

**Schriftliche Anhörung
zu Gesetzentwurf – Drucks. [21/4531](#)**

Stellungnahmen von Anzuhörenden und Sachverständigen



Hessischer Städtetag · Frankfurter Straße 2 · 65189 Wiesbaden

Hessischer Landtag
Innenausschuss
Schlossplatz 1–3
65183 Wiesbaden

per Mail an h.dransmann@ltg.hessen.de
und c.kehrein@ltg.hessen.de

**Schriftliche Anhörung des Innenausschusses
des Hessischen Landtags
Gesetzentwurf der Landesregierung
Gesetz zur Neufassung des Hessischen
Sicherheitsüberprüfungs- und Verschlusssachengesetzes
und zur Änderung einer weiteren Vorschrift
– Drucks. 21/4531 –**

Ihre Nachricht vom:
30.06.2026

Ihr Zeichen:

Unser Zeichen:
050.4 Ba/Bö

Durchwahl:
(0611) 1702-0

E-Mail:
posteingang@hess-staedtetag.de

Datum:
15.07.2026

Stellungnahme Nr.:
035-2026

Sehr geehrter Herr Vorsitzender des Innenausschusses Hering,
sehr geehrte Damen und Herren,

wir bedanken uns für die Übersendung des Entwurfs eines
Gesetzes zur Neufassung des Hessischen
Sicherheitsüberprüfungs- und Verschlusssachengesetz und zur
Änderung einer weiteren Vorschrift.

Nach Befragung unserer Mitglieder können wir mitteilen, dass
unsererseits keine Änderungs- oder Ergänzungswünsche zur
avisierten Neufassung des Hessischen Sicherheitsüberprüfungs-
und Verschlusssachengesetzes bestehen.

Verband der kreisfreien und
kreisangehöriger Städte im
Land Hessen

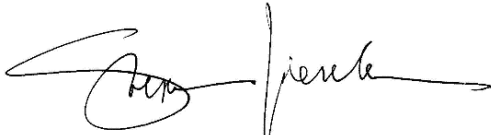
Frankfurter Straße 2
65189 Wiesbaden

Telefon: (0611) 1702-0
Telefax: (0611) 1702-17

posteingang@hess-staedtetag.de
www.hess-staedtetag.de

Dient die Überarbeitung des Hessischen Sicherheitsüberprüfungs- und Verschlusssachengesetzes dazu, ein vergleichbares Sicherheitsniveau zwischen Bund und Land zu gewährleisten, so ist dies auch im Hinblick auf das gestiegene Sicherheitsniveau nicht zu beanstanden.

Mit freundlichen Grüßen

A handwritten signature in black ink, appearing to read 'Stephan Gieseler', with a long horizontal stroke extending to the right.

Stephan Gieseler
Geschäftsführender Direktor

Hessischer Landtag
z.Hd. Frau Kehrein, Herr Dransmann
Schloßplatz 1-3

65183 Wiesbaden

Landesgeschäftsstelle
Dwight-D.-Eisenhower-Str. 9
65197 Wiesbaden
Telefon (0611/97 45 44 04)
Telefax (0611/97 45 44 06)
kontakt@dpolg-hessen.de
www.dpolghessen.de

17.07.2026

**Gesetz zur Neufassung des Hessischen Sicherheitsüberprüfungs- und
Verschlusssachengesetzes und zur Änderung einer weiteren Vorschrift
– Drucks. 21/4531 –**

Sehr geehrte Mitglieder des Innenausschusses,
sehr geehrte Frau Kehrein, sehr geehrter Herr Dransmann,

die DPoIG Hessen bedankt sich für die Möglichkeit der Stellungnahme zum o.g. Gesetzentwurf.

Die DPoIG Hessen sieht den Gesetzentwurf als positive Fortschreitung und Anpassung des Gesetzes an die aktuelle Lage und Sicherheitssituation in Hessen und Europa.
Besonders positiv sticht hervor, dass der Gesetzentwurf nicht nur eine Verlängerung des auslaufenden Gesetzes darstellt, sondern eine Erweiterung und Anpassung an aktuelle Entwicklungen nachvollzogen werden.

Ein Schutz der Mitarbeitenden in sicherheitsrelevanten Bereichen durch Überprüfung von Personen, die mit deren Daten Umgang haben und deren Verpflichtung zur Verschwiegenheit nach § 2 a des Gesetzes, ist ein wichtiger Aspekt aus Sicht der Gewerkschaft um den Mitarbeiterschutz voranzubringen und einer geänderten Gefährdungssituation Rechnung zu tragen.

Besonders die mit der Möglichkeit der Überprüfung in § 3 Abs. 3 einbezogenen Personen erhöhen den sicherheitsrelevanten Anspruch in heutiger Zeit und führen zu einer Verbesserung im Vergleich zur Vergangenheit.

In § 5a erscheint es so, als ob die dort aufgeführten Geheimschutzbeauftragten oder Vertreter in alleiniger Verantwortung für die Einhaltung und Umsetzung des Gesetzes ständen, ein Zusatz zum Beispiel mit dem Wortlaut: „Die Pflichten und grundsätzlichen Verantwortlichkeiten der jeweiligen Behördenleitungen und Führungskräfte bleiben davon unberührt.“ wäre wünschenswert gewesen. Hierdurch wäre zum Ausdruck gekommen, dass es sich bei der Überwachung und Umsetzung des

Gesetzes und der damit verbundenen Hintergründe um eine Gemeinschaftsaufgabe handelt und es hätte die Verantwortlichen nochmals zu einem entsprechenden Handeln aufgefordert.

In den Reisebeschränkungen nach § 15 wird von Seiten der DPolG eine hinnehmbare und verhältnismäßige Maßnahme gesehen, die keinen Grund zur Beanstandung gibt.

Weiterhin wird auch die Datenerhebung nach § 16 Abs. 2 als unkritisch angesehen, da diese Maßnahme nur als sekundäre Option angelegt ist.

Weitere Rechte der Betroffenen scheinen gewahrt bzw. entsprechend berücksichtigt, so wie beispielhaft in § 18 die Vernichtung der Akten, in § 21 die Löschung oder die Datenschutzbestimmungen aus § 32 a.

Wie bereits ausgeführt, steht die DPolG der Neufassung des Gesetzes positiv gegenüber.

A handwritten signature in black ink, consisting of a large, stylized 'G' followed by a vertical line and a small flourish.

Alexander Glunz
Landesvorsitzender



UNIVERSITÄT
ZU KÖLN

Universität zu Köln • Albertus-Magnus-Platz • 50923 Köln

Hessischer Landtag
Vorsitzender des Innenausschusses
Herrn Thomas Hering, MdL
Schlossplatz 1–3
65183 Wiesbaden

Rechtswissenschaftli-
che Fakultät

Institut für Digitalisie-
rung

Lehrstuhl für Öffentli-
ches Recht, Informati-
onsrecht und Rechts-
theorie

Prof. Dr. Indra Spiecker
gen. Döhmann, LL.M.
(Georgetown)

Köln, den 10. Juli 2026

Stellungnahme zum Gesetzentwurf der Landesregierung für ein „Gesetz zur Neufassung des Hessischen Sicherheitsüberprüfungs- und Ver- schlusssachengesetzes und zur Änderung einer weiteren Vorschrift“

Sehr geehrter Herr Hering,

ich bedanke mich, auch im Namen der mitwirkenden Mitarbeiterin Amina Gutjahr, für die Ehre und das Vertrauen des Hessischen Landtags, zum o.g. Gesetzentwurf Stellung zu nehmen. Meine Stellungnahme finden Sie anbei.

Mit freundlichen Grüßen

A handwritten signature in blue ink, appearing to read 'I. Spiecker'.

Prof. Dr. I. Spiecker gen. Döhmann, LL.M. (Georgetown)



Stellungnahme
zum Gesetzentwurf der Landesregierung
für ein
**„Gesetz zur Neufassung des Hessischen Sicherheits-
überprüfungs- und Verschlusssachengesetzes und
zur Änderung einer weiteren Vorschrift“**

Prof. Dr. I. Spiecker gen. Döhmann, LL.M (Georgetown)

unter Mitarbeit von Amina Gutjahr

Universität zu Köln

Institut für Digitalisierung

Lehrstuhl für Öffentliches Recht, Informationsrecht und Rechtstheorie



Inhaltsverzeichnis

I. Einleitung	5
II. Geplante Neuerungen im HSÜVG-E	6
1. Ausweitung des Anwendungsbereichs und Schutzzwecks	6
2. Erweiterung des Begriffs des Sicherheitsrisikos	6
3. Anpassungen bei der Sicherheitsüberprüfung	7
4. Ausweitung der Ermittlungsmaßnahmen.....	8
5. Deutliche Ausweitung der Angaben in der Sicherheitserklärung.....	9
6. Änderungen für den Abschluss der Sicherheitsüberprüfung.....	10
7. Ergänzungen für sicherheitserhebliche Erkenntnisse nach Abschluss der Sicherheitsüberprüfung.....	10
8. Änderungen und Konkretisierungen für die Sicherheits(überprüfungs)akte und deren Aufbewahrungsdauer	11
9. Änderungen für die Sicherheitsüberprüfung im nicht öffentlichen Bereich	12
10. Anpassungen in Bezug auf den Datenschutz und das Zitiergebot.....	13
11. Änderung des Verfassungsschutzkontrollgesetzes.....	13
III. Vergleich mit dem SÜG des Bundes.....	14
1. Strengere hessische Regelungen	14
a) Definition der Verschlussache	14
b) Sicherheitsüberprüfung	14
c) Ermittlungsmaßnahmen	15
2. Weitreichendere Regelungen im SÜG	16
3. Eigenständige hessische Regelungen.....	17
IV. Kritische Würdigung.....	17
1. Notwendige Berücksichtigung der Gesamtbelastung durch Informationseingriffe....	17
2. Einwilligung und Freiwilligkeit bei Sicherheitsüberprüfungen	19
3. Internetrecherche.....	19
4. Betroffenenrechte.....	21
5. Weitestgehende Gleichstellung von betroffener und einbezogener Person.....	21
6. Fehlende Bestimmtheit bei Datenabgleich von Lichtbildern	22



7. Angaben zu Beziehungen zu kriminellen oder terroristischen Vereinigungen und Personen, die verfassungsfeindliche Bestrebungen verfolgen und Kontakte zu ausländischen Nachrichtendiensten.....	23
8. Angaben zu eigenen Internetseiten, Benutzernamen und Nutzer-IDs	23
V. Fazit.....	24

I. Einleitung

Mit dem Entwurf für ein „Gesetz zur Neufassung des Hessischen Sicherheitsüberprüfungs- und Verschlusssachengesetzes und zur Änderung einer weiteren Vorschrift“ (HSÜVG-E) vom 28.5.2026, LT-Drs. 21/4531, beabsichtigt die hessische Landesregierung, den Schutz von Verschlusssachen und sicherheitsempfindlichen Bereichen an die veränderten sicherheitspolitischen Rahmenbedingungen anzupassen.

