptionierung des Berufsgeheimnisträgerschutzes sind neben den Ausführungen des Gerichts auch die Festlegungen der Koalitionsvereinbarung zu beachten, die unter den Maßgaben der verfassungsgerichtlichen Rechtsprechung nach Möglichkeit eine Verbesserung des Schutzniveaus anstrebt. Die Bestimmungen zum Schutz der Berufsgeheimnisträger sollen zunächst - um eine Kollision mit dem staat-

lichen Schutzauftrag für hochwertigste Rechtsgüter zu vermeiden - im Bereich der Datenerhebung installiert werden. Von einer umfassenden Klammerregelung, wie sie die derzeitige Rechtslage noch vorsieht, soll Abstand genommen werden. Der Schutz sowohl der Berufsgeheimnisträger als auch des Kernbereichs privater Lebensgestaltung auf der Anordnungsebene (vor der Anordnung der Überwachungsmaßnahme) und auf der Erhebungsebene (während der laufenden Überwachung, soweit eine unmittelbare Kenntnisnahme erfolgt) wird in den jeweiligen Eingriffsnormen selbst verankert. Nur so ist zum einen eine angemessene Differenzierung nach dem Gewicht der jeweils tangierten Grundrechte und zum anderen eine Berücksichtigung der tatsächlichen und technischen Möglichkeiten möglich. Der Schutz von Vertrauensverhältnissen auf der Verwendungsebene - das heißt wenn es trotz der vorgenannten Schutzmechanismen zu einer Erfassung geschützter Kommunikation gekommen ist - soll hingegen in Form einer einheitlichen Klammerregelung erfolgen.

Für die längerfristige Observation, die Aufzeichnung des nichtöffentlich gesprochenen Wortes außerhalb von Wohnungen und für den Einsatz von verdeckten Ermittlern wird entsprechend den Forderungen des Verfassungsgerichtshofs - wie bisher schon für die Telekommunikationsüberwachung und für die Wohnraumüberwachung - ein Richtervorbehalt vorgesehen.

Der Kritik des Verfassungsgerichtshofs an den Bestimmungen zur nachträglichen Benachrichtigung der von verdeckten Datenerhebungen betroffenen Personen soll dadurch Rechnung getragen werden, dass das endgültige Absehen von der Benachrichtigung generell nur noch nach richterlicher Entscheidung erfolgen darf. Diese Entscheidung kann darüber hinaus erst fünf Jahre nach Beendigung der Maßnahme getroffen werden.

2.
Mit dem Beschluss des Bundesverfassungsgerichts vom 24. Januar 2012, Az.: 1 BvR 1299/05, (Bestandsdatenspeicherung) wurde die bisherige Ausgestaltung des Zugriffs der Sicherheitsbehörden auf Bestandsdaten in § 113 des Telekommunikationsgesetzes (TKG) für teilweise verfassungswidrig erklärt. Betroffen davon ist auch das in der polizeilichen Praxis eminent wichtige Problem der Auskunftserteilung über den Inhaber einer dynamischen IP-Adresse. Nach dem vom Bundesverfassungsgericht vorgegebenen "Doppeltürmodell" besteht Anpassungsbedarf auch im Landesrecht (BVerfG, a. a. O., Rn. 167, nach juris). Das vorliegende Gesetz schafft mit dem neu aufgenommenen § 34 e PAG die geforderte spezifische Rechtsgrundlage im Landesrecht.

3.
In den vergangenen Jahren ist im Rahmen der Vorbereitung verschiedener Großveranstaltungen ein sogenanntes Akkreditierungsverfahren als Bestandteil des Sicherheitskonzepts durchgeführt worden. Alle Personen, die Zugang zu besonders geschützten Bereichen der Stadien hatten (z. B. Pressevertreter, Ordner, Caterer, private Sicherheitsdienste), mussten dabei eine Sicherheitsüberprüfung durch die Polizei- und Verfassungsschutzbehörden durchlaufen. Diese Praxis hat sich weitgehend bewährt. Um dieses Verfahren auf eine gesicherte Rechtsgrundlage zu stellen, sieht das vorliegende Gesetz die Schaffung einer speziellen Befugnisnorm für die Datenübermittlung durch die Polizei an die Veranstalter vor. Damit wird auch einer seit längerem erhobenen Forderung der Datenschutzbeauftragten des Bundes und der Länder Rechnung getragen.

4.
Mit dem Beschluss 2008/615/JI des Rates vom 23. Juni 2008 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität (ABl. L 210 vom 6.8.2008, S. 1) - Ratsbeschluss Prüm - sind weitgehend die Regelungen des am 27. Mai 2005 in Prüm/Eifel unterzeichneten Vertrages zwischen dem Königreich Belgien, der Bundesrepublik Deutschland, dem Königreich Spanien, der Französischen Republik, dem Großherzogtum Luxemburg, dem Königreich der Niederlande und der Republik Österreich zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus, der grenzüberschreitenden Kriminalität und der illegalen Migration (Prümer Vertrag) in den Rechtsrahmen der Europäischen Union überführt worden. Ratsbeschlüsse sind für die Mitgliedstaaten grundsätzlich verbindlich, entfalten jedoch keine unmittelbare Wirkung und bedürfen deshalb der innerstaatlichen Umsetzung.

Auf Bundesebene ist der Ratsbeschluss Prüm mit dem Ausführungsgesetz zum Prümer Vertrag und zum Ratsbeschluss Prüm vom 10. Juli 2006 (BGBl. I S. 1458, 2007 II S. 857), geändert durch Gesetz vom 31. Juli 2009 (BGBl. I S. 2509) vollumfänglich umgesetzt worden.

Allerdings reicht diese Anwendbarkeitsbestimmung des § 1 des Ausführungsgesetzes zum Prümer Vertrag und zum Ratsbeschluss Prüm nur soweit wie die Gesetzgebungskompetenz des Bundes. Die Übermittlung ländereigener Daten ins Ausland zur Gefahrenabwehr und damit auch zur Verhütung von Straftaten erfolgt auf der Grundlage der materiellen Befugnisregelungen in den Polizeigesetzen der Länder. § 3 Abs. 2 und 3 des Bundeskriminalamtsgesetzes (BKAG), nach denen die Polizeien der Länder Datenübermittlungen ins Ausland grundsätzlich über das Bundeskriminalamt abzuwickeln haben, enthält lediglich eine (verfahrensrechtliche) Regelung über den einzuhaltenden Dienstweg, regelt die Datenübermittlung aber nicht in materieller Hinsicht. Darüber hinaus sind unmittelbare Datenübermittlungen ins Ausland nach § 3 Abs. 3 BKAG bei regionaler Kriminalität sowie bei Gefahr im Verzug inzwischen gängige Praxis. § 14 BKAG wiederum, der die Voraussetzungen für die Datenübermittlung ins Ausland durch das Bundeskriminalamt regelt, betrifft nur die Fälle, in denen das Bundeskriminalamt in eigener Zuständigkeit Daten aus den eigenen Datenbeständen übermittelt.

Die Regelungen des Ratsbeschlusses Prüm, die nicht von der Gesetzgebungskompetenz des Bundes umfasst sind, werden durch eine entsprechende Anwendbarkeitsbestimmung im vorliegenden Gesetz in nationales Recht umgesetzt. Die vollständige Umsetzung des Ratsbeschlusses Prüm auch auf Landesebene ist zweckmäßig und erforderlich, um die Möglichkeiten des Ratsbeschlusses Prüm umfassend ausschöpfen zu können.

5.
Der Rahmenbeschluss 2006/960/JI des Rates vom 18. Dezember 2006 über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union (ABl. L 386 vom 29.12.2006, S. 89, L 75 vom 15.3.2007, S. 26) - Schwedische Initiative - wurde am 18. Dezember 2006 vom Europäischen Rat angenommen.

Der Beschluss basiert auf dem Grundsatz, Strafverfolgungsbehörden eines anderen Mitgliedstaats unter den gleichen Bedingungen Zugang zu

vorhandenen Informationen zu gewähren wie innerstaatlichen Strafverfolgungsbehörden. Das sich aus diesem Grundsatz ergebende Diskriminierungsverbot darf nur im Falle des Vorliegens ausdrücklich im Rahmenbeschluss genannter Gründe durchbrochen werden. Dadurch wird der Datenaustausch zwischen den Mitgliedstaaten der Europäischen Union auf neue Grundlagen gestellt.

Gleichzeitig enthält der Rahmenbeschluss Regelungen zu Beantwortungsfristen, die selbst im Vergleich zum innerstaatlichen Datenverkehr neue Maßstäbe setzen. Aus den Mitgliedstaaten der Europäischen Union eingehende Ersuchen sollen in Eilfällen innerhalb von acht Stunden, regelmäßig immerhin in einer Woche und maximal innerhalb von zwei Wochen bearbeitet werden. Können die Fristen nicht eingehalten werden, muss der ersuchende Staat davon in Kenntnis gesetzt werden. Hinsichtlich der Kommunikationswege für den grenzüberschreitenden Datenaustausch lässt der Rahmenbeschluss den Mitgliedstaaten die Wahl zwischen sämtlichen für die internationale Zusammenarbeit im Bereich der Strafverfolgung verfügbaren Kanälen.

