



**DER HESSISCHE BEAUFTRAGTE  
FÜR DATENSCHUTZ UND INFORMATIONSFREIHEIT**

DER HESSISCHE BEAUFTRAGTE  
FÜR DATENSCHUTZ UND INFORMATIONSFREIHEIT  
Postfach 31 63 · 65021 Wiesbaden

Herrn  
Vorsitzenden des Innenausschusses  
des Hessischen Landtages  
Christian Heinz

**Per E-Mail an:**

c.lingelbach@ltg.hessen.de  
m.mueller@ltg.hessen.de

Aktenzeichen <i>Bitte bei Antwort angeben</i>	58.01.70:HSOG-2022
zuständig Durchwahl 14 08 -	Walburg/Strutwolf/Klaffke 157
Ihr Zeichen Ihre Nachricht vom	I A 2.2 10.05.2022
Datum	30.06.2022

**Stellungnahme des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zum Gesetzentwurf zur Änderung sicherheitsrechtlicher Vorschriften und zur Umorganisation der hessischen Bereitschaftspolizei vom 22.03.2022, LT-Drs. 20/8129**

Sehr geehrter Herr Vorsitzender,

für die Einladung zur öffentlichen mündlichen Anhörung in der Sitzung des Innenausschusses am 15. Juli 2022 bedanke ich mich.

Gerne nehme ich die Gelegenheit wahr, vorab schriftlich zum Gesetzentwurf Stellung zu nehmen.

Leider hatte ich keine Gelegenheit, meine datenschutzrechtlichen Bedenken bereits frühzeitig im Rahmen der Erstellung des Gesetzentwurfs anzubringen. Daher möchte ich mich im Folgenden vorwiegend zu den Regelungen äußern, gegen die aus datenschutzrechtlicher Sicht Bedenken bestehen bzw. bei denen ich Änderungsbedarf sehe.

Unsere derzeitige telefonische Erreichbarkeit: Mo. - Fr. von 09:00 - 12:00 Uhr sowie Mo. - Do. von 13:00 - 16:00 Uhr  
Persönliche Termine bitte mit vorheriger Absprache

Gustav-Stresemann-Ring 1 · 65189 Wiesbaden · Telefon (06 11) 14 08-0  
E-Mail [poststelle@datenschutz.hessen.de](mailto:poststelle@datenschutz.hessen.de) · DE-Mail: [poststelle@datenschutz-hessen.de-mail.de](mailto:poststelle@datenschutz-hessen.de-mail.de)  
Internet [www.datenschutz.hessen.de](http://www.datenschutz.hessen.de)  
Bankverbindung: Kontoinhaber HCC/Kanzlei Hess.Landtag/DB · IBAN DE67 5005 0000 0001 0053 62 · BIC HELADEFXXX  
USt IdNr: DE812021807

## I. Zu den Änderungen im Hessischen Verfassungsschutzgesetz (HVSG), Artikel 1

### Zu § 16 HVSG

Die Verlängerung der Prüffristen in § 16 Abs. 7 Satz 1 bei schweren Straftaten mit Staatsschutzbezug auf 10 Jahre begegnet keinen durchgreifenden datenschutzrechtlichen Bedenken, da diese an das Vorliegen tatsächlicher Anhaltspunkte, dass eine Person bestimmte Straftaten plant, begeht oder begangen hat, geknüpft wird.

Problematisch erscheint jedoch, dass die neu hinzugekommene dynamische Verweisung des § 16 Abs. 7 Satz 1 HVSG auf § 3 Abs. 1a des Artikel 10-Gesetzes (G 10) und damit auf die Bundesnorm des § 72 Abs. 1 und 3 Zollfahndungsdienstgesetz (ZFdG) mit weiteren Verweisungen auf das Kriegswaffenkontrollgesetz (KrWaff-KontrG) die Verständlichkeit und Normenklarheit insgesamt beeinträchtigen und vor diesem Hintergrund verfassungsrechtlich bedenklich sind.