Das Sicherheitsüberprüfungs- und Verschlusssachenrecht bildet einen zentralen Baustein des präventiven Geheimschutzes. Es soll sicherstellen, dass sicherheitsempfindliche Tätigkeiten und der Zugang zu Verschlusssachen nur Personen übertragen werden, bei denen keine Sicherheitsrisiken bestehen. Nach der Gesetzesbegründung orientiert sich der Gesetzentwurf ausdrücklich an dem erst Anfang dieses Jahres novellierten Sicherheitsüberprüfungsgesetz des Bundes (SÜG), um ein bundesweit einheitliches Sicherheitsniveau trotz der föderal geprägten Strukturen zu gewährleisten. Während das bisherige HSÜVG in seiner Grundkonzeption erhalten bleibt, sollen insbesondere die Möglichkeiten zur Feststellung von Sicherheitsrisiken erweitert und bestehende Ermittlungsbefugnisse präzisiert werden. Hintergrund ist die zunehmende Bedeutung hybrider Bedrohungen, von Cyberangriffen, Spionage, Sabotage sowie von extremistischen Einflussnahmen auf sicherheitsempfindliche Bereiche. Die Novellierung fügt sich damit in eine allgemeine sicherheitspolitische Entwicklung ein, die auf einen stärkeren Schutz staatlicher Sicherheitsinteressen und sensibler Informationen abzielt und sich auch in anderen aktuellen Gesetzgebungsvorhaben des Bundes widerspiegelt.¹ Der Entwurf führt die bisherige grundlegende Systematik und Ausrichtung des HSÜVG fort, sieht aber eine Erweiterung des Anwendungsbereichs sowie eine deutliche Ausweitung der Überprüfungsmaßnahmen und umfassendere Befugnisse zur Datenerhebung vor.

Die Stellungnahme beschränkt sich auf die Analyse der wesentlichen Änderungen (II.). Die vergleichende Untersuchung zum SÜG des Bundes zeigt, dass der HSÜVG-E die bundesrechtliche Konzeption weitgehend übernimmt. Die Grundstruktur des Gesetzes, die Überprüfungsarten, die Verfahrensregelungen und die datenschutzrechtlichen Vorgaben orientieren sich eng am SÜG, allerdings mit punktuellen materiellen Anpassungen, die im Folgenden dargestellt sind (III.). Die Regelungen des HSÜVG-E – sowohl geplante Änderungen als auch nach dem geltenden HSÜVG bereits bestehende Regelungen – werden abschließend kritisch gewürdigt (IV.).

¹ In dieser Linie reiht sich z.B. das Vorhaben der Koalitionsparteien zur Reform des Informationsfreiheitsgesetzes ein, welche die Hürden für den Zugang zu staatlichen Informationen erheblich verschärfen soll.

II. Geplante Neuerungen im HSÜVG-E

1. Ausweitung des Anwendungsbereichs und Schutzzwecks

Das Gesetz erfasst nach wie vor Personen, die sicherheitsempfindliche Tätigkeiten ausüben bzw. ausüben sollen und ermöglicht für diese die Durchführung einer Sicherheitsüberprüfung bzw. Wiederholungsüberprüfung, § 1 Abs. 1 S. 1 HSÜVG-E. Sicherheitsempfindliche Tätigkeiten übt nach § 1 Abs. 2 HSÜVG-E aus, wer Zugang zu Verschlusssachen hat oder ihn sich verschaffen kann (Nr. 1) oder wer in einer sicherheitsrelevanten Stelle oder Einrichtung tätig ist (Nr. 2–6). Verschlusssachen werden nach ihrer Schutzbedürftigkeit in vier Geheimhaltungsgrade eingeordnet, an die jeweils unterschiedliche Sicherheitsstufen und -überprüfungen geknüpft sind. Die Geheimhaltungsgrade sind STRENG GEHEIM, GEHEIM, VS-VERTRAULICH und VS-NUR FÜR DEN DIENSTGEBRAUCH. Für den Zugang zu einer Verschlusssache der drei erstgenannten Grade sind unterschiedliche Sicherheitsüberprüfungen durchzuführen, der Zugang zu VS-NUR FÜR DEN DIENSTGEBRAUCH erfordert keine Sicherheitsüberprüfung. Je nach in Frage stehender sicherheitsempfindlicher Tätigkeit wird gem. § 6 HSÜVG-E entweder eine einfache Sicherheitsüberprüfung, § 7 HSÜVG-E (Ü1), eine erweiterte Sicherheitsüberprüfung, § 8 HSÜVG-E (Ü2), oder eine erweiterte Sicherheitsüberprüfung mit Sicherheitsermittlungen, § 9 HSÜVG-E (Ü3), durchgeführt.

Zum personellen Anwendungsbereich neu hinzu kommen sollen insbesondere Beschäftigte, die zwar nicht selbst beim Landesamt für Verfassungsschutz (LfV) tätig sind, jedoch im Rahmen ihrer Tätigkeit Zugang zu besonders sensiblen Personal- oder Organisationsdaten des LfV besitzen (Nr. 6). Hintergrund ist die Erkenntnis, dass bereits Informationen über die Identität von Mitarbeitenden des LfV für fremde Nachrichtendienste oder extremistische Akteure von erheblichem Interesse sein können.

Der Gesetzentwurf trägt damit dem Insider-Risiko stärker Rechnung. Nicht mehr allein der Zugang zu geheimhaltungsbedürftigen Informationen, sondern bereits der Zugang zu besonders sensiblen Verwaltungsinformationen kann künftig eine Sicherheitsüberprüfung erforderlich machen.

Außerdem soll mit § 1 Abs. 1 S. 4 HSÜVG-E der vorbeugende personelle Sabotageschutz, der dem Schutz lebenswichtiger und verteidigungswichtiger Einrichtungen dient, explizit als Ziel des Gesetzes aufgenommen werden.

2. Erweiterung des Begriffs des Sicherheitsrisikos

Ein zentraler Begriff im Sicherheitsüberprüfungs- und Verschlusssachenrecht ist der des Sicherheitsrisikos. Ergibt die Sicherheitsüberprüfung ein Sicherheitsrisiko der betroffenen oder einbezogenen Person, ist dies nach § 12 Abs. 1 HSÜVG-E der zuständigen Stelle mitzuteilen, die daraufhin entscheidet, ob das Sicherheitsrisiko der sicherheitsempfindlichen Tätigkeit entgegensteht, § 12 Abs. 3 HSÜVG-E.

Das bisherige Gesetz stellte dabei vor allem auf Zweifel an der Zuverlässigkeit, mögliche Erpressbarkeit durch Anbahnungs- oder Werbeversuche ausländischer Nachrichtendienste und krimineller oder terroristischer Vereinigungen sowie Zweifel am Bekenntnis zur freiheitlichen demokratischen Grundordnung ab. Mit § 2 Abs. 7 Nr. 2 lit. c HSÜVG-E sollen künftig auch Beziehungen zu Personenzusammenschlüssen und Einzelpersonen, die sicherheitsrelevante Bestrebungen nach § 4 Abs. 1 S. 2 und 3 i.V.m. § 3 Abs. 1 BVerfSchG verfolgen, in die Bestimmung des Sicherheitsrisikos einbezogen werden.

Damit reagiert der Gesetzgeber auf die Entwicklung, dass extremistische Aktivitäten zunehmend außerhalb klassischer Vereins- oder Organisationsstrukturen stattfinden und Kontakt auch rein privat zu Einzelpersonen, unabhängig von deren Zugehörigkeit zu einem Personenzusammenschluss bestehen kann.² Die Sicherheitsüberprüfung orientiert sich künftig deshalb stärker am tatsächlichen Gefährdungspotenzial einer Person und weniger ausschließlich an einer formalen Organisationsmitgliedschaft.

Darüber hinaus soll § 2 Abs. 7 S. 3 HSÜVG-E ergänzt werden, der Erkenntnisse über Personen nach § 3 Abs. 3 S. 1 in die einfache Sicherheitsüberprüfung nach § 7 (Ü1) einbezieht. § 3 Abs. 3 regelt die Personen, die in die Sicherheitsüberprüfungen nach §§ 8 und 9 (Ü2 und 3) einbezogen werden sollen. Dies sind Ehe- und Lebenspartner:innen sowie Personen, die mit der betroffenen Person in einer Lebensgemeinschaft leben, sofern sie volljährig sind. In die einfache Sicherheitsüberprüfung nach § 7 sind eigentlich keine weiteren Personen einzubeziehen, allerdings hat die betroffene Person nach § 11 bei jeder Sicherheitsüberprüfung eine Sicherheitserklärung abzugeben. In dieser Erklärung sind nach § 11 Abs. 1 Nr. 19 auch Angaben zu Ehe- und Lebenspartner:innen zu machen. Die Erweiterung des Risikobegriffs in § 2 Abs. 7 S. 3 HSÜVG-E stellt sicher, dass auch bei einer einfachen Sicherheitsüberprüfung nach § 7 Erkenntnisse über Ehe- und Lebenspartnerschaften, die aus der Sicherheitserklärung gewonnen wurden, zu einem Sicherheitsrisiko der betroffenen Person führen können.

3. Anpassungen bei der Sicherheitsüberprüfung

Die Grundstruktur der drei Überprüfungsarten (Ü1, Ü2 und Ü3) bleibt unverändert. Dennoch werden einzelne Regelungen weiterentwickelt. Insbesondere werden die Möglichkeiten erweitert, zusätzliche Ermittlungsmaßnahmen durchzuführen, wenn sich während einer Sicherheitsüberprüfung sicherheitserhebliche Erkenntnisse ergeben.

Eine einfache Sicherheitsüberprüfung (Ü1) nach § 7 HSÜVG ist bislang durchzuführen für Personen, die Zugang zu als VS-VERTRAULICH eingestuften Verschlusssachen erhalten sollen, die bei einer Behörde oder öffentlichen Stelle tätig sind, die i.S.v. § 1 Abs. 2 Nr. 3 HSÜVG zum Sicherheitsbereich erklärt wurde. Aufgenommen werden in diesen Katalog

² Vgl. Eicholt, Das Gesetz zu Modernisierung des Sicherheitsüberprüfungsgesetzes, GSZ 2026, 75 (76).

sollen mit § 7 Abs. 1 Nr. 3 HSÜVG-E ferner Personen, die eine Tätigkeit i.S.v. § 1 Abs. 2 Nr. 6 HSÜVG-E ausüben – diese Modalität soll mit dem Entwurf ebenfalls neu in den Anwendungsbereich des HSÜVG aufgenommen werden³. Bei diesen Tätigkeiten handelt sich um solche bei öffentlichen Stellen, die Einblick in die Personalangelegenheiten des Landesamtes für Verfassungsschutz haben.

Eine erweiterte Sicherheitsüberprüfung (Ü2) nach § 8 HSÜVG ist für Personen durchzuführen, die Zugang zu als GEHEIM eingestufte Verschlusssachen erhalten sollen, die Zugang zu einer großen Zahl von als VS-VERTRAULICH eingestuften Verschlusssachen haben (sollen) oder die bei einer Sicherheitsempfindlichen Stelle i.S.v. § 1 Abs. 2 Nr. 4 HSÜVG tätig sind, welche Teil einer lebens- oder verteidigungswichtigen Einrichtung ist. An der erweiterten Sicherheitsüberprüfung sollen keine Änderungen vorgenommen werden.