Mit dem vorliegenden Gesetz sollen die Regelungen des Rahmenbeschlusses auf Landesebene umgesetzt werden. Die bestehenden Regelungen des Polizeiaufgabengesetzes enthalten zwar bereits eine Reihe von Bestimmungen zum Austausch von Informationen und Erkenntnissen einschließlich personenbezogener Daten im Bereich der grenzüberschreitenden Zusammenarbeit zur Verhütung von Straftaten. Ebenso ist durch das Thüringer Gesetz zur Änderung sicherheits- und verfassungsschutzrechtlicher Vorschriften vom 16. Juli 2008 (GVBl. S. 245) mit § 41 Abs. 1 Satz 2 eine Gleichstellungsregelung eingefügt worden. Regelungsbedarf besteht aber weiterhin für die im Rahmenbeschluss genannten Ausnahmetatbestände, bei deren Vorliegen eine Übermittlung der Daten verweigert werden kann, sowie für die Bestimmungen des Rahmenbeschlusses, die die weitere Verarbeitung der übermittelten Daten regeln.

6.
Der Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (ABl. L 350 vom 30.12.2008, S. 60) - Rahmenbeschluss Datenschutz - zielt darauf ab, die Zusammenarbeit zwischen den Mitgliedstaaten der Europäischen Union zu verbessern. Der Rahmenbeschluss Datenschutz stellt auf den Schutz sämtlicher personenbezogenen Daten ab, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit zwischen den Mitgliedstaaten der Europäischen Union in Strafsachen verarbeitet werden. Mit dem Beschluss werden formelle und materielle Voraussetzungen zur Verarbeitung von Daten geregelt, die zur Verhinderung oder Verhütung von Straftaten

a) aus dem EU-Ausland, von EU-Institutionen oder von Schengen-assoziierten Staaten übermittelt wurden oder
b) ins EU-Ausland, an EU-Institutionen oder in Schengen-assoziierte Staaten zu übermitteln sind

und zwar ab dem Zeitpunkt, zu dem sie tatsächlich übermittelt oder bereitgestellt werden.

Mit dem vorliegenden Gesetz werden die Regelungen des Rahmenbeschlusses auf Landesebene umgesetzt. Umsetzungsbedarf besteht auf Landesebene, soweit das Polizeiaufgabengesetz und das Thüringer Datenschutzgesetz nicht bereits Regelungen enthalten, die den Anforde-

rungen des Rahmenbeschlusses gerecht werden. So enthält der Rahmenbeschluss beispielsweise strengere Zweckbindungsvorschriften für übermittelte Daten und konkrete Vorgaben, unter welchen Voraussetzungen übermittelte Daten an Dritte weitergeleitet werden dürfen. Ebenfalls regelungsbedürftig sind die Kennzeichnungspflichten für übermittelte Daten sowie die verpflichtende Beachtung mitgeteilter Bedingungen und besonderer Verarbeitungsbeschränkungen, insbesondere Fristen, nach deren Ablauf die Daten zu löschen, zu sperren oder auf die Erforderlichkeit ihrer fortgesetzten Speicherung zu prüfen sind.

7.
Der vorliegende Entwurf verfolgt den Zweck, den Gemeinden, Verwaltungsgemeinschaften oder erfüllenden Gemeinden als Maßnahme der Gefahrenvorsorge eine Handhabe zur Verfügung zu stellen, um vor allem Kinder und Jugendliche vor Gefahren zu schützen, die vom Alkoholkonsum im öffentlichen Raum ausgehen. Daher soll besonders in der Nähe von Einrichtungen, wie Schulen, Kindergärten und Kinderspielplätzen der Konsum von Alkohol verboten werden können. Die Gemeinden erhalten ferner die Möglichkeit, in weiteren Gemeindegebietsteilen mit erhöhtem Gefährdungspotenzial Alkoholverbotszonen durch ordnungsbehördliche Verordnung einzurichten, um alkoholbedingten Straftaten und Ordnungswidrigkeiten wirksam entgegentreten zu können.

Kommunale Alkoholverbote können nicht auf der Grundlage der Generalklausel zum Erlass von ordnungsbehördlichen Verordnungen verhängt werden. Nach der Rechtsprechung (vergleiche VGH Mannheim, Urteil v. 28.7.2009, Az.: 1 S 2200/08, NVwZ-RR 2010, 55, 56) wären sie nur zulässig, wenn hinreichende Anhaltspunkte vorhanden wären, dass der Konsum von Alkohol regelmäßig und typischerweise zum Eintritt von Schäden führt. Das Konsumieren von Alkohol stelle noch keine Gefahr für die öffentliche Sicherheit und Ordnung dar, vielmehr liege lediglich ein Gefahrenverdacht oder Besorgnispotenzial vor. Vorsorgemaßnahmen zur Abwehr möglicher Beeinträchtigungen im Gefahrenvorfeld bedürften aber einer speziellen Ermächtigungsgrundlage.

Das Oberverwaltungsgericht Weimar hat sich mit Urteil vom 21. Juni 2012 (Az.: 3 N 653/09) dieser Rechtsprechung angeschlossen und zur Alkoholverbotsregelung in der Erfurter Stadtordnung ausgeführt, dass der Erlass einer solchen Verbotsregelung nicht auf § 27 Abs. 1 Ordnungsbehördengesetz (OBG) gestützt werden könne, denn nur durch das Trinken von Alkohol in der Öffentlichkeit entstehe noch keine allgemeine Gefahrenlage (abstrakte Gefahr), d. h. eine Sachlage, bei der im einzelnen Fall die hinreichende Gefahr dafür besteht, dass in absehbarer Zeit ein Schaden für die öffentliche Sicherheit oder Ordnung eintreten wird. Der Umstand, dass viele, die Ordnungswidrigkeiten und Straftaten begingen, betrunken seien, rechtfertige nicht die Annahme, dass jeder Ordnungswidrigkeiten und Straftaten begehe, der Alkohol zu sich nehme. In Fällen, in denen lediglich ein Gefahrenverdacht oder Gefahrenpotenzial bestehe, sei der Anwendungsbereich des § 27 Abs. 1 OBG aber nicht eröffnet.

Die Kompetenz, Maßnahmen zu treffen, die lediglich der Gefahrenvorsorge dienen, habe, führt das Gericht weiter aus, allein der Gesetzgeber. Dieser könne gesetzliche Regelungen schaffen, durch die er entweder selbst Maßnahmen der Gefahrenvorsorge treffe oder durch die er den Behörden eine Ermächtigung erteile, ordnungsbehördliche Verordnungen unter bestimmten Voraussetzungen auch zur (bloßen) Gefahrenvorsorge zu erlassen. Das Gericht hat jedoch auch die Grenzen

einer gesetzlichen Regelung aufgezeigt. Eine solche sei nur möglich in den Schranken der verfassungsmäßigen Ordnung (Art. 20 Abs. 3 GG), insbesondere unter Wahrung der Grundrechte, namentlich der Freiheitsrechte (vgl. Art. 2 Abs. 1 GG).

B. Zu den einzelnen Bestimmungen

Zu Artikel 1

Zu Nummer 1 (§ 5)

Die Änderung der Überschrift und die Aufhebung der Absätze 3 bis 6 sind aus der erforderlichen Neugestaltung des Berufsgeheimnisträgerschutzes resultierende Folgeänderungen.

Der Verzicht auf die bislang in Absatz 7 enthaltene Definition des Kernbereichs privater Lebensgestaltung erfolgt in Reaktion auf die Ausführungen im Urteil des Thüringer Verfassungsgerichtshofs vom 21. November 2012 (a. a. O. Rn. 242, nach juris), der klargestellt hat, dass der Gesetzgeber von der Verfassung her nicht verpflichtet ist, den Kernbereich privater Lebensgestaltung zu definieren, und zudem darauf hinwies, dass eine abschließende abstrakte Definition auch kaum möglich sein wird.

Zu Nummer 2 (§ 19)

Aus der Aufgabe der Straftatenkataloge resultierende Folgeänderung

Zu Nummer 3 (§ 31)

Mit der Änderung des Polizeiaufgabengesetzes im Jahr 2008 wurde in Absatz 5 ein umfangreicher zweistufiger Straftatenkatalog eingeführt, der die Begriffe der schweren Straftat und der besonders schweren Straftat legal definieren sollte, die bei verschiedenen Eingriffsbefugnissen als Tatbestandsmerkmale herangezogen wurden. Den Katalogen lag kein speziell auf die Gefahrenabwehr abgestimmtes Konzept zu Grunde, es handelte sich vielmehr um eine inhaltsgleiche Übernahme der in den strafprozessualen Bestimmungen für die Telekommunikationsüberwachung (§ 100a StPO) und die Wohnraumüberwachung (§ 100c StPO) enthaltenen Kataloge.

Bereits das Bundesverfassungsgericht hat im Beschluss zur Vorratsdatenspeicherung (BVerfG vom 28. Oktober 2008, Az.: 1 BvR 256/08) grundsätzliche Zweifel an der Eignung von Straftatenkatalogen bei der Bestimmung von Eingriffsvoraussetzungen für präventives Handeln ausgesprochen.