Die in Bezug auf die elektronischen Akten eingefügte Protokollierungspflicht u. a. für Zwecke der Datenschutzkontrolle in § 16 Abs. 10 HVSG füllt die für das Landesamt für Verfassungsschutz (LfV) Hessen aufgrund der Nichtanwendbarkeit des § 71 HDSIG bestehende Lücke. Dies ist – in Verbindung mit der strengen Zweckbindung – aus datenschutzrechtlicher Sicht zu begrüßen. Die Aufbewahrungsfrist für die Protokolldaten bis zum Ende des folgenden Kalenderjahres selbst erscheint vor dem Hintergrund der Verlängerung der Speicherfristen jedoch im Verhältnis sehr kurz bemessen.

### Zu § 26 Abs. 1 Satz 1 HVSG

Es ist aus datenschutzrechtlicher Sicht zu begrüßen, dass die Voraussetzung zur Auskunftserteilung für betroffene Personen, auf einen konkreten Sachverhalt hinzuweisen, gestrichen werden soll.

Allerdings hat die betroffene Person nach wie vor ein besonderes Interesse an einer Auskunft darzulegen – die Auskunftserteilung im Anwendungsbereich der DS-GVO und der JI-Richtlinie ist nicht an eine solche Vorgabe geknüpft.

## **II. Zu den Änderungen im Hessischen Gesetz über die öffentliche Sicherheit und Ordnung (HSOG), Artikel 2**

### **Zu § 12a HSOG**

Grundsätzlich ist die Einführung einer eigenen Vorschrift zum Schutz zeugnisverweigerungsberechtigter Berufsgeheimnisträger mit dem § 12a HSOG n. F. aus datenschutzrechtlicher Sicht zu begrüßen.

Durch mehrere Rückausnahmen in den Absätzen 1 - 4 wird jedoch die Normenklarheit und Verständlichkeit in Mitleidenschaft gezogen. Bei der praktischen Anwendung der Vorschriften sind so Auslegungsschwierigkeiten nicht auszuschließen.

Der relative Schutz von Vertrauensverhältnissen, beispielsweise bei Ärzten sowie Presse- und Medienvertretern, ist gemäß § 12a Abs. 2 Satz 1 HSOG n. F. an eine „Prüfung der Verhältnismäßigkeit unter Würdigung des öffentlichen Interesses“ geknüpft. Diese Prüfung dürfte die Rechtsanwender, mithin die Polizeibehörden, in der Praxis nicht selten vor große Herausforderungen stellen. Zudem ist eine Dokumentationspflicht – zumindest nach dem Wortlaut des Regelungsvorschlags – nicht vorgesehen. Es steht daher zu befürchten, dass die Vornahme der Verhältnismäßigkeitsprüfungen nur schwer nach-/überprüfbar sein werden und die Regelung dadurch weitestgehend leerlaufen könnte. Eine unabhängige Kontrolle des Schutzes zeugnisverweigerungsberechtigter Berufsgeheimnisträger bei besonders eingriffsintensiven Maßnahmen wird unter diesen Voraussetzungen jedenfalls durch meine Behörde kaum möglich sein.

### **Zu § 13a Abs. 2 HSOG**

Die vorgeschlagene Ergänzung, Bedienstete, die eine Tätigkeit in einer Behörde mit Vollzugsaufgaben anstreben, regelmäßig auch anhand von Datenbeständen des LfV Hessen zu überprüfen, ist zwar nachvollziehbar, birgt aber aufgrund der Besonderheit der Datenbestände des Verfassungsschutzes einige rechtliche Risiken.

Zunächst ist es bereits problematisch, eine solche als Regelvorgabe ausgestaltete Überprüfung, die im Ergebnis aufgrund „weicher“ Erkenntnisse des Verfassungsschutzes Personen von bestimmten Berufsgruppen ausschließen kann, in einem Po-

lizeigesetz zu verankern. Im Grunde handelt es sich hier um ein Hindernis für die Zulassung zum Staatsdienst, für zumeist beamtenrechtliche Tätigkeiten, und sollte daher auch in den entsprechenden Gesetzen verankert werden.