Eine erweiterte Sicherheitsüberprüfung mit Sicherheitsübermittlung (Ü3) nach § 9 HSÜVG wird durchgeführt bei Personen, die Zugang zu als STRENG GEHEIM eingestuften Verschlusssachen erhalten sollen, die mit einer hohen Zahl von als GEHEIM eingestuften Verschlusssachen zu tun haben oder die beim Landesamt für Verfassungsschutz tätig sind. In den Anwendungsbereich der Sicherheitsüberprüfung Ü3 sollen mit § 9 Abs. 1 Nr. 4 HSÜVG-E Personen aufgenommen werden, die nicht *beim* LfV tätig sind, aber eine Tätigkeit *für* das LfV wahrnehmen, „die eine Überprüfung rechtfertigt“. Außerdem soll Satz 2 angefügt werden, wonach diese Personen auch schon vor Abschluss der Ü3 für das LfV tätig werden dürfen, sofern sie nicht in den dienstlichen Räumlichkeiten des LfV tätig sind und nur Zugriff zu als VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuften Verschlusssachen erhalten.

4. Ausweitung der Ermittlungsmaßnahmen

Den umfangreichsten materiellen Änderungen unterliegt § 10 des Gesetzentwurfs. § 10 HSÜVG regelt die Maßnahmen, die das Landesamt für Verfassungsschutz als mitwirkende Behörde je nach Art der Sicherheitsüberprüfung durchführt. Bereits nach geltendem Recht ist der Maßnahmenkatalog umfangreich. Er umfasst insbesondere die sicherheitsmäßige Bewertung der Angaben in der Sicherheitserklärung, Auskünfte aus dem Bundeszentralregister und dem Gewerbezentralregister, Anfragen bei Polizei- und Sicherheitsbehörden sowie – seit der Novelle 2019 – unter bestimmten Voraussetzungen die Anforderung einer SCHUFA-Datenübersicht sowie die Einsichtnahme in allgemein zugängliche Internetseiten und öffentlich sichtbare Bereiche sozialer Netzwerke. Damit bestand bereits vor der Neufassung ein differenziertes Instrumentarium zur Aufklärung sicherheitsrelevanter Erkenntnisse. Der Gesetzentwurf ersetzt dieses Instrumentarium nicht, sondern erweitert und präzisiert es.

³S.o., S. 3.

Hierzu gehört insbesondere eine verbesserte Identitätsprüfung durch zusätzliche Melde-registerauskünfte (§ 10 Abs. 1 Nr. 5), die es ermöglichen soll, die Angaben der betroffenen Person zu ihrer Meldeadresse aus der Sicherheitserklärung überprüfen zu können. Laut der Gesetzesbegründung soll ein Datenabgleich bei den Meldebehörden allerdings nicht bei jeder Sicherheitsüberprüfung, sondern nur erfolgen, soweit dies erforderlich ist.

Besonders hervorzuheben ist außerdem die ausdrückliche gesetzliche Grundlage für die Auswertung allgemein zugänglicher Informationen im Internet und in sozialen Netzwerken nach § 10 Abs. 1a S. 3 HSÜVG-E. Bei Sicherheitsüberprüfungen nach §§ 8 und 9 kann diese Auswertung auch für die einbezogenen Personen erfolgen. Für diese wurde eine redakti-onelle Änderung vorgenommen und das Wort „eigene“ vor Internetseiten gestrichen, um zu verdeutlichen, dass nicht nur von der betroffenen oder einbezogenen Person selbst erstellte Internetseiten einbezogen werden, sondern eine umfassende Prüfung aller im Internet frei zugänglichen Informationen erfolgt. Aus der Gesetzesbegründung ergibt sich, dass die Streichung des Wortes „eigene“ nicht dazu führen solle, dass Daten, die durch einen Cyberangriff oder ein Datenleck versehentlich in den öffentlichen Teil des Internets gelangt sind, in die Sicherheitsüberprüfung einbezogen werden. Solche Daten seien vielmehr wie nicht öffentliche Daten zu behandeln.⁴

5. Deutliche Ausweitung der Angaben in der Sicherheitserklärung

Auch für die Sicherheitserklärung nach § 11 HSÜVG-E, die von jeder betroffenen Person abzugeben ist, sollen einige weitreichende Änderungen vorgenommen werden. Zunächst sieht § 11 Abs. 1 Nr. 12a HSÜVG-E vor, dass künftig auch Angaben zu Beziehungen zu krim-inellen oder terroristischen Vereinigungen gemacht werden müssen. Außerdem sollen auch Angaben über Beziehungen zu Personenzusammenschlüssen oder Einzelpersonen, die sicherheitsrelevante Bestrebungen nach § 4 Abs. 1 S. 2 und 3 i.V.m. § 3 Abs. 1 BVerf-SchG verfolgen, in die Sicherheitserklärung einbezogen werden.

Eine weitere erhebliche Ausweitung betrifft die nunmehr erforderliche Einreichung von Lichtbildern der einbezogenen Personen, § 11 Abs. 1 S. 2 HSÜVG-E. Ein Lichtbild der be-troffenen Person ist auch nach dem geltenden HSÜVG einzureichen. Zudem soll Satz 3 angefügt werden, wonach die Lichtbilder auch in elektronischer Form verlangt werden können.

Mit dieser Änderung soll bezweckt werden, dass die Identifikation der betroffenen und der einbezogenen Personen erleichtert wird. Die Abgabe von Lichtbildern in elektroni-scher Form soll zudem den Abgleich mit Datenbanken sowie die Internetrecherche er-leichtern.⁵

⁴ LT-Drs. 21/4531 v. 28.05.2026, S. 30.

⁵ LT-Drs. 21/4531 v. 28.05.2026, S. 31.

Schließlich sieht der Entwurf vor, § 11 einen Satz 6 anzufügen, wonach nach Abgabe der Sicherheitserklärung auftretende Anzeichen die darauf hindeuten, dass die betroffene oder eine einbezogene Person Beziehungen zu ausländischen Nachrichtendiensten, kriminellen oder terroristischen Vereinigungen oder zu Personenzusammenschlüssen oder Einzelpersonen, die relevante Bestrebungen nach dem BVerfSchG verfolgen hat oder sie in Anbahnungs- oder Werbungsversuche ausländischer Nachrichtendienste verwickelt ist, unverzüglich der zuständigen Stelle anzuzeigen sind.

6. Änderungen für den Abschluss der Sicherheitsüberprüfung

§ 12 HSÜVG regelt den Abschluss der Sicherheitsüberprüfung. Die zuständige Stelle entscheidet auf Grundlage der Erkenntnisse der mitwirkenden Behörde, ob ein Sicherheitsrisiko vorliegt. Ergibt die Gesamtwürdigung, dass kein Sicherheitsrisiko besteht, kann die betroffene Person mit der sicherheitsempfindlichen Tätigkeit betraut werden. Bei sicherheitserheblichen Erkenntnissen ist die betroffene Person grundsätzlich anzuhören; die Entscheidung trifft jedoch die zuständige Stelle und nicht die mitwirkende Behörde. Diese Grundentscheidung bleibt auch im Gesetzentwurf erhalten. Die wesentlichen Änderungen betreffen vielmehr die Ausgestaltung der Entscheidungsmöglichkeiten der zuständigen Stelle.

Die wichtigste Neuerung besteht mit der Ergänzung von § 12 Abs. 3 um einen Satz 3 darin, dass die zuständige Stelle künftig ausdrücklich Auflagen mit der Entscheidung über das Nichtvorliegen eines Sicherheitsrisikos verbinden kann. Bislang sah das Gesetz nur die Feststellung vor, dass ein Sicherheitsrisiko besteht oder nicht besteht. Die Aufnahme dieser Möglichkeit eröffnet eine abgestufte Entscheidungsmöglichkeit zwischen einer uneingeschränkten Zulassung und dem vollständigen Ausschluss von der sicherheitsempfindlichen Tätigkeit.

Neu hinzugefügt werden soll ferner ein Satz 4 in § 12 Abs. 3, der die Verpflichtung der zuständigen Stelle enthält, die mitwirkende Behörde zu informieren, wenn sie von deren sicherheitsfachlicher Bewertung abweicht. Dadurch soll die Kommunikation zwischen entscheidender und mitwirkender Behörde verbessert werden.⁶

7. Ergänzungen für sicherheitserhebliche Erkenntnisse nach Abschluss der Sicherheitsüberprüfung

Bereits das geltende HSÜVG verpflichtet die zuständige Stelle und die mitwirkende Behörde in § 13, sich gegenseitig über nachträglich bekannt gewordene sicherheitserhebliche Erkenntnisse zu unterrichten. Auch Veränderungen der persönlichen und dienstlichen Verhältnisse sind bereits teilweise mitzuteilen, Abs. 3. Insofern werden beispielhaft – nicht

⁶ LT-Drs. 21/4531 v. 28.05.2026, S. 32.

abschließend – einige relevante Änderungen aufgelistet. Hierzu zählen die Umsetzung, Abordnung Versetzung oder das Ausscheiden aus dem Dienst (Nr. 1), Änderungen des Namens des Wohnsitzes oder der Staatsangehörigkeit (Nr. 2), Anhaltspunkt für Überschuldung, Pfändungs- und Überweisungsbeschlüsse sowie laufende Insolvenzverfahren (Nr. 3), laufende Straf- und Disziplinarverfahren bzw. dienst- und arbeitsrechtliche Maßnahmen (Nr. 4) und die Aufnahme einer Nebentätigkeit (Nr. 5). In die beispielhafte Auflistung soll in § 13 Abs. 3 Nr. 2 HSÜVG-E auch die Änderung des Vornamens und des Geschlechts aufgenommen werden. Auch hierfür wird als Begründung auf die erleichterte Identitätsfeststellung verweisen.⁷

Durch Ergänzung eines Abs. 4 soll der zuständigen Stelle außerdem die Möglichkeit eröffnet werden, der betroffenen Person auch vor der endgültigen Entscheidung über das Vorliegen eines Sicherheitsrisikos die Ausübung der sicherheitsrelevanten Tätigkeit zu entziehen, „sofern die besondere Bedeutung der Erkenntnisse und die Art der sicherheitsempfindlichen Tätigkeit dies erfordern und die Untersagung keinen Aufschub duldet“.