Der Thüringer Verfassungsgerichtshof hat diesen Ansatz weiter vertieft und dabei insbesondere auch die Auswirkungen der unveränderten Übernahme strafprozessualer Tatbestandsmerkmale im Gefahrenabwehrrecht dargestellt (a. a. O., Rn. 227 ff, nach juris). Letztlich kam er zum Schluss, dass das Gebot der Normenklarheit und Bestimmtheit dem Gesetzgeber bei der Verweisung auf Straftatenkataloge enge Grenzen setzt, wenn er präventiv-polizeiliche Befugnisse regeln will. Der Charakter der Gefahrenabwehr als Rechtsgüterschutz verlange, dass bei der Normierung von Grundrechtseingriffen die zu schützenden Rechtsgüter und die Intensität ihrer Gefährdung in den Blick genommen würden.

Das vorliegende Gesetz gibt daher den Straftatenkatalog des § 31 Abs. 5 auf, weil nach der Entscheidung des Thüringer Verfassungsgerichtshofs kein sinnvoller Anwendungsbereich mehr verbleibt:

a) die Bestimmung zur Gewahrsamnahme zur Verhütung bzw. Unterbindung einer Straftat (§ 19 Abs. 1 Nr. 2) ist auch ohne den Katalog vollziehbar,
b) zur Situation bei der polizeilichen Beobachtung (§ 37) wird auf die Ausführungen zu Artikel 1 Nr. 11 verwiesen und
c) die Bestimmung zur Rasterfahndung wurde durch den Verfassungsgerichtshof nicht betrachtet.

Allerdings wird in der Norm ebenfalls auf einen Straftatenkatalog Bezug genommen, weshalb eine Überarbeitung erforderlich ist.

Zu Nummer 4 (§§ 34 bis 34 b)

Zu § 34

§ 34 diente bislang neben der Regelung der besonderen Mittel der Datenerhebung an sich auch als Klammerregelung für Verfahrensvorschriften im Zusammenhang mit der nachträglichen Benachrichtigung mit Wirkung für alle verdeckten Datenerhebungen. Mit dem vorliegenden Gesetz wird die Bestimmung auf ihren Regelungskern zurückgeführt; gemeinsam für alle Maßnahmen der verdeckten Datenerhebung geltende Vorschriften werden im neugefassten § 36 geregelt.

Zu Absatz 1

Satz 1 regelt die tatbestandlichen Voraussetzungen für den Einsatz besonderer Mittel der Datenerhebung. Diese dürfen nur zur Abwehr konkreter Gefahren für die genannten hochwertigen Rechtsgüter gegen Störer oder deren Nachrichtenmittler zum Einsatz kommen.

Satz 2 untersagt die Anordnung, wenn im Zuge der vorherigen Prognose tatsächliche Anhaltspunkte dafür vorliegen, dass die Maßnahme ausschließlich Inhalte aus dem Kernbereich privater Lebensgestaltung erfassen würde.

Nach der Rechtsprechung des Bundesverfassungsgerichts haben heimliche Überwachungsmaßnahmen staatlicher Stellen einen unantastbaren Kernbereich privater Lebensgestaltung zu wahren, dessen Schutz sich aus Artikel 1 GG ergibt. Selbst überwiegende Interessen der Allgemeinheit können einen Eingriff in den Kernbereich nicht rechtfertigen. Diesem absoluten Schutz unterfallen vor allem Vorgänge, die das Wesen der jeweiligen Persönlichkeit in ihrem Innersten offenbaren. Der Kernbereich privater Lebensgestaltung ist jedoch erst dann tangiert, wenn das Gespräch tiefste innere Vorgänge privatester Natur offenbart. Es besteht ferner kein Schutz für Kommunikationsinhalte, die in unmittelbarem Bezug zu konkreten gefahrverursachenden Handlungen stehen, wie etwa Angaben über die Planung bevorstehender Straftaten.

Dabei verbietet sich eine schematische Betrachtung; die Bestimmung des Kernbereichs kann unter Berücksichtigung der verfassungsgerichtlichen und höchstrichterlichen Rechtsprechung nur im Einzelfall erfolgen. Hinweise auf eine Nähe zum Kernbereich können vorrangig aus den Kommunikationsthemen, aber auch aus den äußeren Umständen erschlossen werden.

Als inhaltliche Indizien für eine mögliche Kernbereichsrelevanz können folgende Gesprächsthemen angesehen werden: Sexualität und Liebesverhältnisse, schwere lebensbedrohliche Erkrankungen, Religion, Äußerungen von Emotionen (jede Form des "Außer-sich-Seins", Raserei, Traum), Erörterung existenzieller oder familiärer Fragen, die auf keinen Fall nach außen dringen sollen.

Indiziell kann ein besonderes Vertrauensverhältnis zwischen den kommunizierenden Personen sein (zum Beispiel Gespräche mit Familienangehörigen, insbesondere wenn sie im selben Haushalt leben, oder sonstigen engsten Vertrauten und Freunden). Von Bedeutung können das Ausmaß und die Art der im Rahmen der Kommunikation geäußerten Gefühle bzw. deren emotionale Tiefe sein, ebenso wie die Detailtiefe, Intensität und Dauer der Kommunikation zu einem Themenbereich. Beispiele für kernbereichsrelevante Kommunikation können sein:

a) Äußerungen über das Intimleben (Dinge höchstpersönlicher Natur, die gewöhnlich nur bei besonderem Vertrauen und auch nur mit ganz wenigen Personen besprochen werden, zum Beispiel intensive Liebesbezeugungen, Ausdrucksformen der Sexualität),
b) Gespräche mit Vertrauenspersonen und Familienangehörigen, in denen existenzielle Fragen (zum Beispiel Selbstmordgedanken) oder privateste Angelegenheiten (zum Beispiel Abtreibungen) erörtert werden, auch tief empfundene Emotionen,
c) detaillierte Gespräche über die Kommunikationspartner betreffende erhebliche psychische oder physische Krankheiten.

Satz 3 spricht ein Verbot der Inanspruchnahme von Berufsgeheimnisträgern im Sinne der §§ 53 und 53a StPO als Nachrichtenmittler aus. Damit werden sowohl der herausgehobenen Funktion der unterschiedlichen Berufsgeheimnisträger Rechnung getragen als auch die Grundrechte unbeteiligter Dritter effektiv geschützt. Die Eröffnung der Möglichkeit der Überwachung eines Berufsgeheimnisträgers, um auf diesem Wege quasi indirekt an Informationen über den eigentlichen Störer zu gelangen, würde nicht nur die in weiten Teilen auf Vertrauen basierende Berufsausübung der genannten Berufsgruppen berühren, sondern auch die vertrauliche Kommunikation einer Vielzahl unbeteiligter Dritter (zum Beispiel der sonstigen Mandanten eines Rechtsanwalts) erfassen. Unberührt davon bleibt die Möglichkeit des Handelns gegen einen Berufsgeheimnisträger, der selbst für die Gefahr verantwortlich ist.

Zu Absatz 2

Die Bestimmung benennt die unterschiedlichen Mittel der Datenerhebung.

Zu Absatz 3

Die Bestimmung dient der Sicherung des Schutzes des Kernbereichs privater Lebensgestaltung und der vertraulichen Kommunikation mit Berufsgeheimnisträgern während einer Observation oder eines verdeckten Einsatzes technischer Mittel zum Abhören oder zur Aufzeichnung des nicht öffentlich gesprochenen Wortes. Kommt es im Verlauf der Maßnahme zur Berührung des Kernbereichs privater Lebensgestaltung oder geschützter Vertrauensverhältnisse, ist die unmittelbare Kenntnisnahme (Mithören, Beobachten) zu unterbrechen. Eine Fortsetzung der unmittelbaren Kenntnisnahme ist erst zulässig, wenn der Kernbereich bzw. das Vertrauensverhältnis voraussichtlich nicht mehr betroffen ist. Für den Fall, dass die Inhalte der Gespräche die bevorstehende Verletzung

hochwertiger Rechtsgüter zum Gegenstand haben, liegt diesbezüglich kein Kernbereich und folglich auch kein schutzwürdiges Vertrauensverhältnis vor (vergleiche BVerfGE 80, 367). Diese Wertung war für die nicht als Ausdruck der Menschenwürde geschützten Vertrauensverhältnisse zu Berufsgeheimnisträgern zu übernehmen (Satz 1 Nr. 3). Anders verhält es sich nur bei Gesprächen mit einem Geistlichen (Satz 1 Nr. 2). Die Inhalte dieser Gespräche gehören zum Menschenwürdegehalt und sind dem staatlichen Zugriff daher entzogen. So gehört der Schutz der Beichte oder der Gespräche mit Beichtcharakter zum verfassungsrechtlichen Menschenwürdegehalt der Religionsausübung im Sinne des Artikels 4 Abs. 1 und 2 GG (BVerfG, Urteil vom 03.03.2004, Az.: 1 BvR 2378/93, NJW 2004, S. 999, 1004). Eine Fortsetzung der unmittelbaren Kenntnisnahme ist erst zulässig, wenn der Kernbereich mit hoher Wahrscheinlichkeit nicht mehr betroffen ist.