Des Weiteren fehlt es im § 13a Abs. 2 HSOG an Regelungen, wie der Bewerber oder die Bewerberin im Fall einer Ablehnung aufgrund von Erkenntnissen des Verfassungsschutzes Rechtsschutz suchen kann. In § 13a Abs. 2 Satz 4 und 5 HSOG ist lediglich vorgesehen, dass der betroffenen Person mitzuteilen ist, wo sie weitere Auskünfte zu dem Verfahren erhalten, und dass sie sich an meine Behörde wenden kann; zudem ist ihr Gelegenheit zur Stellungnahme zu geben. Spezifische Vorgaben für die Behandlung der Stellungnahme, wann die Gelegenheit zu dieser zu geben ist und welche Informationen dafür mitgeteilt werden müssen, fehlen jedoch in der Vorschrift. Im Unterschied hierzu macht etwa § 7 Luftsicherheitsgesetz für Zuverlässigkeitsüberprüfungen konkrete Ausführungen zur Ausgestaltung des Verfahrens.

- Hinzu kommt noch die Besonderheit, dass eine Auskunftserteilung beim LfV Hessen an bestimmte einschränkende Vorgaben geknüpft ist und die Ablehnung einer Auskunftserteilung nach § 26 Abs. 3 HVSG keiner Begründung bedarf. So ist denkbar, dass die betroffenen Personen für die Tätigkeit als Bedienstete bei einer Behörde mit Vollzugsaufgaben aufgrund von Erkenntnissen des Verfassungsschutzes abgelehnt werden, ohne jedoch zu erfahren, um welche Erkenntnisse es sich hierbei handelt und wie sie ggf. gegen eine solche Ablehnung konkret vorgehen können.

#### **Zu § 14 Abs. 3a HSOG**

In § 14a Abs. 3 HSOG n. F. soll eine Ergänzung dergestalt vorgesehen werden, dass die Voraussetzungen für eine Videoüberwachung nach Abs. 3 Satz 1 „in den öffentlich zugänglichen Bereichen von Flughäfen, Personenbahnhöfen, Sportstätten, Einkaufszentren und Packstationen als erfüllt“ anzusehen sind. Mithin soll an diesen Örtlichkeiten künftig die Kriminalitätsanalyse entfallen und eine Videoüberwachung regelmäßig zulässig sein.

Zunächst ist die Norm im Hinblick auf die örtlichen Grenzen der aufgezählten Örtlichkeiten problematisch, da es an einer hinreichenden Bestimmtheit der „öffentlich zugängliche Bereiche“ dieser Örtlichkeiten in der vorgeschlagenen Regelung mangelt.

Bezüglich des Großflughafens Frankfurt am Main ergeben sich räumliche Abgrenzungsproblematiken, bspw. wo genau beginnt und endet der Bereich Flughafen. Zudem könnten auch öffentliche Straßen auf dem Flughafengelände dieser Regelung unterfallen, was bei einer Videoüberwachung dieser Straßen ohne entsprechende Einschränkung zu einer umfangreichen Erfassung von amtlichen Kennzeichen durchfahrender Kraftfahrzeuge führen würde. Eine solche Ausgestaltung wird von meiner Behörde vor dem Hintergrund des kriminalpräventiven Zwecks von Videoüberwachungsmaßnahmen nach § 14 Abs. 3 HSOG für unverhältnismäßig erachtet.

Des Weiteren ist aus datenschutzrechtlicher Sicht nicht nachvollziehbar, warum Packstationen grundsätzlich als Kriminalitätsschwerpunkt i. S. v. § 14 Abs. 3 Satz 1 HSOG eingeordnet werden sollen. In Hessen dürften zwischenzeitlich mehrere Hundert Packstationen, ausschließlich eines privatwirtschaftlichen Unternehmens, betrieben werden. Da diese in der Regel an gut zugänglichen und stark frequentierten Örtlichkeiten betrieben werden, dürfte eine Vielzahl von Personen von einer solchen Maßnahme betroffen werden. Es kann zudem nicht nachvollzogen werden, inwieweit durch eine präventive Videoüberwachung Kriminalität in öffentlich zugänglichen Bereichen von Packstationen verhindert werden kann. Ziel einer Videoüberwachungsmaßnahme nach § 14 Abs. 3 HSOG ist grundsätzlich die Verdrängung von Straßensriminalität. Bei Kriminalität im Zusammenhang mit Packstationen dürfte es sich regelmäßig nicht um Straßensriminalität, sondern eher um andere Kriminalitätsphänomene, wie etwa Vermögensdelikte, handeln. Eine präventive Videoüberwachung dürfte im Hinblick auf solche Deliktsbereiche jedoch – auch vor dem Hintergrund der Speicherdauer der Videoaufnahmen (i. d. R. 14 Tage) sowie der Art und Weise der Tatbegehungen – wenig zielführend sein und auch zur Täterermittlung kaum beitragen können.