Die Begründung stellt heraus, dass sicherheitserhebliche Erkenntnisse jederzeit auftreten können und deshalb auch zwischen zwei regulären Sicherheitsüberprüfungen zeitnah berücksichtigt werden müssen. Ziel sei eine kontinuierliche sicherheitsmäßige Bewertung und nicht lediglich eine punktuelle Überprüfung in größeren Zeitabständen. Für die vorläufige Untersagung verlangt die Landesregierung ausdrücklich dringende Gründe und ein besonderes öffentliches Interesse; außerdem sei das Verfahren anschließend beschleunigt fortzuführen.⁸

8. Änderungen und Konkretisierungen für die Sicherheits(überprüfungs)akte und deren Aufbewahrungsdauer

§ 17 HSÜVG regelt die Führung der Sicherheitsakte durch die zuständige Stelle sowie der Sicherheitsüberprüfungsakte durch die mitwirkende Behörde. Bereits nach geltendem Recht gilt, dass die Sicherheitsakte keine Personalakte ist und grundsätzlich nur der aktuell zuständigen Dienststelle zur Verfügung steht. Bei einem Wechsel der Dienststelle oder des Dienstherrn wird die Sicherheitsakte an die neue Dienststelle abgegeben, sofern dort ebenfalls eine sicherheitsempfindliche Tätigkeit ausgeübt werden soll.

Neu eingefügt werden soll in § 17 Abs. 3 ein zusätzlicher Satz 3. Danach kann die Sicherheitsakte bereits vor einem beabsichtigten Wechsel des Dienstherrn oder der Dienststelle der zukünftigen Dienststelle zur Einsicht zugänglich gemacht werden. Eine Übermittlung

⁷ LT-Drs. 21/4531 v. 28.05.2026, S. 32.

⁸ LT-Drs. 21/4531 v. 28.05.2026, S. 32.

der Akte soll zu diesem Zeitpunkt allerdings noch nicht erfolgen. Vielmehr wird lediglich eine kurzfristige Einsicht ermöglicht.

Die Landesregierung begründet die Änderung ausdrücklich mit einer praktischen Gesetzeslücke. In der Praxis müsse häufig bereits vor einer Versetzung oder einem Dienstherrnwechsel geklärt werden, ob eine Person überhaupt für die neue sicherheitsempfindliche Tätigkeit geeignet sei. Das bisherige Gesetz ermögliche dies nicht ausreichend. Die Einsicht solle daher ausschließlich der Vorbereitung der Entscheidung über den Wechsel dienen.⁹

§ 18 HSÜVG regelt die Dauer der Aufbewahrung sowie die Vernichtung der Sicherheitsakten und Sicherheitsüberprüfungsakten nach Abschluss der Sicherheitsüberprüfung oder nach Beendigung der sicherheitsempfindlichen Tätigkeit. § 18 Abs. 2 soll um einen neuen Satz ergänzt werden, der die Vernichtung der Sicherheitsakte bzw. Sicherheitsüberprüfungsakte unverzüglich nach dem Tod der betroffenen Person vorsieht, da nach dem Tod kein Interesse mehr am Erhalt der Informationen bestehe.¹⁰

9. Änderungen für die Sicherheitsüberprüfung im nicht öffentlichen Bereich

Der Fünfte Teil des Gesetzentwurfs enthält lediglich punktuelle Änderungen der Vorschriften über Sicherheitsüberprüfungen im nicht öffentlichen Bereich. Anders als im öffentlichen Bereich werden hier weder neue Ermittlungsmaßnahmen eingeführt noch der Umfang der Sicherheitsüberprüfung wesentlich erweitert. Vielmehr dienen die Änderungen überwiegend der Klarstellung bestehender Rechtsfolgen, der Harmonisierung mit den Vorschriften für öffentliche Stellen sowie der Schließung einzelner praktischer Regelungslücken.

Der HSÜVG-E sieht insofern zunächst vor, § 26 um einen Satz 5 zu ergänzen, wonach eine Beschäftigung an einer sicherheitsempfindlichen Stelle ohne erfolgreiche Sicherheitsüberprüfung unzulässig ist. Ebenso darf die Tätigkeit nach Entzug der Ermächtigung oder Zulassung nicht fortgeführt werden. Nach der Gesetzesbegründung soll hierdurch lediglich die bereits bestehende Rechtslage ausdrücklich klargestellt werden.¹¹

Materielle Auswirkungen sind hiermit kaum verbunden. Bereits nach bisherigem Recht setzte die Wahrnehmung einer sicherheitsempfindlichen Tätigkeit den erfolgreichen Abschluss der Sicherheitsüberprüfung voraus. Die Ergänzung erhöht jedoch die Rechtsklarheit und erleichtert die praktische Anwendung durch private Arbeitgeber.

Die Änderungen der §§ 27 und 28 verfolgen das Ziel, die Verfahrensabläufe im nichtöffentlichen Bereich an diejenigen für öffentliche Stellen anzugleichen.

⁹ LT-Drs. 21/4531 v. 28.05.2026, S. 33.

¹⁰ LT-Drs. 21/4531 v. 28.05.2026, S. 33.

¹¹ LT-Drs. 21/4531 v. 28.05.2026, S. 33.

In § 27 Abs 2 HSÜVG-E soll klargestellt werden, dass nachträgliche Änderungen der Sicherheitserklärung denselben Anforderungen an Vollständigkeit und Richtigkeit unterliegen wie die erstmalige Erklärung. Zu diesem Zweck verweist die Vorschrift nun ausdrücklich auf § 25 Satz 3 HSÜVG-E.

§ 28 Abs. 1 HSÜVG-E soll neu gefasst und sprachlich an § 13 HSÜVG-E angepasst werden. Wie in § 13 HSÜVG-E wird hervorgehoben, dass die Aufzählung mitteilungspflichtiger Veränderungen nicht abschließend ist. Darüber hinaus werden Änderungen des Vornamens und des Geschlechts ausdrücklich als meldepflichtige Umstände aufgenommen, um die eindeutige Identifizierung der betroffenen Person sicherzustellen.

Diese Änderungen besitzen überwiegend klarstellenden Charakter. Sie schaffen einen Gleichlauf zwischen öffentlichem und nichtöffentlichem Bereich und vereinheitlichen die Verwaltungspraxis, ohne den Umfang der Sicherheitsüberprüfung wesentlich zu erweitern.

§ 29 soll um eine ausdrückliche Regelung ergänzt werden, wonach der interne Datenschutzbeauftragte der nicht öffentlichen Stelle keinen Zugang zu den Sicherheitsakten erhalten darf. Die Regelung stärkt den Geheimschutz sensibler Sicherheitsakten. Zugleich beschränkt sie die interne Datenschutzkontrolle innerhalb des Unternehmens.

10. Anpassungen in Bezug auf den Datenschutz und das Zitiergebot

§ 32a HSÜVG verweist auf die Anwendbarkeit des Hessischen Datenschutz- und Informationsfreiheitsgesetzes (HDSIG) und regelt die datenschutzrechtliche Kontrolle der nach dem HSÜVG erfolgenden Datenverarbeitung. Die Vorschrift wurde bereits durch die Novelle 2019 eingeführt und dient dazu, das Verhältnis zwischen den Regelungen des HSÜVG und dem Datenschutzrecht zu bestimmen.

Hier sollen lediglich redaktionelle Änderungen vorgenommen werden, die die genaue Gesetzesbezeichnung und ihre Fundstelle im Gesetzesblatt enthalten.

Mit § 32b HSÜVG-E soll erstmals eine eigenständige Vorschrift eingeführt werden, die das Zitiergebot des Art. 63 Abs. 2 HV umsetzt, indem auf mögliche Einschränkungen des Grundrechts auf informationelle Selbstbestimmung aus Art. 12a HV hingewiesen wird.

11. Änderung des Verfassungsschutzkontrollgesetzes

Schließlich sieht der HSÜVG-E eine Änderung von § 1 Abs. 5 des hessischen Verfassungsschutzkontrollgesetzes (VerfSchutzKG) vor. Gegenstand von § 1 Abs. 5 VerfSchutzKG ist die parlamentarische Kontrollkommission, die die Tätigkeiten des LfV kontrolliert. Zu Beginn jeder Wahlperiode werden die Mitglieder der parlamentarischen Kontrollkommission vom Landtag aus seiner Mitte besetzt, § 1 Abs. 2 VerfSchutzKG. § 1 Abs. 5 VerfSchutzKG sieht vor, dass die parlamentarische Kontrollkommission nach Ablauf der Legislaturperiode oder der Auflösung des Landtags so lange im Amt bleibt, bis eine neue Kontrollkommission gewählt wurde und ihr Amt aufgenommen hat. Nach § 3 Abs. 4 Nr. 1 HSÜVG ist

für Mitglieder des Landtags keine Sicherheitsüberprüfung durchzuführen. Wird ein Mitglied der parlamentarischen Kontrollkommission nicht erneut in den Landtag gewählt, bleibt aber noch bis Amtsantritt der neuen Kommission im Amt, könnte § 3 Abs. 4 Nr. 1 HSÜVG nicht mehr greifen und eine Sicherheitsüberprüfung erforderlich werden. Um die Handlungsfähigkeit der parlamentarischen Kontrollkommission zu gewährleisten, soll die Änderung des § 1 Abs. 5 VerfSchutzKG garantieren, dass § 3 Abs. 4 Nr. 1 HSÜVG so lange weiterhin für die Personen gilt, die nicht erneut in den Landtag gewählt wurden, bis sie aus der parlamentarischen Kontrollkommission ausscheiden.

III. Vergleich mit dem SÜG des Bundes

Die Gesetzesbegründung stellt den HSÜVG-E ausdrücklich in den Kontext der Änderung des Sicherheitsüberprüfungsgesetzes des Bundes, das im Januar 2026 geändert wurde. Das SÜG hat dabei in vielen Bereichen Verschärfungen vorgenommen, die aber nach dem gelten HSÜVG trotzdem noch einmal strenger sind. Der folgende Vergleich geht daher vor allem auf die Bereiche ein, in denen das SÜG inhaltlich andere Anforderungen stellt, also entweder strenger, weniger streng oder strukturell anders ausgestaltet ist als der HSÜVG-E bzw. das bestehende HSÜVG, um hier neue Aspekte in die Diskussion einzubringen, die nicht bereits über die Diskussion zum SÜG erfasst sind.

1. Strengere hessische Regelungen

a) Definition der Verschlussache

Ein erster Unterschied zwischen SÜG und HSÜVG betrifft die Definition der Verschlussache. Der HSÜVG-E übernimmt die Grunddefinition der Verschlussache aus dem SÜG, hält diese aber knapper. § 2 Abs. 1 HSÜVG-E definiert Verschlussachen als im öffentlichen Interesse, insbesondere zum Schutz des Wohles des Bundes oder eines Landes, geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse. Diese Formulierung entspricht wörtlich § 4 Abs. 1 S. 1 SÜG. Das SÜG enthält in § 4 Abs. 1 S. 2 und 3 darüber hinaus ausdrückliche Klarstellungen zu Kryptomitteln sowie zu Geschäfts-, Betriebs-, Erfindungs-, Steuer- und sonstigen privaten Geheimnissen oder Umständen des persönlichen Lebensbereichs. Die hessische Regelung ist hier weniger ausdifferenziert. Materiell dürfte dies allerdings nur begrenzte Auswirkungen haben, weil auch die hessische Definition weit genug ist, um geheimhaltungsbedürftige Gegenstände, Erkenntnisse und sonstige Informationen zu erfassen. Gleichwohl ist das SÜG an dieser Stelle klarstellend weiter.

b) Sicherheitsüberprüfung

Das SÜG sieht in § 2 Abs. 1a zwei Konstellationen vor, in denen auf eine Sicherheitsüberprüfung verzichtet werden kann: Zum einen ist ein Verzicht möglich, wenn bereits vor weniger als fünf Jahren eine gleich- oder höherwertige Überprüfung ohne Feststellung eines Sicherheitsrisikos abgeschlossen wurde. Zum anderen kann im Einzelfall zur Abwehr einer gegenwärtigen und erheblichen Gefahr auf eine Sicherheitsüberprüfung verzichtet

werden. § 3 Abs. 1 Satz 3 HSÜVG enthält nur die erste Fallgruppe. Eine dem § 2 Abs. 1a Satz 1 Nr. 2 SÜG entsprechende Regelung zur Gefahrenabwehr enthält der HSÜVG-E nicht.