Häufig wird die Polizei nicht sofort zuverlässig erkennen können, ob insbesondere der Kernbereich privater Lebensgestaltung betroffen ist (siehe hierzu auch die Ausführungen bei Absatz 1). Dies gilt vor allem dann, wenn die Kommunikation in einer Fremdsprache geführt wird. Bestehen seitens der Polizei Zweifel, ob die erfassten Inhalte tatsächlich dem Kernbereich privater Lebensgestaltung zuzuordnen sind, kann eine automatisierte Aufzeichnung fortgesetzt werden. Gerade zu Beginn einer Maßnahme oder eines Ermittlungskomplexes wird die zutreffende Einordnung der Gesprächsinhalte zunächst schwerfallen. Erst mit einem gewissen Überblick über das Kommunikationsverhalten der Betroffenen wird es möglich sein, eine bewusste "Vertarnung" unmittelbar gefahrenbezogener Inhalte zu erkennen. Daneben wird es auch darum gehen, sprachliche Besonderheiten wie floskelhafte religiöse Beteuerungen oder sexuelle Prahlereien ohne emotionale Beteiligung (beispielsweise im Rotlichtmilieu) von echten Kernbereichsinhalten zu unterscheiden. Ebenso müssen zunächst Erkenntnisse über das persönliche Umfeld der Betroffenen gewonnen werden, um zu erkennen, wer zum engeren Familienkreis und zu den Vertrauenspersonen gehört, bei denen eine Offenbarung kernbereichsrelevanter Inhalte in Frage kommt.

Zweifelsfälle können sich vor allem auch ergeben, wenn Kommunikationsvorgänge mit Berufsgeheimnisträgern erfasst werden. Der Umstand, dass der Störer Kontakt mit einem Berufsgeheimnisträger aufnimmt, ist für sich betrachtet ein Indiz dafür, dass möglicherweise ein geschütztes Vertrauensverhältnis berührt sein könnte. Ob dem tatsächlich so ist, hängt allerdings von den konkreten Inhalten ab.

Diese automatischen Aufzeichnungen dürfen durch die Polizei jedoch erst nach Freigabe durch den anordnenden Richter verwendet werden (dies kommt bei einer Observation nicht in Betracht). Für den Fall, dass die Inhalte der Gespräche die bevorstehende Verletzung hochwertiger Rechtsgüter zum Gegenstand haben, liegt diesbezüglich kein Kernbereich und folglich auch kein schutzwürdiges Vertrauensverhältnis vor (vergleiche BVerfG, Beschluss vom 14.9.1989, Az.: 2 BvR 1062/87, BVerfGE 80, 367). Eine Fortsetzung der unmittelbaren Kenntnisnahme ist erst zulässig, wenn der Kernbereich mit hoher Wahrscheinlichkeit nicht mehr betroffen ist. Etwaige automatische Aufzeichnungen dürfen durch die Polizei erst nach Freigabe durch den anordnenden Richter verwendet werden (dies kommt bei einer Observation nicht in Betracht).

Die nach Absatz 2 Nr. 3 bis 5 eingesetzten Personen handeln mit Sozialbezug. Sie agieren und kommunizieren offen, lediglich ihre Zusammenarbeit mit der Polizei ist unbekannt. Vertrauliches wird ihnen freiwillig

mitgeteilt. Ein verfahrensmäßiger Kernbereichs- oder Vertrauensverhältnisschutz kann daher hier nicht eingreifen.

Zu den Absätzen 4 und 5

Die Bestimmung regelt die Anordnung der Maßnahmen. Im Gegensatz zur bisherigen Rechtslage, die die Anordnungen lediglich unter Behördenleitervorbehalt stellte, fordert das vorliegende Gesetz für die längerfristige Observation, den Einsatz technischer Mittel außerhalb von Wohnungen und für den Einsatz eines verdeckten Ermittlers grundsätzlich die Anordnung durch den Richter. Für Fälle von Gefahr im Verzug wird der Polizei ein Eilanordnungsrecht eröffnet. Mit der Einführung des Richtervorbehalts wird den diesbezüglichen Forderungen des Verfassungsgerichtshofs entsprochen, der insbesondere mit Blick auf die Eingriffsschwere und unter Hinweis auf die Ausgestaltung der vergleichbaren Regelungen in der Strafprozessordnung eine Einbindung des Richters angemahnt hatte.

Zu Absatz 6

Die Bestimmung enthält die bisher in § 36 getroffenen ergänzenden Verfahrensregelungen zum Einsatz verdeckter Ermittler.

Zu § 34 a

Die Bestimmung zur präventiv-polizeilichen Telekommunikationsüberwachung wurde infolge des Urteils des Thüringer Verfassungsgerichtshofs sowohl im Hinblick auf die Ausgestaltung des Tatbestands als auch hinsichtlich der Regelungen zum Umgang mit schutzwürdiger Kommunikation überarbeitet. Bislang waren in § 34 a eine Vielzahl unterschiedlicher Eingriffsbefugnisse in einer Norm zusammengefasst, was die Anwendung der Norm sowohl für die Vollzugspraxis als auch für die Gerichte in der Vergangenheit nicht immer einfach gestaltete. Insoweit erfolgt mit dem vorliegenden Entwurf eine Neugliederung der Eingriffsbefugnisse mit Bezug zum Fernmeldegeheimnis. § 34 a deckt nach dem neuen Regelungskonzept künftig ausschließlich den Bereich der Inhaltsüberwachung ab.

Zu Absatz 1

Die Bestimmung enthält - im Grundaufbau § 34 Abs. 1 folgend - die Tatbestandsmerkmale und die wesentlichen Schutzvorkehrungen für den Kernbereich privater Lebensgestaltung und zum Schutz der Berufsgeheimnisträger auf der Anordnungsebene.

Die Tatbestandsalternative in Satz 1 Nr. 3 deckt eine Fallkonstellation ab, die so nur bei der Telekommunikationsüberwachung auftreten kann. Neben der direkten Überlassung von Kommunikationsgeräten durch Unbeteiligte ist vor allem an die Nutzung von mehreren Personen zugänglichen Endgeräten (Vereinsheime, Gaststätten, studentische Wohngemeinschaften etc.) zu denken.

Der Kernbereichsschutz ist auf der Anordnungsebene schwächer ausgeprägt als bei der Wohnraumüberwachung. Dies ist vor allem dem Umstand geschuldet, dass im Vorfeld der Maßnahme kaum eine Prognose über einen möglichen Kernbereichsbezug der Kommunikationsinhalte möglich ist. Eine inhaltsgleiche Regelung enthält § 34 b Abs. 1 Satz 1 in der bisherigen Fassung; diese Norm wurde durch den Verfassungs-

gerichtshof ausdrücklich nicht beanstandet (a. a. O. Rn. 251, nach juris). Der Berufsgeheimnisträgerschutz folgt dem gleichen Modell wie in § 34: eine Inanspruchnahme als Nachrichtenmittler ist ausgeschlossen. Maßnahmen gegen Berufsgeheimnisträger, die selbst für die Gefahr verantwortlich sind, unterliegen hingegen keinen Einschränkungen.

Zu den Absätzen 2 und 3

Die Bestimmungen eröffnen die Möglichkeit zur sogenannten Quellen-Telekommunikationsüberwachung. Die bereits nach der bisherigen Rechtslage bestehende Befugnis (§ 34 a Abs. 2 Satz 2 a. F.) wird ohne inhaltliche Änderungen mit den speziellen Verfahrensbestimmungen (§ 34 b Abs. 5 und 6 a. F.) in den neu gefassten § 34 a überführt.

Zu Absatz 4

Die Bestimmung regelt den Schutz des Kernbereichs privater Lebensgestaltung und der Kommunikation mit Berufsgeheimnisträgern während der laufenden Überwachungsmaßnahme. Die Bestimmung ordnet, wie auch § 34 Abs. 3, eine Unterbrechung der unmittelbaren Kenntnisnahme an, wenn der Kernbereich privater Lebensgestaltung oder die vertrauliche Kommunikation mit Berufsgeheimnisträgern berührt wird. Eine Unterbrechung der Aufzeichnung wird hingegen nicht angeordnet, weil eine solche Anordnung nach den technischen Gegebenheiten bei der Telekommunikationsüberwachung wirkungslos bliebe. Die Telekommunikationsüberwachung erfolgt unter Mithilfe der Telekommunikationsunternehmen, die bei Vorliegen einer entsprechenden richterlichen Anordnung durch § 110 des Telekommunikationsgesetzes (TKG) in Verbindung mit den Bestimmungen der Telekommunikations-Überwachungsverordnung zur Übermittlung einer Kopie der zu überwachenden Kommunikation an die berechtigte Stelle verpflichtet sind. Insoweit erfolgt über die gesamte Laufzeit der Anordnung zwangsweise eine Aufzeichnung der Kommunikationsinhalte, die durch die Polizei nicht unterbrochen werden kann. Auch für den Bereich der sogenannten Quellen-Telekommunikationsüberwachung wird nach derzeitigem Stand davon ausgegangen, dass eine Möglichkeit zur Unterbrechung der Aufzeichnung nicht bestehen wird. Die bisherige Debatte über den sogenannten "Staatstrojaner" hat gezeigt, dass jegliche Einwirkungsmöglichkeit des Staates auf das zu überwachende System durch die Fachwelt und durch die kritische Öffentlichkeit mit einem hohen Maß an Skepsis betrachtet wird. Eben eine solche "Fernsteuerungsmöglichkeit" der Überwachungssoftware und damit auch ein zusätzlicher Eingriff in das zu überwachende System wären allerdings wohl vonnöten, wenn eine Möglichkeit zur temporären Unterbrechung der Übertragung geschaffen werden sollte.