Bezüglich der öffentlich zugänglichen Bereiche von Sportstätten halte ich eine erweiterte Regelung für verzichtbar, da die dort auftretende Kriminalität nicht durch die Örtlichkeit ausgelöst wird. Vielmehr sind es dort stattfindende Veranstaltungen – sportliche wie gesellschaftliche und kulturelle – die nach individueller prognostischer Bewertung auch aufgrund der aktuellen Regelung gemäß § 14 Abs. 3 HSOG zu kriminalpräventiven Zwecken videoüberwacht werden dürfen. Die grundsätzliche Erlaubnis zur offenen Videoüberwachung allein aufgrund der Tatsache, dass es sich

um den öffentlich zugänglichen Bereich einer Sportstätte handelt, erscheint daher nicht angemessen und unverhältnismäßig. Die vorgeschlagene Regelung würde lediglich eine solche Betrachtung des Einzelfalles bzw. der einzelnen Veranstaltung verzichtbar machen.

Die Qualifizierung aller Einkaufszentren als Kriminalitätsschwerpunkte im Sinne von § 14 Abs. 3 Satz 1 HSOG ist ebenfalls nicht sachgerecht. Zum einen besteht auch für den privatwirtschaftlichen Betreiber von Einkaufszentren die Möglichkeit einer Videoüberwachung (nach § 4 BDSG / DS-GVO). Zum anderen können Polizeibehörden und örtliche Gefahrenabwehrbehörden bereits aufgrund der derzeitigen Rechtslage kriminalpräventive Videoüberwachungsmaßnahmen durchführen, soweit sich in einem Einkaufszentrum ein Kriminalitätsschwerpunkt nachvollziehbar darstellen lässt.

Insgesamt erscheint die Novellierung der Regelungen zur gefahrenabwehrrechtlichen Videoüberwachung des öffentlichen Raumes arbeitsökonomischen Erwägungen geschuldet, da an den klassifizierten Örtlichkeiten ohne Feststellungen zu einem tatsächlichen Kriminalitätsschwerpunkt eine Videoüberwachung ermöglicht werden soll. Eine Betrachtung der Verhältnismäßigkeit im Hinblick auf den Grundrechtseingriff der jeweiligen Videoüberwachungsmaßnahme würde dann künftig entfallen – eine aus datenschutzrechtlicher Sicht eher als Verschlechterung einzuordnende Änderung im Vergleich zur aktuellen Rechtslage.

### **Zu § 14a HSOG**

Die von meiner Behörde in der Vergangenheit formulierten Anforderungen zur Überarbeitung der bisherigen Gesetzesfassung wurden im Wesentlichen umgesetzt. Der neue § 14a Abs. 1a HSOG enthält demgemäß Vorgaben zum Schutz von Personen außerhalb von Fahrzeugen bei der Bildaufzeichnung sowie zum Schutz der erhobenen Daten selbst vor unbefugtem Zugriff.

Die Anforderungen des Bundesverfassungsgerichts (BVerfG) mit Urteil vom 11. März 2008 (1 BvR 2074/05) sowie des Beschlusses vom 18.12.2018 (1 BvR 3187/10) wurden zum Anlass für Änderungen genommen. Die Zwecke der Datenerhebung sind nun in § 14a Abs. 1 HSOG abschließend geregelt und an konkrete Gefahrentat-

bestände bzw. den Schutz von Rechtsgütern von erheblichem Gewicht geknüpft (vgl.: BVerfG, Beschluss vom 18.12.2018, 1 BvR 3187/10, Rn. 73). Abs. 1 enthält nun weitere Beschränkungen der Datenerhebung in örtlicher Hinsicht (vgl.: a.a.O., Rn. 75).