Auch hinsichtlich der Form der Einwilligung (bzw. in der Terminologie des SÜG: der Zustimmung) in die Sicherheitsüberprüfung ist das HSÜVG auch vor seiner Änderung bereits strenger als das novellierte SÜG. Während § 2 Abs. 1 S. 3 SÜG auch die elektronische Form nach Maßgabe des § 3a VwVfG genügen lässt, findet nach § 4 Abs. 1 S. 5 HSÜVG § 3a Abs. 4 VwVfG ausdrücklich keine Anwendung.

Bei den Ausnahmen von der einfachen Sicherheitsüberprüfung geht der HSÜVG-E ebenfalls weiter als das SÜG. § 8 Abs. 2 SÜG enthält besondere Ausnahmetatbestände, in denen von der Durchführung einer Ü1 abgesehen werden kann, etwa bei bereits festgestellter Zuverlässigkeit nach dem Luftsicherheitsgesetz, wenn die Betrauung mit der sicherheitsempfindlichen Tätigkeit unaufschiebbar ist oder die Einstufung als Verschlussache voraussichtlich vor Abschluss der Sicherheitsüberprüfung wieder aufgehoben wird. Nach § 7 Abs. 2 HSÜVG-E kann von der Sicherheitsüberprüfung nur abgesehen werden in Bereichen, die i.S.v. § 1 Abs. 2 Nr. 3 HSÜVG-E zum Sicherheitsbereich erklärt wurden und wenn Art oder Dauer der Tätigkeit dies im Einzelfall zulassen. Auch hier übernimmt Hessen die bundesrechtlichen Ausnahmen nicht und bleibt daher restriktiver.

Besonders deutlich wird die strengere hessische Linie bei kurzfristigen Tätigkeiten im Bereich der erweiterten Sicherheitsüberprüfung. Das SÜG lässt in bestimmten Fällen eine nicht abgeschlossene Überprüfung für eine kurzzeitige Tätigkeit von höchstens acht Wochen zu, sofern die nicht überprüfte Person durch eine überprüfte Person ständig begleitet wird, § 9 Abs. 2 Nr. 1 lit. b SÜG. § 8 Abs. 3 HSÜVG-E begrenzt diesen Zeitraum demgegenüber „in der Regel“ auf höchstens vier Wochen. Hessen reduziert damit den Zeitraum, in dem eine nicht vollständig überprüfte Person ausnahmsweise eine sicherheitsempfindliche Tätigkeit wahrnehmen kann.

c) Ermittlungsmaßnahmen

Auch bei den Ermittlungsmaßnahmen enthält der HSÜVG-E punktuell strengere oder intensivere Regelungen. So sieht § 10 Abs. 1 HSÜVG-E bereits bei der einfachen Sicherheitsüberprüfung (Ü1) Anfragen an das Landeskriminalamt vor. Nach § 12 Abs. 2 Nr. 1 SÜG erfolgen Anfragen an die Polizeidienststellen erst zusätzlich bei der erweiterten Sicherheitsüberprüfung (Ü2). Hessen zieht polizeiliche Erkenntnisse damit früher in das Verfahren ein.

Hinzu kommt die Schufa-Datenübersicht. § 10 Abs. 1a HSÜVG-E erlaubt der mitwirkenden Behörde, bei Hinweisen auf eine mögliche finanzielle Angreifbarkeit eine Datenübersicht der Schufa Holding AG bei der betroffenen Person anzufordern; bei Personen aus dem Bereich des Landesamtes für Verfassungsschutz ist diese Datenübersicht sogar in jedem Fall anzufordern. Eine entsprechende ausdrückliche Schufa-Regelung enthält das SÜG

nicht. Das hessische Recht schafft damit ein zusätzliches Instrument zur Bewertung finanzieller Angreifbarkeit und möglicher Erpressbarkeit.

2. Weitreichendere Regelungen im SÜG

Umgekehrt enthält das SÜG auch Instrumente, die der HSÜVG-E nicht oder nur eingeschränkt übernimmt. Das betrifft zunächst die Einstufung von Sicherheitsbereichen. Entsprechend § 1 Abs. 2 Nr. 3 HSÜVG-E sieht auch § 1 Abs. 2 Nr. 3 SÜG vor, dass bestimmte Bereiche zum „VS-Sicherheitsbereich“ erklärt werden können. Nach dem HSÜVG-E ist für diese Bereiche nur eine einfache Sicherheitsüberprüfung (Ü1) durchzuführen, § 7 Abs. 1 Nr. 2 HSÜVG-E. Auf Bundesebene sind VS-Sicherheitsbereiche jedoch Gegenstand der erweiterten Sicherheitsüberprüfung (Ü2), § 9 Abs. 1 Nr. 4 SÜG.

Ein entscheidender Aspekt, in dem das SÜG strengere Regelungen vorsieht als der HSÜVG-E betrifft die Maßnahmen bei der Sicherheitsüberprüfung. Nach § 12 Abs. 1 Nr. 5 SÜG ist die Internetrecherche ab der Ü1 eine Standardmaßnahme, die bei jeder Sicherheitsüberprüfung durchzuführen ist. Die Möglichkeit der Internetrecherche ist zwar auch im HSÜVG-E vorgesehen, allerdings handelt es sich dabei um eine „kann“-Vorschrift, die nicht zwingend bei jeder Sicherheitsüberprüfung erfolgen muss, § 10 Abs. 1a S. 3 HSÜVG-E. Dieser Satz, der die Möglichkeit der Internet-Recherche und die Einsicht öffentlicher Teile sozialer Netzwerke ermöglicht, soll zudem mit dem HSÜVG-E neu eingeführt werden, es handelt sich daher also um eine Anpassung an das SÜG. Dementsprechend kann davon ausgegangen werden, dass sich die Landesregierung in ihrem Entwurf bewusst dagegen entschieden hat, die Internetrecherche als obligatorische Maßnahme aufzunehmen.

Wie auch im HSÜVG-E ist in § 13 Abs. 1 S. 2–4 SÜG im Rahmen der Sicherheitserklärung vorgesehen, dass dieser Lichtbilder der betroffenen sowie der mitbetroffenen Person(en) beizufügen sind und dass diese auch in elektronischer Form verlangt werden können. Bei der Einbeziehung der mitbetroffenen Personen und der elektronischen Form handelt es sich um eine neue Änderung, die erst mit dem HSÜVG-E geändert werden soll. Allerdings geht § 13 SÜG noch weiter, indem dort ausdrücklich auch die Möglichkeit vorgesehen ist, die Lichtbilder für einen automatisierten Abgleich mit Datenbanken zu nutzen. In den HSÜVG-E wurde das nicht ausdrücklich aufgenommen. Aus der Gesetzesbegründung ergibt sich dennoch, dass die Möglichkeit, elektronische Lichtbilder zu verlangen, den automatisierten Datenabgleich bezweckt.¹²

¹² LT-Drs. 21/4531 v. 28.05.2026, S. 31.

3. Eigenständige hessische Regelungen

Ein wesentlicher struktureller Unterschied zwischen dem SÜG und dem HSÜVG besteht in der Möglichkeit, Sicherheitshinweise zu erteilen. Diese können nach § 12 Abs. 1 HSÜVG erteilt werden, wenn kein Sicherheitsrisiko festgestellt wurde. Dabei handelt es sich gem. § 2 Abs. 9 HSÜVG um fallbezogene Empfehlungen, die zur weiteren Betreuung der betroffenen Person notwendig erscheinen. Die Sicherheitshinweise schaffen damit eine zusätzliche Handlungsmöglichkeit unterhalb der Schwelle eines Sicherheitsrisikos. Eine vergleichbare gesetzliche Definition enthält das SÜG nicht.

Eine weitere hessische Besonderheit besteht in der Definition lebenswichtiger Einrichtungen. Während das SÜG in § 5 Abs. 1 Nr. 2 darauf abstellt, dass die Beeinträchtigung einer für das Funktionieren des Gemeinwesens unverzichtbaren Einrichtung erhebliche Unruhe in großen Teilen der Bevölkerung und damit Gefahren für die öffentliche Sicherheit oder Ordnung auslösen würde, ergänzt § 2 Abs. 4 Nr. 2 HSÜVG ausdrücklich die Gefährdung der Versorgung der Bevölkerung mit wichtigen Dingen des Lebens. Diese Ergänzung erweitert den Anwendungsbereich des vorbeugenden personellen Sabotageschutzes und verdeutlicht, dass nicht erst erhebliche Unruhen in der Bevölkerung maßgeblich sein sollen, sondern bereits eine Gefährdung zentraler Versorgungsfunktionen.

IV. Kritische Würdigung

Die Zielsetzung der Novellierung des Hessischen Sicherheitsüberprüfungs- und Verschlusssachengesetzes, vertrauliche Informationen und sensible staatliche Sicherheitsbereiche von unzulässiger Einflussnahme, nicht zuletzt auch durch extremistische Akteure, zu schützen, ist grundsätzlich zu begrüßen.

Dennoch kann den Änderungen nicht uneingeschränkt zugestimmt werden; so kommt insbesondere ein berechtigter und für den Geheimnisschutz wichtiger Datenschutz an mancher Stelle zu kurz. Im Folgenden wird daher auf einige Kritikpunkte eingegangen. Dabei handelt es sich nicht ausschließlich um Änderungen, die im HSÜVG-E vorgesehen sind, sondern zum Teil auch um allgemeine Kritik am bereits geltenden HSÜVG sowie am SÜG des Bundes – sofern dessen Regelungen übernommen wurden –, die ihm Wege des Gesetzgebungsprozesses seiner Novellierung zu berücksichtigen ist. Diese Kritik wird aber weniger aufgegriffen, weil sie bereits bekannt ist.

1. Notwendige Berücksichtigung der Gesamtbelastung durch Informationseingriffe

Bevor die konkreten Kritikpunkte und Änderungsvorschläge vorgebracht werden, muss ein grundsätzliches Prinzip beachtet werden, das bei der Kritik stets im Hintergrund steht und dem der HSÜVG-E Rechnung zu tragen hat, nämlich die Gesamtbelastung durch Informationseingriffe, die sog. Gesamtüberwachungsrechnung.