Findet kein unmittelbares Mithören statt, so ist auf der Erhebungsebene keine Einwirkungsmöglichkeit auf den Überwachungsvorgang vorhanden. Die Verwirklichung des Kernbereichsschutzes geht dann sofort auf die Verwendungsebene (§ 36, insbesondere Absatz 2) über.

Zu den Absätzen 5 und 6

Die Bestimmungen regeln die Anordnungskompetenz und die formalen Anforderungen an die Anordnung.

Zu Absatz 7

Die Bestimmung regelt die Mitwirkungspflichten der Telekommunikationsunternehmen und erklärt die Regelungen des Justizvergütungs- und

Entschädigungsgesetzes hinsichtlich der Entschädigung für die Mitwirkung für anwendbar.

Zu § 34 b

Die Bestimmung regelt den Zugriff auf Telekommunikationsverkehrsdaten und auf Nutzungsdaten von Telemediendiensten.

Zu Absatz 1

Die Bestimmung legt die Tatbestandsvoraussetzungen für den Zugriff der Polizei auf Telekommunikationsverkehrsdaten fest. Die tatbestandlichen Anforderungen sind dabei grundsätzlich die gleichen wie bei der Inhaltsüberwachung. Satz 1 Nr. 4 erfasst die in der polizeilichen Praxis häufigen Fälle der Ortung von Mobiltelefonen. Da insbesondere bei vermissten Personen zum Zeitpunkt der Anordnung noch nicht klar sein wird, ob sich diese aufgrund des eigenen Verhaltens in einer Gefahrenlage befinden oder die Gefährdung durch Dritte ausgelöst wird, erfolgt die Regelung in einer eigenen Tatbestandsalternative.

Eine Bestimmung zum Kernbereichsschutz ist entbehrlich, da Verbindungsdaten zwar durchaus tiefe Einblicke in das Kommunikationsverhalten des Betroffenen erlauben, dabei jedoch mangels Offenbarung von Kommunikationsinhalten der Kernbereich privater Lebensgestaltung niemals betroffen sein kann. Anders liegt es hingegen bei Berufsgeheimnisträgern. Insbesondere bei Berufsgruppen wie Journalisten oder zum Teil auch Abgeordneten kann der Zugriff auf Verkehrsdaten zur Offenlegung des gesamten Quellennetzes führen und damit die Berufsausübung erheblich beeinträchtigen. Dieser Eingriff ist mit Blick auf das Gewicht der Schutzgüter nur in den Fällen zu rechtfertigen, in denen der Berufsgeheimnisträger selbst für die Gefahr verantwortlich ist.

Zu Absatz 2

Die Bestimmung regelt die Voraussetzungen des Zugriffs auf Nutzungsdaten von Telemediendiensten. Nach § 15 des Telemediengesetzes (TMG) sind Nutzungsdaten insbesondere Merkmale zur Identifikation des Nutzers, Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und Angaben über die vom Nutzer in Anspruch genommenen Telemedien. Der Zugriff der Polizei auf diese Daten erfolgt bisher auf der Grundlage der Generalklausel zur Datenerhebung (§ 32) in Verbindung mit §§ 15 Abs. 5 Satz 4 und § 14 Abs. 2 TMG. An dieser Ausgestaltung des Zugriffs wurde in letzter Zeit in der Literatur immer mehr Kritik geübt. Insbesondere wurde dabei vorgetragen, dass ein Zugriff auf Telemedieninhalte zwingend die Inanspruchnahme von Telekommunikationsdiensten voraussetze und insoweit eine Nähe zum Fernmeldegeheimnis gegeben sei. Das vorliegende Gesetz trägt dieser Auffassung Rechnung und macht den Zugriff auf Telemediendaten von den gleichen Voraussetzungen abhängig, wie sie für den Zugriff auf Telekommunikationsverkehrsdaten vorliegen müssen.

Zu Absatz 3

Die Bestimmung verweist hinsichtlich der Anordnung der Maßnahme auf § 34 a Abs. 5 und 6. Satz 2 enthält für die Fälle der nichtindividualisierten Verkehrsdatenabfrage ("Funkzellenabfrage") eine Sonderregelung hinsichtlich des Anordnungsinhalts. In den in Rede stehenden Fällen ist die Rufnummer bzw. die Gerätekennung noch nicht bekannt, sondern soll erst durch den Abgleich von Verkehrsdaten ermittelt werden. An die

Stelle der entsprechenden Angaben in der Anordnung tritt daher eine möglichst enge räumliche und zeitliche Eingrenzung der Kommunikation, zu der Verkehrsdaten übermittelt werden sollen.

Zu Nummer 5 (§§ 34 c bis 34 e)

Zu § 34 c

Die Bestimmung erfasst den bisher in § 34 a Abs. 2 Satz 1 Nr. 2 und 3 a.F. geregelten Einsatz des IMSI-Catchers.

Zu § 34 d

Die Bestimmung erfasst die bisher in § 34 a Abs. 4 a. F. geregelte Befugnis zur Unterbrechung beziehungsweise Verhinderung von Telekommunikation. Abweichend von der bisher geltenden Regelung wird der Richtervorbehalt für die Anordnung aufgegeben, da die Maßnahme nicht zur Erhebung von Daten führen und insoweit erst recht keinen Eingriff in das Fernmeldegeheimnis auslösen kann.

Zu § 34 e

Die Bestimmung setzt die durch das Bundesverfassungsgericht mit dem Beschluss vom 24. Januar 2012, Az.: 1 BvR 1299/05 (Bestandsdatenspeicherung) geforderte Neuregelung des Zugriffs der Sicherheitsbehörden auf Bestandsdaten nach § 113 TKG um. Die Ausgestaltung der Norm orientiert sich an den auf Bundesebene mit dem Gesetz zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Bestandsdatenauskunft für das Bundeskriminalamt und die Bundespolizei geschaffenen Bestimmungen.

Zu Nummer 6 (§§ 35 und 36)

Zu § 35

Die Bestimmung zur Wohnraumüberwachung wird in Hinblick auf die tatbestandlichen Voraussetzungen (Aufgabe der Bezugnahme auf Straftatenkataloge) und bezüglich des Berufsgeheimnisträgerschutzes an die Rechtsprechung des Verfassungsgerichtshofs angepasst. Ansonsten bleibt die Regelung weitgehend unverändert. Die Regelungen zur Unterbrechung bei einem festgestellten oder drohenden Eingriff in ein Vertrauensverhältnis in Absatz 6 wurden an die Systematik in § 34 Abs. 3 und § 34 a Abs. 4 angepasst.

Zu § 36

Im neu gefassten § 36 werden wesentliche für alle Maßnahmen der verdeckten Datenerhebung gemeinsam geltende Vorschriften zusammengefasst.

Zu Absatz 1

Satz 1 schreibt zum einen die besondere Kennzeichnung der durch verdeckte Datenerhebung gewonnenen Erkenntnisse vor. Satz 1 betont den Grundsatz der Zweckbindung; die erhobenen Daten sollen grundsätzlich nur zur Abwehr der Gefahr verwendet werden dürfen, die zur Anordnung der Maßnahme geführt hat. Satz 3 ermöglicht eine Verwendung in

anderen Verfahren nur dann, wenn im Zielverfahren eine verdeckte Datenerhebung hätte angeordnet werden dürfen.

Zu Absatz 2

Absatz 2 stellt die zentrale Norm zum Schutz des Kernbereichs privater Lebensgestaltung und des Vertrauensverhältnisses zu Berufsgeheimnisträgern auf der Verwendungsebene dar. Im Gegensatz zur Prognosesituation vor der Anordnung oder zu den Handlungsmöglichkeiten während der laufenden Überwachung, wo zwischen den unterschiedlichen Überwachungsmaßnahmen differenziert werden kann und muss, kann der Schutz auf der Verwendungsebene durch eine Klammerregelung erfolgen, weil die zu beurteilenden Daten bereits erhoben worden sind.

Die Bestimmung regelt Verwendungsverbote und Löschgebote, falls es zur Erhebung von Daten gekommen sein sollte, die dem Kernbereich privater Lebensgestaltung oder einem Vertrauensverhältnis zu bestimmten Berufsgeheimnisträgern zuzuordnen sind. Es sind beispielsweise Fälle denkbar, in denen eine Kernbereichsrelevanz zum Zeitpunkt der Erhebung nicht erkannt wird, da die Gespräche in einer Fremdsprache geführt werden und die Kernbereichsrelevanz erst nach Übersetzung durch einen Dolmetscher zu Tage tritt. Nach dem Entwurf wird ein Verwendungsverbot, das mit dem Gebot der unverzüglichen Löschung gekoppelt ist, für diese Inhalte statuiert.

Satz 3 erlaubt eine ausnahmsweise Verwendungsmöglichkeit zur Abwehr einer gegenwärtigen Gefahr für Leben oder Freiheit einer Person. Ein Untätigbleiben der Polizei bei einer solchen Gefahrenlage für höchste Rechtsgüter ist hinsichtlich der staatlichen Schutzpflicht für Leben und Freiheit nicht zu rechtfertigen, wobei die Verwendung der Daten - außer bei Gefahr im Verzug - von einer richterlichen Entscheidung abhängig ist.