Zweifel an der hinreichenden Normenklarheit verbleiben in Bezug auf § 14a Abs. 2 HSOG. Das Bundesverfassungsgericht hatte eine Konkretisierung des Begriffs „Fahndungsbestand“ gefordert (vgl.: BVerfG, Urteil vom 11. März 2008, 1 BvR 2074/05, Rn. 100 ff.). § 14a Abs. 2 HSOG sieht den automatischen Abgleich der Bilddaten und Kennzeichen mit dem „Fahndungsbestand der Sachfahndungsdateien des beim Bundeskriminalamt nach den Vorschriften des Bundeskriminalamtsgesetzes vom 1. Juni 2017 [...] und des beim Hessischen Landeskriminalamt nach den Vorschriften dieses Gesetzes geführten polizeilichen Informationssystems“ vor. In der gegenwärtigen Gesetzesfassung bereitet schon die umstrittene Natur der Verweisung nicht unerhebliche Probleme (Bauerle, in: Möstl/Bauerle, BeckOK Polizei- und Ordnungsrecht Hessen, § 14a HSOG, 25. Edition, Stand: 01.04.2022, Rn. 107). Eine Novellierung des § 14a Abs. 2 HSOG in dieser Hinsicht ist dennoch nicht erfolgt.

Eine Konkretisierung und Präzisierung der jeweils betroffenen Datenbestände ist auch für zukünftige Gesetzesvorhaben mit Blick auf den Grundsatz der Zweckbindung und den perspektivisch fortschreitenden Einsatz von Software zur Analyse immer größerer Datenbestände durch die Hessische Polizei dringend geboten. Sie muss dabei wenigstens den aktuell einbezogenen Datenbeständen und absehbaren Nutzungsszenarien Rechnung tragen, um eine zukunftsfähige Grundlage für rechtssichere Polizeiarbeit bieten zu können.

### **Zu § 15 HSOG**

Die Streichung der zeitlichen Obergrenze von einem Jahr für die Verlängerung der richterlichen Anordnung von verdeckten Maßnahmen begegnet aus datenschutzrechtlicher Sicht keinen Bedenken. Durch den Richtervorbehalt für die jeweilige Verlängerung sollte eine hinreichend unabhängige Kontrolle sichergestellt sein.

Es bleibt aber zu beachten, dass sich in Einzelfällen dennoch eine absolute Höchstdauer aus dem Grundsatz der Verhältnismäßigkeit ergeben kann (BVerfG, Urteil vom 20. April 2016 1 BvR 966/09, Rn. 171).

#### **Zu § 20 Abs. 6 HSOG**

Der neu angefügte Satz bezüglich Vorgabe für eine Verwaltungsvorschrift zur Regelung der Meldungen von Verfahrensausgängen seitens der Staatsanwaltschaften an die Hessische Polizei ist aus datenschutzrechtlicher Sicht zu begrüßen. Ich hatte bereits in meinem 48. Tätigkeitsbericht, Nr. 6.2., Seite 36 ff., auf diese Problematik aufmerksam gemacht.

Allerdings mangelt es der Norm nach wie vor an der in den Polizeigesetzen anderer Bundesländer sowie im Bundeskriminalamtgesetz (BKAG) vorgesehenen Negativprognose für eine präventivpolizeiliche Nutzung von personenbezogenen Daten aus der Strafverfolgung.

#### **Zu § 25a HSOG**

Die als redaktionell bezeichnete Änderung in § 25a Abs. 1 S. 1 HSOG stellt m. E. im Gesamtkontext der Norm noch einmal klar, dass es sich nicht um kategorisierbare „Einzelfälle“, sondern um einen jeweils individuell zu betrachtenden „begründeten Einzelfall“ handelt. Dies ist auch im Rahmen einer durchzuführenden Güter- und Interessenabwägung in Bezug auf die einzelne Maßnahme zu beachten.