Angesichts der multiplen Gefährdungen für die informationelle Selbstbestimmung in Zeiten von Big Data, Verbunddateien und KI ist dieser Ansatz auch auf Informationseingriffe

insgesamt übertragen.¹³ Bei Informationseingriffen – gerade im besonders sensiblen Sicherheitsbereich – ist aufgrund der Fülle staatlicher Informationseingriffe nicht nur jede einzelne Maßnahme isoliert, sondern in ihrer Gesamtwirkung auf die Freiheitsrechte der Bürger:innen zu betrachten. Während einzelne Eingriffe für sich genommen noch verhältnismäßig erscheinen können, können sie sich durch ihre Häufung, Kombination und technische Verknüpfbarkeit zu einer erheblichen Belastung verdichten. In der Rechtswissenschaft wurde dafür der Begriff der Überwachungsgesamtrechnung eingeführt. Sie verlangt, bei der Bewertung neuer Befugnisse auch bestehende Überwachungsinstrumente einzubeziehen und zu prüfen, ob das Gesamtniveau staatlicher Überwachung noch mit den grundrechtlichen Freiheitsgarantien vereinbar ist.¹⁴

Dass die Gesamtheitlichkeit in der Gesamtüberwachungsrechnung bereits fragwürdig ist,¹⁵ betrifft in der Regel das Bürger-Staat-Verhältnis, also Bürger:innen, die außerhalb des Staates stehen. Für das HSÜVG geht es dagegen üblicherweise um Personen, die ein besonderes Näheverhältnis zum Staat aufweisen. Die Maßstäbe davon sind also nicht ohne Weiteres übertragbar, auch wenn klar ist, dass die Grundrechte unverändert auch im Internum des Staats gelten. Vor diesem Hintergrund ist es daher besonders wichtig, dass die mit der Sicherheitsüberprüfung verbundenen Informationseingriffe verhältnismäßig sind, in einem nachvollziehbaren Verfahren erfolgen und datenschutzkonform sind. Hier wären explizite Löschungsverpflichtungen, eng(er) begrenzte Zugriffsschranken und klarere Zuweisungen der Zuständigkeit innerhalb der zuständigen Behörden weitere Möglichkeiten, die das HSÜVG nicht nutzt.

¹³ Gutjahr/Hornung/Schaller/Spiecker gen. Döhmman, Eingriffe in Informationsrechte: Staatliche Verantwortung bei Datenschutz und IT-Sicherheit, Studie des Nationalen Forschungszentrums für angewandte Cybersicherheit ATHENE, S. 31, abrufbar über: https://www.athene-center.de/fileadmin/content/PDF/2025-Systematic-Privacy.pdf?_=1761919641.

¹⁴ Dazu grundlegend BVerfGE 125, 260 (324); Roßnagel, NJW 2010, 1238 (1240); Zudem wird in aktuellen Forschungsansätzen wie dem periodischen Überwachungsbarometer des MPI zur Erforschung von Kriminalität, Sicherheit und Recht die praktische Umsetzbarkeit untersucht, s. <https://www.freiheit.org/de/ueberwachungsbarometer> sowie der in drei Bänden erschienene umfassende Forschungsbericht dies., Überwachungsgesamtrechnung für Deutschland; s. ferner insbesondere Löffelmann, Überwachungsgesamtrechnung und Verhältnismäßigkeitsgrundsatz, 2022 sowie die Beiträge in Zöller/Esser/Voigt/Gerson/Niedernhuber (Hrsg.), Sicherheitsgesetzgebung und Überwachungsgesamtrechnung, 2023.

¹⁵ Vgl. den Forschungsbericht des MPI zur Überwachungsgesamtrechnung, https://www.bmjv.de/Shared-Docs/Publicationen/DE/Fachpublikationen/2025_Forschungsbericht_Ueberwachungsgesamtrechnung.pdf?__blob=publicationFile&v=6.

2. Einwilligung und Freiwilligkeit bei Sicherheitsüberprüfungen

Auch wenn sowohl die betroffene als auch die einbezogene Person nach § 4 HSÜVG in die Sicherheitsüberprüfung einwilligen, werden gleichwohl in großem Umfang ihre personenbezogenen Daten verarbeitet. Vorliegend hängt für die betroffenen Personen von der Durchführung und dem Ausgang der Sicherheitsüberprüfung viel ab, da diese darüber entscheidet, ob sie ihrer sicherheitsempfindlichen Tätigkeit (weiterhin) nachgehen dürfen. Nicht nur die Feststellung eines Sicherheitsrisikos, sondern auch die Verweigerung der Einwilligung für eine Sicherheitsüberprüfung führen dazu, dass die betroffene Person nicht in sicherheitsempfindlichen Bereichen arbeiten kann. Daher wird sie – trotz möglicher Datenschutzbedenken – erwartbar in die Sicherheitsüberprüfung einwilligen und auch dem Eindruck unterliegen, faktisch „keine andere Wahl“ zu haben. Ob unter diesen Gesichtspunkten eine Einwilligung überhaupt den Anforderungen an Freiwilligkeit genügen kann, kann aber zumindest auch mit guten Gründen bezweifelt werden. Daher sollte eine Rechtsgrundlage geschaffen werden, die eine Einwilligung ersetzt, gleichzeitig aber sehr enge Grenzen für die weitere Verwendung dieser Daten, den Zugriff darauf und die Löschung vorsieht. Daran fehlt es.

3. Internetrecherche

Zunächst ist anzumerken, dass die Internetrecherche, die nach § 10 Abs. 1a S. 3 HSÜVG bereits jetzt möglich ist, intensive Eingriffe in die informationelle Selbstbestimmung verursachen kann und das nicht nur für die betroffene Person selbst und die einbezogene Person, sondern auch für Dritte, deren Daten möglicherweise ebenfalls gesichtet werden. Zwar ist zu begrüßen, dass der Entwurf der Landesregierung die Internetrecherche weiterhin als „Kann“-Maßnahme vorsieht und nicht, wie das SÜG, als stets im Rahmen einer Sicherheitsüberprüfung durchzuführende Maßnahme.

Deutlich zu widersprechen ist der Aussage in der Gesetzesbegründung, die Einsicht öffentlich zugänglicher Informationen im Internet stelle keinen Eingriff in die Rechte der betroffenen Person dar, da sie von ihnen freiwillig zur Verfügung gestellt werden.¹⁶ Auch öffentlich zugängliche Informationen sind grundsätzlich vom europa- und nationalrechtlichen Verfassungsrecht geschützt.¹⁷ Sie sind nicht etwa frei verfügbar und frei auslesbar und frei verwertbar.

¹⁶ So zur Rasterfahndung BVerfGE 120, 378 (399); *Barczak*, in: Brosius-Gersdorf (Hrsg.), Dreier GG, Art. 2 Abs. 1, Rn. 93; *Schantz*, in: Simitis/Hornung/Spiecker gen. Döhmman (Hrsg.), DatenschutzR, Art. 6 Abs. 1 DSGVO, Rn. 132 ff.

¹⁷ So zur Rasterfahndung BVerfGE 120, 378 (399); *Barczak*, in: Brosius-Gersdorf (Hrsg.), Dreier GG, Art. 2 Abs. 1, Rn. 93; *Schantz*, in: Simitis/Hornung/Spiecker gen. Döhmman (Hrsg.), DatenschutzR, Art. 6 Abs. 1 DSGVO, Rn. 132 ff.

Dennoch ist der HSÜVG-E im Hinblick auf die Internetrecherche sehr weitreichend und sollte deutlich präzisiert werden. Die Streichung des Wortes „eigene“ im HSÜVG-E ermöglicht nunmehr die Recherche auf sämtlichen öffentlich zugänglichen Internetseiten und nicht nur den eigenen, von der betroffenen Person selbst erstellten Seiten. Anders, als es die Gesetzesbegründung nahelegt, handelt es sich dabei um eine nicht unerhebliche Ausweitung des Anwendungsbereichs.¹⁸ Der Gegenstand der Internetrecherche ist mit der Einbeziehung sämtlicher allgemein zugänglicher Internetseiten und öffentlich sichtbarer Teile sozialer Netzwerke zudem unverhältnismäßig weit und unbestimmt. Es wird nicht deutlich, welche Teile/Seiten des Internets durchsucht werden und welche Mittel dabei eingesetzt werden dürfen. Unklar ist auch, ob die Behörden zur Recherche eigene Profile erstellen dürfen. Der BfDI merkt insofern in Bezug auf die Neuerung des SÜG zu Recht an, die Möglichkeit der Internetrecherche berge die Gefahr der Entstehung von „chilling effects“¹⁹, also von Verhaltensanpassungen Einzelner aus Sorge, ihr Verhalten könne „verdächtig“ erscheinen.²⁰ Daher könnte es dazu kommen, dass die Internetnutzung gezielt zurückgefahren wird, um solchen Profilbildungen durch die Öffentliche Hand zu entgehen – damit würde aber ein Bereich wichtiger Personen unterrepräsentiert sein in der öffentlichen Diskussion, etwa in Sozialen Medien.

Besonders problematisch ist, dass bei Internetrecherchen zwangsläufig auch personenbezogene Daten Dritter erfasst werden können, die keinen Bezug zur Sicherheitsüberprüfung haben. Werden für die Sicherheitsüberprüfung zum Beispiel Fotos der betroffenen oder einbezogenen Person im Internet gesichtet, auf denen auch unbeteiligte Dritte abgebildet sind, werden deren Daten automatisch ebenfalls von der mitwirkenden Behörde im Rahmen der Sicherheitsüberprüfung verarbeitet. Während die Einbeziehung von Ehe- und Lebenspartner:innen nach § 3 Abs. 3 S. 1 HSÜVG sich noch mit dem Näheverhältnis jedenfalls in Bezug auf Ermittlungen im Rahmen des Geheimnisschutz möglicherweise noch rechtfertigen lässt²¹, gilt dies etwa für Kinder wegen des erhöhten Schutzes Minderjähriger nicht. Zudem muss die Verarbeitung von Dritten, die mit der sicherheitsempfindlichen Tätigkeit nichts zu tun haben, unterbleiben; die Sicherheitsüberprüfung rechtfertigt die Eingriffe in ihre Rechte nicht und führt wiederum zu „chilling effects“, weil damit das soziale Umfeld von Staatsbeschäftigten den Kontakt zu diesen zu reduzieren angeregt werden könnte. Die Norm muss deshalb präziser gefasst werden. Dazu sollte

¹⁸ LT-Drs. 21/4531 v. 28.05.2026, S. 31.

¹⁹ Staben, Der Abschreckungseffekt auf die Grundrechtsausübung; Schwabenbauer, Heimliche Grundrechtseingriffe, S. 140 ff.; Assion, Überwachung und Chilling Effects, in: Telemedicus e.V. (Hrsg.), Überwachung und Recht, S. 31 ff.; Oermann/Staben, Der Staat 52 (2013), 630; S. auch Spiecker gen. Döhmman, in: Kischel/Kube (Hrsg.), HStR⁴ I, § 20, Rn. 32.