Zu den Absätzen 3 bis 5

Die Bestimmungen dienen der nach der Rechtsprechung des Verfassungsgerichtshofs erforderlichen Neugestaltung der nachträglichen Benachrichtigung der von einer verdeckten Datenerhebung betroffenen Personen.

Absatz 3 bestimmt den Kreis der Benachrichtigungsadressaten. Satz 3 trifft eine Sonderregelung für ein Unterlassen der Benachrichtigung bei zufällig Betroffenen Personen, die insbesondere bei Telekommunikationsüberwachungen häufig zu verzeichnen sind. Satz 4 gibt die Kriterien vor, die vor der Einleitung von Schritten zur Ermittlung der Identität eines unbekannten Betroffenen abzuwägen sind. Die Bestimmung geht von dem Grundsatz aus, dass eine Vertiefung des Grundrechtseingriffs nur um der Benachrichtigung willen nach Möglichkeit zu vermeiden ist.

Absatz 4 benennt die Gründe, die eine zeitweilige Zurückstellung der Benachrichtigung tragen können. Bei der Beurteilung der Frage, ob durch die Benachrichtigung die weitere Verwendung einer verdeckt handelnden Personen gefährdet werden könnte, ist eine Einzelfallbetrachtung unter Beachtung der durch den Verfassungsgerichtshof aufgestellten Maßgaben (a. a. O., Rn. 285, nach juris) vorzunehmen. Satz 3 trifft eine Regelung für Fälle, in denen sich den präventiven Maßnahmen ein strafrechtliches Ermittlungsverfahren anschließt. Im Gegensatz zur bisherigen Regelung (§ 34 Abs. 9 Satz 6 a. F.) wird die Verpflichtung zur Benachrichtigung nicht auf die Staatsanwaltschaft übertragen, sondern

verbleibt bei der Polizei. Diese hat sich mit der Staatsanwaltschaft über den Zeitpunkt der Benachrichtigung abzustimmen, um eine Gefährdung des Ermittlungsverfahrens auszuschließen.

Absatz 5 regelt die Einbindung des Richters bei der nachträglichen Benachrichtigung. Satz 1 verkürzt im Vergleich zur bestehenden Rechtslage die Zeitspanne, für die die Polizei die Benachrichtigung aufgrund eigener Entscheidung zurückstellen kann, auf sechs Monate. Jede weitere Zurückstellung bedarf ebenso wie die Entscheidung über das endgültige Absehen von der Benachrichtigung der richterlichen Entscheidung. In Anlehnung an § 20w BKAG wird zudem - obwohl durch den Verfassungsgerichtshof nicht zwingend für notwendig erachtet (a. a. O., Rn. 291 ff, nach juris) - als zusätzliche Sicherung bestimmt, dass die Entscheidung über das endgültige Absehen von der Benachrichtigung erst fünf Jahre nach Beendigung der Maßnahme ergehen darf.

Absatz 6 trifft Regelungen zur Zuständigkeit und zum anzuwendenden Verfahren für richterliche Entscheidungen nach den Absätzen 2 und 5 sowie nach den §§ 34 bis 34 c, 34 e und 35. Im Gegensatz zur bisherigen Rechtslage wird die bisher allgemein gehaltene Verweisung auf das Gesetz über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit (FamFG) konkretisiert. Durch die in Satz 2 zugelassenen Abweichungen werden die Besonderheiten verdeckter polizeilicher Datenerhebungen besser berücksichtigt und damit auch den verschiedentlich aus der gerichtlichen Praxis erhobenen Forderungen entsprochen.

Die Sätze 4 bis 7 eröffnen der Polizei die Möglichkeit, die richterliche Entscheidung im Wege der Beschwerde überprüfen zu lassen. Die Regelung muss im Polizeiaufgabengesetz getroffen werden, weil § 59 Abs. 3 FamFG für die Beschwerdebefugnis einer Behörde eine gesetzliche Regelung fordert. Für die Beschwerde der Betroffenen gegen die gerichtlichen Entscheidungen nach den §§ 34 bis 34 c, 34 e und 35 gelten die allgemeinen Bestimmungen des Buches 1 des FamFG, dabei insbesondere die §§ 58 ff. FamFG.

Absatz 7 führt die bisher an unterschiedlichen Stellen im Gesetz geregelten Berichtspflichten der Landesregierung gegenüber dem Landtag an einer zentralen Stelle zusammen.

Zu Nummer 7 (§ 37)

Die Regelungen zur Ausschreibung zur polizeilichen Beobachtung und zur gezielten Kontrolle sind wegen der Streichung der Straftatenkataloge in § 31 Abs. 5 zu überarbeiten. Die bisherige Differenzierung zwischen polizeilicher Beobachtung und gezielter Kontrolle in tatbestandlicher Hinsicht wird aufgegeben. Zur Auslegung des unbestimmten Rechtsbegriffs der "Straftat von erheblicher Bedeutung" kann die durch Rechtsprechung und Lehre für den Bereich der Strafverfolgung entwickelte Definition herangezogen werden. Danach sind Straftaten von erheblicher Bedeutung, insbesondere Verbrechen sowie schwerwiegende Vergehen, für die allgemein folgende drei Kriterien herangezogen werden:
- die Tat muss mindestens dem Bereich der mittleren Kriminalität zuzuordnen sein,
- sie muss den Rechtsfrieden empfindlich stören und
- dazu geeignet sein, das Gefühl der Rechtssicherheit der Bevölkerung erheblich zu beeinträchtigen (vergleiche BVerfG, Beschluss vom 14. Dezember 2000, Az.: 2 BvR 1741/99, BVerfGE 103, 21 [34]; Ur-

teil vom 12. März 2003, Az. 1 BvR 330/96 u. a. BVerfGE, 107, 299 [322]).

Die erforderliche konkrete Betrachtung nach Art und Schwere der Tat im Einzelfall ist im Vorfeld der Anordnung einer polizeilichen Beobachtung im Gegensatz zur Prognosesituation bei anderen verdeckten Maßnahmen problemlos möglich, weil ein entscheidendes Kriterium der bisherige "kriminelle Werdegang" und damit eine gesicherte Faktenbasis ist.

Absatz 5 trifft eine spezifische Regelung zum Kreis der nachträglich zu benachrichtigenden Personen. Ansonsten gilt über die Verweisung in Satz 2 für die Benachrichtigung die Regelung des § 36.

Zu Nummer 8 (§ 41)

Aus der Schaffung einer gesonderten Regelung zur Umsetzung der Schwedischen Initiative im neu eingefügten § 41 b resultierende Folgeänderung

Zu Nummer 9 (§§ 41 a bis 41 d)

Zu § 41 a

Die Bestimmung ermächtigt die Polizei zur Datenübermittlung an öffentliche oder nichtöffentliche Stellen im Zusammenhang mit der Durchführung sogenannter "Akkreditierungsverfahren" bei Großveranstaltungen. Die Datenübermittlung setzt die vorherige Einwilligung des Betroffenen voraus und ist inhaltlich auf die Aussage beschränkt, ob aus polizeilicher Sicht Sicherheitsbedenken bestehen oder nicht. Weitergehende Informationen, wie zum Beispiel Angaben zu in der Vergangenheit durchgeführten Ermittlungsverfahren, dürfen an die Veranstalter nicht übermittelt werden.

Zu § 41 b

§ 41 b schafft im Anwendungsbereich der Schwedischen Initiative die Befugnis der Polizei, Daten zu Zwecken der Verhütung von Straftaten an Polizeibehörden sowie an sonstige für die Verhütung oder Verfolgung von Straftaten zuständige öffentliche Stellen eines Mitgliedstaates der Europäischen Union oder eines Schengen-assoziierten Staates zu übermitteln. Klarstellend sei in diesem Zusammenhang festgehalten, dass die Staatsanwaltschaften nicht zu den Strafverfolgungsbehörden im Sinne der Schwedischen Initiative zählen.

Zu Absatz 1

Absatz 1 verankert den Gleichbehandlungsgrundsatz für Datenübermittlungen auf Ersuchen eines Mitgliedstaates der Europäischen Union zu Zwecken der Verhütung von Straftaten. Die Regelung tritt an die Stelle des bisherigen § 41 Abs. 1 Satz 2.

Zu Absatz 2

Absatz 2 beruht auf Artikel 5 Abs. 1 und 3 der Schwedischen Initiative und regelt die formellen Anforderungen, die an ein Ersuchen nach § 41 b zu stellen sind.

Zu Absatz 3

Absatz 3 normiert den Gleichbehandlungsgrundsatz für Spontanübermittlungen personenbezogener Daten zur Verhütung von Straftaten im Sinne des Artikels 2 Abs. 2 des Rahmenbeschlusses 2002/584/JI des Rates vom 13. Juni 2002 über den Europäischen Haftbefehl und die Übergabeverfahren zwischen den Mitgliedstaaten (ABl. L 190 vom 18. Juli 2000, S. 1), geändert durch den Rahmenbeschluss 2009/299/JI des Rates vom 26. Februar 2009 (ABl. L 91 vom 27. März 2009, S. 24) und setzt damit Artikel 7 der Schwedischen Initiative um.