#### **Zu § 27 HSOG**

Die Gesetzesänderung stellt zunächst eine erhebliche Verlängerung der Aussondierungsprüffristen dar. So darf bei „fortbestehendem Tatverdacht“ bezüglich der kategorisierten Straftaten eine Verlängerung der Speicherung um 10 Jahre erfolgen, bei sonstigen Straftaten von erheblicher Bedeutung (§ 13 Abs. 3 HSOG) um weitere 5 Jahre. Eine grundsätzliche personenbezogene Negativprognose als rechtliche Voraussetzung für eine polizeiliche Speicherung ist in der bisherigen Fassung des HSOG sowie auch im vorliegenden Entwurf nicht vorgesehen – eine solche Regelung, wie sie etwa § 18 Abs. 1 Nr. 3, Abs. 2 Nr. 2 BKAG vorsieht, fehlt. Vor dem Hintergrund der erweiterten Speichermöglichkeiten erscheint als Voraussetzung für die Speicherung im polizeilichen Informationssystem POLAS-Hessen eine individuell personenbezogene Negativprognose nunmehr noch dringlicher geboten.

Die Formulierung „bei fortbestehendem Verdacht“ als Zulässigkeitsvoraussetzung für eine weitere Speicherung zieht keine tatsächliche Schranke ein, da nicht erkennbar bzw. nachvollziehbar ist, wie etwa nach Ablauf der ersten 10 Jahre Regelspeicherung plötzlich ein Verdacht nicht mehr fortbestehen könnte. Würde der Tatverdacht bis Erreichen der ersten Aussonderungsprüffrist ausgeräumt (Aussonderungsprüffristen gemäß § 15 Abs. 1 HSOG-DVO), würde dies unmittelbar eine Löschung der Daten auslösen. Ist dies nicht der Fall, soll der Tatverdacht nunmehr „automatisch“ fortbestehen und keinen diesbezüglichen Überprüfungsaufwand mehr generieren, wie dies bisher nach Erreichen der ersten Aussonderungsprüffrist erforderlich war (§ 15 Abs. 3, 4 HSOG-DVO). Die Formulierung wird dadurch letztlich zu einer Regelspeicherung von 15 oder 20 Jahren bei kategorisierten bzw. klassifizierten Straftaten führen, ohne dass zum Zeitpunkt der Verlängerung eine Prüfung bzw. Überprüfung, ob tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass die Person solche Straftaten begehen wird, erfolgen muss. Eine entsprechende Überprüfung ist nunmehr erst bei einer weiteren Verlängerung vorgesehen (§ 27 Abs. 4 Satz 5 HSOG n. F.).

Die aktuellen Regelungen erlauben bereits eine Verlängerung der Speicherungen unter dem Vorbehalt einer Prüfung bzw. Überprüfung nach den Vorgaben von § 15 Abs. 3 und 4 HSOG-DVO. Die neue Regelung erweitert daher tatsächlich nicht die präventiven Möglichkeiten der Polizei im Rahmen der polizeilichen Erfordernisse, sondern erspart den Polizeibehörden lediglich den bisherigen Prüfungs- bzw. Überprüfungsaufwand nach § 15 Abs. 3, 4 HSOG-DVO. Der Begründungsaufwand für die korrespondierenden Grundrechtseingriffe wird somit um 5 bzw. 10 Jahre in die Zukunft verschoben. In der Praxis dürfte diese erleichterte Verlängerung der Speicherung zu einer verlängerten Regelspeicherung im neuen gesetzlichen Rahmen führen.