²⁰ BT-Drs. 21/120 v. 10.04.2025, S. 47 f.; zum Vorstehenden s. auch Eicholt, GSZ 2026, 75 (76 f.).

²¹ Dazu näher unten, im nächsten Punkt.

deutlich geregelt werden, was „allgemein zugänglich“ und „öffentlich sichtbarer Teil sozialer Netzwerke“ bedeutet, ob eine Registrierung (auch versteckt) von Mitarbeitenden der Behörden auf Plattformen zulässig ist, ob automatisierte Suchwerkzeuge eingesetzt werden dürfen und wie Treffer zu dokumentieren, zu verifizieren und gegebenenfalls wieder zu löschen sind.²² Ohne solche Konkretisierungen besteht die Gefahr einer uneinheitlichen Praxis und einer überschießenden Erhebung von Zufallsinformationen.²³

4. Betroffenenrechte

§ 32a HSÜVG verweist zwar auf die Anwendbarkeit des HDSIG. Die Vorschrift enthält in Abs. 2 ein eigenes Beschwerderecht, mit dem Betroffene sich an den Datenschutzbeauftragten wenden können. In Bezug auf Auskunfts- und Informationsrechte findet im Übrigen das HDSIG Anwendung. Um Betroffene über ihre Rechte gezielt zu informieren und möglichst niedrige Schwellen zu schaffen, sollte in das HSÜVG zur Vermeidung von Unsicherheiten vergleichbare Parallelnormen aufgenommen werden.

5. Weitestgehende Gleichstellung von betroffener und einbezogener Person

Die insgesamt im HSÜVG-E vorgenommene weitestgehende Gleichstellung der betroffenen Person und den einbezogenen Personen erscheint in der vorgesehenen Breite nicht verhältnismäßig. Zwar dürften Ehe- und Lebenspartner:innen der betroffenen Person in der Regel sehr nahestehen, allerdings werden sie nach § 3 Abs. 3 S. 1 HSÜVG in die Sicherheitsüberprüfungen Ü2 und Ü3 stets einbezogen, auch wenn sie – abgesehen von dem Näheverhältnis zur betroffenen Person – keinen unmittelbaren Bezug zu der sicherheitsempfindlichen Tätigkeit der betroffenen Person haben. Dass sie in gleichem Umfang Gegenstand der Maßnahmen nach § 10 HSÜVG sind, insbesondere der Internetrecherche, stellt einen tiefgreifenden Eingriff in ihre informationelle Selbstbestimmung dar.²⁴ Dies gilt erst recht für Kinder, insbesondere minderjährige, weil hier der Schutz von Ehe und Familie noch einmal besonderes Gewicht erfordert.

Bezüglich der einbezogenen Personen muss daher zwischen den Zielen unterschieden werden, nämlich zwischen Geheimschutz einerseits, also dem Schutz von geheimhaltungsbedürftigen Informationen, und dem vorbeugenden personellen Sabotageschutz für Lebens- und verteidigungswichtige Einrichtungen andererseits. Zwar können persönliche

²² Vgl. Eicholt, GSZ 2026, 75 (77).

²³ Vgl. BT-Drs. 21/120 v. 10.04.2025, S. 48; Eicholt, GSZ 2026, 75 (76 f.).

²⁴ Vgl. Gutjahr/Hornung/Schaller/Spiecker gen. Döhmman, Eingriffe in Informationsrechte: Staatliche Verantwortung bei Datenschutz und IT-Sicherheit, Studie des Nationalen Forschungszentrums für angewandte Cybersicherheit ATHENE, S. 31, abrufbar über: https://www.athene-center.de/fileadmin/content/PDF/2025-Systematic-Privacy.pdf?_=1761919641.

Näheverhältnisse im Geheimschutz regelmäßig für Anbahnungs-, Erpressungs- oder Loyalitätsrisiken relevant sein. Allerdings ist nicht ersichtlich, dass nicht vergleichbare Risiken in der Sphäre von Personen aus dem privaten Umfeld der betroffenen Person im Sabotageschutz ebenso relevant sind und sich ebenso auf die Zuverlässigkeit der betroffenen Person auswirken.²⁵

Hilfreich könnte hier ein gestuftes Vorgehen sein, bei dem die einbezogenen Personen einem generellen Screening unterzogen werden, das allerdings deutlich weniger intensiv ausgestaltet ist als bisher, und nur bei Anhaltspunkten verstärkte punktuelle Eingriffe möglich sind.

6. Fehlende Bestimmtheit bei Datenabgleich von Lichtbildern

Ein weiterer zentraler Kritikpunkt betrifft die Bestimmtheit von § 10 Abs. 1a HSÜVG-E. Die Möglichkeit, Lichtbilder in elektronischer Form zu verlangen, soll laut der Gesetzesbegründung dazu dienen, den automatischen Datenabgleich zu ermöglichen. Dass ein automatischer Abgleich mit Datenbanken vorgesehen ist, wurde aber nicht in den Gesetzestext aufgenommen werden. Der automatisierte Abgleich mit Datenbanken stellt für die betroffene und die einbezogene Person aber – auch unabhängig von deren Einwilligung – einen intensiven Informationseingriff dar²⁶ und die Rechtsgrundlage dafür sollte sich unmittelbar aus dem Gesetzestext ergeben – wie in § 19 Abs. 1 für die Daten aus § 11 Abs. 1 Nr. 1 bis 6 der Fall. Aktuell verstößt der Entwurf in dieser Hinsicht mindestens gegen das verfassungsrechtliche Bestimmtheitsgebot;²⁷ eine Rechtsgrundlage ist damit nicht geschaffen.

Unabhängig davon ist die automatisierte Verarbeitung von Lichtbildern verfassungsrechtlich bedenklich. Der Fotografie einer Person lassen sich unmittelbar eine Reihe von personenbezogenen Daten wie das Geschlecht, das ungefähre Alter, Anhaltspunkte über die ethnische Herkunft, wenn Symbole in Form von Schmuck getragen werden, möglicherweise auch Hinweise auf religiöse oder politische Überzeugungen. Wird dies mit anderen Faktoren gekoppelt, ist inzwischen unproblematisch z.B. auch die Ermittlung des Blutdrucks oder des Pulses bei der Aufnahme selbst möglich. Bei den Letzteren beiden Datenkategorien handelt es sich gem. Art. 9 Abs. 1 DSGVO sogar um sensible Daten. Darüber hinaus können digitale Lichtbilddateien auch Metadaten mit weiteren personenbezoge-

²⁵ So auch BT-Drs. 21/120 v. 10.04.2025, S. 47.

²⁶ S. nur zu Hessendata BVerfG NJW 2023, 1196 (1201).

²⁷ S. zum Bestimmtheitsgebot *Sommermann*, in: Huber/Voßkuhle (Hrsg.), GG, Art. 20, Rn. 289 ff.

nen Daten, zum Beispiel auch über die Person, die das Foto aufgenommen hat, enthalten.²⁸ Vom automatisierten Abgleich der Lichtbilder mit Datenbanken sollte der Gesetzgeber daher insgesamt absehen. Wird kein automatisierter Datenabgleich durchgeführt, ist wiederum die Erhebung von Lichtbildern in elektronischer Form nicht erforderlich.

Wird darauf nicht verzichtet, sollten die Datenbanken genau benannt werden; zudem sollte für jede einzelne Datenbank eine alle zwei Jahre stattfindende Überprüfung der Erforderlichkeit stattfinden; es sollte eine Gesamtbeschränkung der Datenbanken aufgenommen werden.

7. Angaben zu Beziehungen zu kriminellen oder terroristischen Vereinigungen und Personen, die verfassungsfeindliche Bestrebungen verfolgen und Kontakte zu ausländischen Nachrichtendiensten

Fraglich ist zudem die praktische Bedeutung der Angabe in der Sicherheitserklärung zu Beziehungen zu kriminellen und terroristischen Vereinigungen, zu Einzelpersonen oder Personengruppen, die verfassungsfeindliche Bestrebungen verfolgen sowie zu Kontakten zu ausländischen Nachrichtendiensten gem. § 11 Abs. 1 Nr. 12, 12a und 13 HSÜVG-E. Problematisch ist, dass die betroffenen Personen – insbesondere bei ausländischen Nachrichtendiensten, da diese in der Regel verdeckt auftreten – womöglich selbst gar nicht wissen, dass sie entsprechende Kontakte haben. Darüber hinaus ist nicht unwahrscheinlich, dass gerade Personen, die entsprechende Beziehungen pflegen, diese nicht offenlegen. Die praktische Bedeutung dieser Angaben dürfte daher gering sein.²⁹

Darüber hinaus bezieht sich § 11 Abs. 1 Nr. 12a HSÜVG-E wohl auf kriminelle und terroristische Vereinigungen im Sinne der §§ 129 ff. StGB. Diese Straftatbestände definieren zwar jeweils den Begriff der kriminellen terroristischen Vereinigung, enthalten jedoch keine Auflistung von Vereinigungen, die von diesen Begriffen erfasst sind. Die Behörden, die §§ 129 ff. StGB sowie § 11 Abs. 1 Nr. 12a HSÜVG-E anwenden, werden aber interne Listen der betroffenen Vereinigungen führen. Dabei wird nicht transparent, wer darüber entscheidet, welche Vereinigungen als terroristisch oder kriminell eingeordnet werden. § 11 Abs. 1 Nr. 12a HSÜVG-E ist daher recht weit und unbestimmt.³⁰

8. Angaben zu eigenen Internetseiten, Benutzernamen und Nutzer-IDs

Die erforderliche Angabe der Adressen eigener Internetseiten und Benutzernamen oder IDs bei sozialen Netzwerken im Rahmen der Sicherheitserklärung sollte auf einen Zeitraum von drei Jahren beschränkt werden, da die Regelung ansonsten sehr weitreichend ist. Da

²⁸ Seiler, in: Schwartmann/Benedikt/Reif (Hrsg.), Datenschutz im Internet, Kap. 12, A, Rn. 3 f.

²⁹ Eicholt, GSZ 2026, 75 (77).

³⁰ Eicholt, GSZ 2026, 75 (77).

viele Personen im Laufe ihres Lebens mehrere Internetseiten und mehrere Profile bei verschiedenen sozialen Netzwerken nutzen, kann diese Vorschrift zu sehr umfassenden Datenerhebungen und in der Folge zu Profilbildungen führen. Zwar handelt es sich beim Geheim- und personellen Sabotageschutz um hochrangige Schutzgüter, doch steht diesen auch ein „Recht auf Vergessen“ und Re-Sozialisierung der betroffenen Personen gegenüber.³¹ Nicht alle Aussagen, die eine Person öffentlich im Internet getätigt hat und die möglicherweise bereits Jahrzehnte zurückliegen, sind für eine Sicherheitsüberprüfung relevant. Zudem wird die umfassende Durchsicht sämtlicher Internetseiten und Social-Media-Profile ohne zeitliche Begrenzung dem Grundsatz der Datensparsamkeit nicht gerecht.³²

Dies gilt erst recht im Hinblick auf Kinder und Jugendliche: Werden Sicherheitsüberprüfungen bei Personen durchgeführt und dazu auch auf deren Daten aus dieser Lebensphase zurückgegriffen, ist die Selbstkontrolle der Betroffenen zu dieser Zeit nicht sicher gewährleistet. Entwicklungsoffenheit von Persönlichkeiten darf nicht dazu führen, dass im Staatsdienst eine Selektion von Personen allein darüber erfolgt, wer möglicherweise keine Persönlichkeitsentwicklung vollzogen hat.