Zu Absatz 4

Die Bestimmung ordnet die Dokumentation jedweder Datenübermittlung an. Als weitere datenschutzrechtliche Sicherung wird zudem bestimmt, dass Verwendungsbeschränkungen und Löschfristen an den empfangenden Staat mitzuteilen sind. Dieser ist nach den Artikeln 9, 12 und 16 des Rahmenbeschlusses Datenschutz sowie des Artikels 8 Nr. 4 Satz 3 und 4 der Schwedischen Initiative zur Einhaltung dieser Fristen verpflichtet.

Zu Absatz 5

In Absatz 4 wird ausdrücklich festgelegt, dass die Zulässigkeit der Datenübermittlung an eine Polizeibehörde oder sonstige für die Verhütung oder Verfolgung von Straftaten zuständige öffentliche Stelle eines Mitgliedstaates der Europäischen Union auf Grundlage des § 41 Abs. 4 unberührt bleibt. Hierdurch wird klargestellt, dass § 41 b zwar im Falle der Erfüllung der Anforderungen der Absätze 2 und 3 eine Erleichterung des Informationsaustausches darstellt, zugleich aber keine Erschwerung gegenüber der bisherigen Rechtslage eintreten soll, sofern die in den Absätzen 2 und 3 genannten Voraussetzungen im Einzelfall nicht erfüllt sein sollten.

Zu Absatz 6

Die Absätze 6 und 7 beinhalten die in Artikel 10 Abs. 1 und 2 der Schwedischen Initiative enthaltenen Gründe, aus denen eine Datenübermittlung, die in den Anwendungsbereich des Rahmenbeschlusses fällt, verweigert werden kann bzw. muss. Bei den in Absatz 5 neu eingefügten Verweigerungsgründen handelt es sich um zwingende Verweigerungsgründe.

Absatz 6 Nr. 2 beruht auf Artikel 10 Abs. 1 Buchst. b der Schwedischen Initiative. Danach kann die zuständige Strafverfolgungsbehörde die Datenübermittlung auch dann verweigern, wenn der Erfolg laufender polizeilicher oder staatsanwaltschaftlicher Ermittlungen gefährdet würde.

Absatz 6 Nr. 2 setzt Artikel 1 Abs. 7 der Schwedischen Initiative um, der an die Pflicht der Mitgliedstaaten zur Wahrung der in Artikel 6 des Vertrags über die Europäische Union niedergelegten Grundrechte und allgemeinen Rechtsgrundsätze erinnert.

Absatz 6 Nr. 3 schließt darüber hinaus die Übermittlung von Daten aus, die nicht vorhanden sind und erst durch Zwangsmaßnahmen erhoben werden müssten. Diese Regelung beruht auf Artikel 1 Abs. 5 der Schwedischen Initiative. Danach sind die Mitgliedstaaten nicht verpflichtet, Informationen und Erkenntnisse durch Zwangsmaßnahmen im Sinne des nationalen Rechts zu erlangen. Zwangsmaßnahmen in diesem Sinne sind Maßnahmen, die gegen oder ohne den Willen der betroffenen Person

durchgesetzt werden und die aufgrund des damit einhergehenden wesentlichen Grundrechtseingriffs einer speziellen gesetzlichen Grundlage bedürfen, also nicht auf eine Generalklausel oder vergleichbare Grundnormen gestützt werden können. Dabei ist allerdings zu berücksichtigen, dass das Übermittlungsverbot nicht für bereits "vorhandene" Daten gilt. Zu den vorhandenen Daten zählen grundsätzlich sämtliche Daten der Strafverfolgungsbehörden, also beispielsweise auch INPOL-Dateien.

Zu Absatz 7

Neben den obligatorischen Übermittlungsverboten in Absatz 6 werden in Absatz 7 darüber hinaus fakultative Verweigerungsgründe normiert. Absatz 7 Nr. 1 beruht auf Artikel 3 Abs. 3 in Verbindung mit Artikel 2 Buchst. d der Schwedischen Initiative. Danach erstreckt sich der Gleichbehandlungsgrundsatz lediglich auf die bei den Strafverfolgungsbehörden vorhandenen oder verfügbaren Informationen und Erkenntnisse. Wie bereits ausgeführt, verpflichtet der Rahmenbeschluss die Mitgliedstaaten nicht, Daten durch strafprozessuale oder polizeirechtliche Maßnahmen erst zu erheben. Ziel des Rahmenbeschlusses ist es vielmehr, den grenzüberschreitenden Austausch von bei den Strafverfolgungsbehörden vorhandenen oder für diese ohne Weiteres verfügbaren Informationen zu erleichtern.

Der zweite Verweigerungsgrund ergibt sich aus Artikel 10 Abs. 2 der Schwedischen Initiative. Danach kann die Datenübermittlung auch dann unterbleiben, wenn sie die Verhütung von Straftaten betrifft, die nach deutschem Recht mit einer Freiheitsstrafe von im Höchstmaß einem Jahr oder weniger bedroht sind.

Zu Absatz 8

Absatz 8 regelt, dass als Polizeibehörde oder sonstige für die Verhütung oder Verfolgung von Straftaten zuständige öffentliche Stelle eines Mitgliedstaates der Europäischen Union im Sinne der Absätze 1 und 3 jede von diesem Staat gemäß Artikel 2 Buchst. a der Schwedischen Initiative benannte Stelle gilt.

Zu Absatz 9

Absatz 9 bestimmt, dass die Regelungen des § 41 b auch für die sogenannten Schengen-assoziierten Staaten gelten, also für die Staaten, die die Bestimmungen des Schengen-Besitzstandes aufgrund eines Assoziierungsübereinkommens mit der Europäischen Union über die Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstandes anwenden. Dies entspricht den Vorgaben der Schwedischen Initiative.

Zu § 41 c

Der Rahmenbeschluss Datenschutz und die Schwedische Initiative enthalten beide umsetzungsbedürftige Regelungen, die die Verarbeitung empfangener Daten aus anderen Mitgliedstaaten der Europäischen Union, aus Schengen-assoziierten Staaten sowie von EU-Institutionen im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen betreffen.

Zu Absatz 1

Absatz 1 regelt in Umsetzung von Artikel 11 des Rahmenbeschlusses Datenschutz, dass die innerhalb des Anwendungsbereichs des Beschlus-

ses übermittelten Daten grundsätzlich nur für die Zwecke verarbeitet werden dürfen, für die sie übermittelt wurden, sowie Ausnahmen von diesem Grundsatz, nach dem insbesondere bei Zustimmung des übermittelnden Staates eine Zweckänderung vorgenommen werden darf. Weitere Ausnahmen sind in den Nummern 2 bis 4 geregelt. Nach Nummer 2 ist eine Zweckänderung möglich zur Verhütung von Straftaten, zur Strafverfolgung oder zur Strafvollstreckung, auch wenn es sich nicht um die Straftaten oder Sanktionen handelt, für die die Daten ursprünglich übermittelt wurden. Eine Zweckänderung ist nach Nummer 3 auch für bestimmte justizielle und verwaltungsbehördliche Verfahren möglich. Dies sind beispielsweise Verfahren zum Entzug eines Waffenscheins wegen Gewaltdelikten mit Waffen, Verfahren des Sorgerechtsentzugs im Zusammenhang mit einer Kindesmisshandlung oder Verfahren in Handelssachen nach einem betrügerischen Bankrott. Nach Nummer 4 ist eine Zweckänderung auch zur Abwehr einer gegenwärtigen und erheblichen Gefahr für die öffentliche Sicherheit möglich. Danach ist ein qualifizierter Gefahrenmaßstab erforderlich. "Gegenwärtig" drückt wie "unmittelbar bevorstehend" die zeitliche Nähe der Gefahrenentwicklung bzw. ein gesteigertes Maß der Wahrscheinlichkeit des Schadenseintritts aus. Die Erheblichkeit kann sich aus dem betroffenen Rechtsgut, der Tatbegehung oder dem möglichen Ausmaß des Schadens ergeben.

Zu Absatz 2

Absatz 2 normiert die Zweckbindung nach Artikel 8 Abs. 3 sowie Artikel 1 Abs. 4 der Schwedischen Initiative, die Anwendung findet, wenn personenbezogene Daten von den Staaten, in denen der Rahmenbeschluss gilt und entsprechend des Formblatts nach dessen Anlage oder sonst erkennbar nach dem Rahmenbeschluss an die Polizei übermittelt werden. Die übermittelten Daten dürfen danach ohne Zustimmung des übermittelnden Staates nur für den Zweck der Übermittlung oder zur Abwehr einer unmittelbaren und erheblichen Gefahr für die öffentliche Sicherheit verarbeitet werden. Damit ist eine Umwidmung von präventiven in repressive Zwecke ohne Zustimmung des übermittelnden Staates ausgeschlossen. Der Rahmenbeschluss sieht jedoch vor, dass der übermittelnde Staat seine Zustimmung zur zweckändernden Verarbeitung der übermittelten Daten bereits bei der Übermittlung der Daten erteilen kann.