In Abgrenzung zu den Daten aus dem Bundeszentralregister werden im polizeilichen Informationssystem auch Straftaten erfasst und gespeichert, bei denen es nicht zu einer Anklage oder zu einer Verurteilung gekommen ist. Insbesondere Einstellungen gemäß § 170 Abs. 2 StPO wegen eines mangelnden Tatverdachts sind hier höchst problematisch, da oftmals ein Tatnachweis nicht geführt werden konnte. Dies sind ebendiese Fälle, in denen etwa § 18 Abs. 1 Nr. 3 BKAG explizit eine Negativprognose fordert, da diese Personen nicht mehr Beschuldigte sind und nicht verurteilt wur-

den. Quantitativ spielen diese Einstellungen gemäß § 170 Abs. 2 StPO eine nicht unerhebliche Rolle im Datenbestand POLAS-Hessen.

Es ist daher aus datenschutzrechtlicher Sicht nicht hinnehmbar, dass bei solchen Verfahrenseinstellungen die korrespondierenden Daten ohne weitere Prüfung bzw. Überprüfung nochmals für 5 oder 10 Jahre gespeichert werden können. In der Folge würden Personen, bei denen letztlich ein Tatnachweis nicht geführt werden konnte, präventivpolizeilich als Täter stigmatisiert und müssen ggf. etwa über Zuverlässigkeitsprüfungen in vielen Lebensbereichen Einschränkungen hinnehmen.

Weiterhin soll auch die bisherige Prüffrist bei Erwachsenen in Fällen von geringerer Bedeutung – bisher 3 Jahre gemäß § 27 Abs. 4 Nr. 1 HSOG i. V. m. § 15 Abs. 1 Satz 2 HSOG-DVO – nunmehr auf 5 Jahren verlängert werden. Auch dies ist vor dem Hintergrund der dargestellten Problematiken aus datenschutzrechtlicher Sicht kritisch zu betrachten.

#### **Zu § 31 Abs. 2 HSOG**

Die Möglichkeit zum verpflichtenden Tragen/Mitführen eines technischen Mittels zur Überwachung des Aufenthaltsortes gemäß § 31a Abs. 1 HSOG ist zwar in § 31 Abs. 2 HSOG n. F. als Kann-Regelung ausgestaltet, macht aber ansonsten keine konkreten Vorgaben und sieht auch keine Einschränkungen vor.

Die Anordnung einer elektronischen Aufenthaltsüberwachung erscheint jedoch dann – auch aus datenschutzrechtlicher Sicht – nicht sachgerecht, wenn bspw. keinerlei Anhaltspunkte dafür vorliegen, dass die betreffende Person sich nicht an den Platzverweis, das Aufenthalts- oder Kontaktverbot hält. Die gesetzliche Regelung sollte dies klarstellen, um eine verhältnismäßige und verfassungskonforme Anwendung der Norm sicherzustellen.

#### **Zu § 31a Abs. 1 HSOG**

Die in § 31a Abs. 1 HSOG n. F. vorgesehene Verpflichtung, ein zur Verfügung gestelltes Mobiltelefon zur Ermöglichung einer Sprachverbindung zwischen betroffener Person und datenverarbeitender Stelle ständig in betriebsbereitem Zustand bei sich zu führen, ist vor dem Hintergrund, dass der jeweilige Aufenthaltsort über die gemäß

§ 31a Abs. 1 HSOG eingesetzte Technik bereits übertragen wird, aus datenschutzrechtlicher Sicht nicht zu beanstanden.

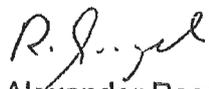
Es sollte jedoch sichergestellt werden, dass im Rahmen der Nutzung des verpflichtend mitzuführenden Mobiltelefons nur diejenigen personenbezogenen Daten erhoben und weiterverarbeitet werden, die für eine ggf. notwendige Verbindung/Sprachverbindung erforderlich sind.

### **Zu § 98a HSOG**

Bei der Einführung einer Legitimations- und Kennzeichnungspflicht für die Vollzugs-polizei handelt es sich um eine nachvollziehbare Neuregelung, die datenschutzrechtlich grundsätzlich nicht zu beanstanden ist.

Allerdings sollten im Rahmen der noch zu schaffenden Verwaltungsvorschriften nach § 98a Abs. 4 HSOG n. F. auch mögliche Belange des Beschäftigtendatenschutzes beachtet werden.

Mit freundlichen Grüßen



Prof. Dr. Alexander Rossnagel