Zu Absatz 3

Damit die Verarbeitungsbeschränkungen beider Rahmenbeschlüsse in der Praxis eingehalten werden können, müssen die empfangenen Daten gekennzeichnet werden. Satz 1 regelt diese Kennzeichnungspflicht. Die Sätze 2 und 3 statuieren auf der Grundlage der Artikel 9, 12 und 16 des Rahmenbeschlusses Datenschutz sowie des Artikels 8 Nr. 4 Satz 3 und 4 der Schwedischen Initiative die Pflicht, die von dem übermittelnden Mitgliedstaat mitgeteilten Beschränkungen und Bedingungen für die Datenverarbeitung zu beachten. Für mitgeteilte Lösch- oder Sperrfristen gilt diese Pflicht mit der Einschränkung, dass die übermittelten Daten auch nach Fristablauf für laufende Strafverfolgungs- oder - vollstreckungsverfahren noch verarbeitet werden dürfen. Ausgehend von Artikel 8 Abs. 2 des Rahmenbeschlusses Datenschutz wird in Satz 4 klargestellt, dass die Polizei nach den allgemeinen Vorschriften unverzüglich unrichtige Daten zu berichtigen und unzulässig gespeicherte Daten zu löschen oder im Einzelfall zu sperren hat. Satz 5 setzt Artikel 15 des Rahmenbeschlusses Datenschutz und Artikel 8 Abs. 4 Satz 5 der Schwedischen Initiative um. Danach hat der empfangende Mitgliedstaat dem übermittelnden Mitgliedstaat auf dessen Ersuchen zur Datenschutzkontrolle Auskunft über die Verarbeitung der übermittelnden Daten zu erteilen.

Zu Absatz 4

Absatz 4 regelt in Umsetzung von Artikel 13 des Rahmenbeschlusses Datenschutz die Voraussetzungen für die Weiterübermittlung empfangener Daten an andere öffentliche Stellen außerhalb des Anwendungsbereichs des Beschlusses. Die Angemessenheit des Datenschutzniveaus wird unter Berücksichtigung aller Umstände beurteilt, die bei Datenübermittlungen von Bedeutung sind; insbesondere können die Art der Daten, die Zweckbestimmung, die Dauer der geplanten Verarbeitung, das Herkunfts- und das Endbestimmungsland, die für den Empfänger geltenden Rechtsnormen sowie die dort geltenden Standesregeln und Sicherheitsmaßnahmen herangezogen werden. Die vorherige Zustimmung kann sich, zusammenfassend für künftige Einzelfälle, auf bestimmte Kategorien von Daten oder bestimmte Drittstaaten erstrecken.

Zu Absatz 5

Absatz 5 regelt in Umsetzung von Artikel 14 des Rahmenbeschlusses Datenschutz die Voraussetzungen für die Weiterübermittlung empfangener Daten an nichtöffentliche Stellen innerhalb der Europäischen Union.

Zu Absatz 6

In Absatz 6 wird klargestellt, dass die Absätze 1 bis 5 nicht nur im Verhältnis zu den Mitgliedstaaten Anwendung finden, sondern auch im Verhältnis zu den Schengen-assoziierten Staaten sowie zu den Behörden und Informationssystemen, die aufgrund des Vertrages über die Europäische Union oder des Vertrages zur Gründung der Europäischen Gemeinschaft errichtet worden sind.

Zu § 41 d

Die Bestimmung regelt, dass der Ratsbeschluss Prüm bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen mit den Mitgliedstaaten der Europäischen Union anwendbar ist. Die Anwendbarkeitsbestimmung umfasst die Regelungen des Ratsbeschlusses Prüm, die sich auf die materiellen Anforderungen bei der Datenübermittlung zur Verhütung von Straftaten, auf die allgemeine Gefahrenabwehr sowie die operativen polizeilichen Befugnisse beziehen. Der übrige Bereich ist durch § 1 des Ausführungsgesetzes zum Prümer Vertrag und zum Ratsbeschluss Prüm bereits erfasst.

Zu Nummer 10 (§ 43)

Es handelt sich um die Klarstellung, dass der Datenabgleich mit dem Gesamtdatenbestand der Polizei nicht nur bei Störern im Sinne der §§ 7 und 8, sondern auch bei Personen zulässig ist, die an einem gefährlichen Ort, an einem gefährdeten Objekt oder an einer polizeilichen Kontrollstelle angetroffen werden. In der jüngeren Vergangenheit wurde vereinzelt die Auffassung vertreten, dass an den genannten Orten für einen Abgleich mit dem Gesamtdatenbestand zusätzliche Tatbestandsmerkmale erfüllt sein müssten.

Zu Nummer 11 (§ 44)

Die Änderung von Absatz 1 ist eine aus der Aufgabe der Straftatenkataloge resultierende Folgeänderung.

Mit Absatz 5 wird der Personenkreis, der nach der durchgeführten Maßnahme zu benachrichtigen ist, für die Rasterfahndung speziell bestimmt: Benachrichtigt werden diejenigen Personen, gegen die nach Rasterung der Daten weitere Ermittlungen geführt wurden. Ansonsten gilt über die Verweisung in Satz 2 für die Benachrichtigung die Regelung des § 36.

Zu Nummer 12

Die Streichung behebt ein Redaktionsversehen des Gesetzgebers. Die Verweisungen gehen ins Leere, weil § 46 im Jahr 2008 geändert wurde.

Zu Nummer 13

Redaktionelle Anpassung

Zu Artikel 2 (Änderung des Ordnungsbehördengesetzes)

Zu Nummer 1

Zu Absatz 1

Die Regelung verfolgt den Zweck, den Gemeinden, Verwaltungsgemeinschaften oder erfüllenden Gemeinden als Maßnahme der Gefahrenvorsorge eine Handhabe zur Verfügung zu stellen, um vor allem Kinder und Jugendliche vor Gefahren zu schützen, die vom Alkoholkonsum im öffentlichen Raum ausgehen. Daher soll besonders in der Nähe von Einrichtungen wie Schulen, Kindergärten und Kinderspielplätzen der Konsum von Alkohol verboten werden können. Die Bestimmung des Absatzes 1 Satz 1 ist in Anlehnung an entsprechende Regelungen im Thüringer Glücksspielgesetz und im Thüringer Spielhallengesetz übernommen worden. Die Gewährleistung eines effektiven Kinder- und Jugendschutzes sowie der allgemeine Gesundheitsschutz sind gemäß Artikel 19 Abs. 4 der Verfassung des Freistaats Thüringen ein Handlungsauftrag an den Gesetzgeber. Die vorliegende Regelung ist geeignet und erforderlich, um diese Ziele zu verfolgen.

Das Verbot gilt nicht für Bereiche, die nach Gaststättenrecht konzessioniert sind ("außerhalb zugelassener Freischankflächen").

Zu Absatz 2

Mit Absatz 2 erhalten die Gemeinden die Möglichkeit, in weiteren Gemeindegebietsteilen mit erhöhtem Gefährdungspotenzial Alkoholverbotszonen durch ordnungsbehördliche Verordnung einzurichten, um alkoholbedingten Straftaten und Ordnungswidrigkeiten wirksam entgegentreten zu können.

Die Entscheidung über die Einrichtung einer Alkoholverbotszone wird als Aufgabe des übertragenen Wirkungskreises (§ 1 Satz 1 OBG) getroffen. Die Ausgestaltung der zu erlassenden Verordnung obliegt daher der zuständigen Ordnungsbehörde unter Berücksichtigung der konkreten örtlichen Verhältnisse.

Die Einrichtung einer Alkoholverbotszone ist nur möglich, wenn die zuständige Ordnungsbehörde über konkrete Anhaltspunkte zur Gefahrenlage an den jeweiligen Orten durch eine in tatsächlicher Hinsicht genügend abgesicherte Prognose verfügt.

Das Verbot des Alkoholkonsums gilt nicht für Bereiche, die nach Gaststättenrecht konzessioniert sind ("außerhalb zugelassener Freischankflächen").

Der Alkohol ist als hierzulande häufigstes berauschendes Mittel besonders hervorgehoben (vergleiche § 316 Abs. 1 StGB).

Im Fall des Absatzes 2 ist der Verordnungsgeber verpflichtet, regelmäßig zu überprüfen, ob die Voraussetzungen für die ordnungsbehördliche Überprüfung noch vorliegen.

Zu Absatz 3

Durch das Aufstellen von Hinweisschildern, auch in Form von Piktogrammen, werden die Einwohner und Gäste der Gemeinden, die von der Verordnungsermächtigung Gebrauch machen, davon in Kenntnis gesetzt, dass das Trinken von Alkohol im Verbotsbereich eine mit Geldbuße bedrohte Handlung ist. Dies soll insbesondere auch der Tatsache Rechnung tragen, dass sich Alkoholverbotszonen noch nicht flächendeckend im Bundesgebiet durchgesetzt haben und demzufolge auch nicht im Bewusstsein der Bevölkerung verankert sein können. Im Übrigen sind die gesetzlichen Anforderungen des § 31 Abs. 3 OBG zu beachten.

Zu Nummer 2

Redaktionelle Anpassung

Artikel 3

Die Bestimmung trägt dem Zitiergebot aus Artikel 19 Abs. 1 des Grundgesetzes und Artikel 42 Abs. 3 der Verfassung des Freistaats Thüringen Rechnung.

Zu Artikel 4

Die Bestimmung regelt das Inkrafttreten des Gesetzes.