V. Fazit

Der Gesetzentwurf ist in seiner Zielrichtung grundsätzlich zu begrüßen. Angesichts veränderter sicherheitspolitischer Rahmenbedingungen, insbesondere durch Spionage, Sabotage, Cyberangriffe und extremistische Einflussnahmen, besteht ein nachvollziehbares Bedürfnis, den Schutz von Verschlusssachen und sicherheitsempfindlichen Bereichen zu verschärfen.

Gleichwohl zeigt die Analyse, dass der Entwurf an mehreren Stellen zu weit reicht oder zu unbestimmt ist. Dies betrifft insbesondere die Internetrecherche/Recherche öffentlicher Informationen, die weitgehende Gleichstellung betroffener und einbezogener Personen, den möglichen automatisierten Abgleich elektronischer Lichtbilder sowie den Umfang der in der Sicherheitserklärung anzugebenden Informationen. Gerade weil Sicherheitsüberprüfungen tief in die informationelle Selbstbestimmung eingreifen und auch Personen erfassen können, die selbst keine sicherheitsempfindliche Tätigkeit ausüben, bedarf es klarer gesetzlicher Grenzen, nachvollziehbarer Verfahrensregelungen und effektiver datenschutzrechtlicher Kontrolle.

³¹ Vgl. Art. 17 DSGVO; *Barczak*, in: Brosius-Gersdorf (Hrsg.), Dreier GG, Art. 2 Abs. 1, Rn. 83 ff.

³² Dazu *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmman (Hrsg.), DatenschutzR, Art. 5 DSGVO, Rn. 116 ff.



Zwischen der Ausweitung der Sicherheitsüberprüfung im SÜG und im geplanten neuen HSÜVG einerseits sowie den aktuellen Plänen zur Reform des Informationsfreiheitsgesetzes andererseits lässt sich ein gemeinsamer rechtspolitischer Trend erkennen: Beide Vorhaben verschieben das Verhältnis zwischen staatlicher Sicherheitsvorsorge und staatlicher Transparenz zugunsten der Sicherheitsinteressen.

Diese Entwicklung ist nicht per se unzulässig, sollte aber kritisch und vor allem mit sehr genauen gesetzgeberischen Vorgaben begleitet werden. Ein moderner Geheim- und Sabotageschutz darf nicht allein auf möglichst umfassende Datenerhebung setzen, sondern muss den verfassungsrechtlichen Anforderungen an Verhältnismäßigkeit, Bestimmtheit und Transparenz staatlichen Handelns Rechnung tragen und klare Grenzen setzen. Diese sollten vor allem an einer zeitlichen Beschränkung, präziseren Benennungen der Zwecke und Eingriffsvoraussetzungen und der Zugriffsmöglichkeiten ansetzen. Der Rechtsstaat bewährt sich auch dann, wenn er herausgefordert ist, das ist sein Kern. Der Entwurf muss daher an den genannten Stellen nachgeschärft werden, um den berechtigten Sicherheitsinteressen des Staates Rechnung zu tragen, ohne die grundrechtlich geschützten Interessen der betroffenen und einbezogenen Personen unverhältnismäßig zu beeinträchtigen.

Für Rückfragen stehen wir selbstverständlich zur Verfügung.

Köln, den 29.07.2027

20. Juli 2026

STELLUNGNAHME

EINGEGANGEN

23. Juli 2026

HESSISCHER LANDTAG

Prof. Dr.iur. Hansjörg Huber M.A.

Hessischer Landtag

Gesetzentwurf

Gesetz zur Neufassung des Hessischen Sicherheitsüberprüfungs-
und Verschlusssachengesetzes und zur Änderung einer weiteren Vorschrift

Kurz: SÜG

Drucksache 21/4531

Die Stellungnahme will in zwei Teilen auf die Regelungen des Gesetzes
eingehen.

In Teil 1 soll zwischen den bevollmächtigten Sicherheitsbehörden
unterschieden werden.

In Teil 2 soll auf die möglicherweise kostenintensiven Auswirkungen für
die Privatwirtschaft eingegangen werden.

Zu Teil 1

Sicherheitsbehörden sind hier insbesondere der BND, das BAMAD und das LAVerf.Sch.

Es ist allgemein bekannt, dass die „Dienste“ trotz Überschneidungen unterschiedliche Zielstellungen verfolgen.

Ziel von BND und BAMAD unser Gemeinwesen, unseren Staat, unsere kritische Infrastruktur gegen im weitesten Sinne „Angriffe“ von außen abzuschildern.

Aufgabe des LAVerf.Sch die freiheitlich demokratische Grundordnung gegen gewaltsame, kämpferische Umstürze zu schützen.

Vereinfacht ausgedrückt wenden sich BND und BAMAD gegen Angriffe von außen.

Aufgabe der LAVerf.Sch ist es den demokratischen Staat gegen Angriffe von Innen zu schützen. Vereinfacht ausgedrückt.

Dabei hat die Existenz eines LAVerf.Sch im internationalen Rechtsvergleich westlicher Staaten mit echter Gewaltenteilung eine absolute Alleinstellung/rechtliche Ausnahme.

Die Digitalisierung des Staatsapparates bietet enorme Möglichkeiten den Standard der Sicherheitsüberprüfung im vorbeugenden personellen Sabotageschutz deutlich zu erhöhen.

Ein zentraler Punkt ist dabei die Modernisierung der Befugnisse zur Verarbeitung personenbezogener Daten im Dateiensystem.

Ein nicht unwesentlicher Teil besteht im Abbau bisheriger Ausnahmeregelungen, bei gleichzeitiger Ausweitung von Ermessensspielräumen.

Verbunden mit der Hoffnung der Beschleunigung von Findungsabläufen.

Vorstellbar ist eine Überprüfung aller zugänglicher Internetplattformen einschließlich sozialer Netzwerke im Wege einer einfacher Sicherheitsüberprüfungen bei Gefahren von außen.

Kurz bei Maßnahmen seitens BND und BAMAD, aufgrund der gestiegenen Gefährdungslage.

Nach Innen hingegen sind die Bürger mit einem hohen Grundrechtsschutz ausgestattet, nicht zuletzt durch Art. 5 GG Meinungsfreiheit.

Das BVerfG hat in dauernder Rechtsprechung die Meinungsfreiheit als grundlegendes Grundrecht gestärkt.

Die Grenzen verständlicherweise sehr weit gezogen.

So ist beispielsweise der in Wort und Schrift sowie digital geäußerte Wunsch eine parlamentarische Monarchie einzuführen natürlich von der Meinungsfreiheit gedeckt.

Gleichzeitig hat das BVerfSchutz aufgrund seines selbst eingeführten unbestimmten Rechtsbegriffs „Delegitimierung des Staates“ die Inhalte des Sagbaren unter Umständen verengt.

Die Urteile des BVerfG haben Gesetzeskraft, alle Behörden als vollziehende Gewalt sind aufgrund Art. 20 Abs. 3 GG an diese Urteile gebunden.

Es kann nicht sein, daß Behörden leichtfertig handeln, um sich dann von Gerichten in die Schranken weisen zu lassen.

Vor ihrem Tätigwerden sind Behörden gehalten eigenverantwortlich die Bindung an Recht und Gesetz einzuhalten.

Aufgrund der hohen Hürde der Grundrechte 1-19 GG unterliegt die Erweiterung des SÜG für Kontrollen nach Innen rechtlichen Vorbehalten. Der Gesetzgeber sollte dies ähnlich wie die Behörde bei der Anwendung im Vorfeld mitbedenken und nicht davon ausgehen: „Ist es falsch, dann werden es die Gerichte schon korrigieren“.

Teil 2

Kritische Infrastruktur und Betriebe der privaten Wirtschaft werden im Rahmen der Vertrauenswürdigkeitsprüfung in das System des Entwurfs zur Änderung des SÜG (Sicherheitsüberprüfungsgesetzes) miteinbezogen.

Das bedeutet, dass Internetrecherche einschließlich sozialer Netzwerke nun umfassender durchgeführt werden können.

Dies um Sicherheitsrisiken bei allen Überprüfungsarten zu ermitteln.

Diese Änderung zielt darauf ab die Zuverlässigkeit eines Mitarbeiters, einer Mitarbeiterin zu prüfen.

Gleichzeitig ist Gegenstand der Kontrolle eine denkbare Angreifbarkeit durch ausländische Nachrichtendienste festzustellen.

Die Prüfung erstreckt sich dann auch auf das Umfeld sowie Risiken durch Einzelpersonen.

Begründet wird dies durch den Gesetzgeber mit der zunehmenden Bedeutung von Internetsuchen für eine Aussage über die Zuverlässigkeit und mögliche Angreifbarkeit von Beschäftigten.

Als Ziel nennt es der Gesetzgeber eine Antwort auf die veränderte digitale Wirklichkeit zu geben.

Diese Antwort ist die umfassende Datenerhebung.

Natürlich gibt es von Seiten der sicherheitsrelevanten Privatwirtschaft verständliche Wünsche, welche im Gesetz wiederzufinden sein sollten.

Zuallererst stellt sich die Frage der Kostentragung. Wenn die Vertrauensschutzwürdigkeitsprüfung durch externe Dienste z.B. das LAVerfSchutz vorgenommen wird, dann fallen grundsätzlich Gebühren an.

Aus Sicht der Betriebe ist es daher wünschenswert Gebühren gar nicht erst tragen zu müssen oder zumindest erwarten zu können, daß diese, wenn sie denn anfallen, zielgerichtet wieder den Maßnahmen der beteiligten Behörde zugute kommen.

Des Weiteren sollten Wiederholungen der Prüfungen in regelmäßigen Abständen vorgenommen werden können.

Am Wichtigsten ist daher wohl die Frage nach der Rechtsfolge einer Prüfung mit negativem Ergebnis für den Geprüften.

Hat dieses Ergebnis arbeitsrechtliche Folgen dergestalt, dass eine Kündigung ausgesprochen werden kann?

Im Gegensatz zum Beamtenstatus, der die dauerhafte FDGO Treue als Voraussetzung für die Ernennung bzw. den Verbleib im Dienst festlegt. Und auch im Gegensatz zu den Angestellten im öffentlichen Dienst, bei denen die Hürden für eine Entlassung schon höher sind, da ihnen ein besonderes Näheverhältnis zum Staat fehlt,

ist bei privaten Arbeitnehmern von privaten Arbeitgebern die Rechtsfolge Kündigung noch offen.

Jeder private Angestellte besitzt ein Tätigkeitsprofil, welches vor Arbeitsgerichten eingeklagt werden kann.

Das heißt selbst eine Versetzung innerhalb der betroffenen Firma, in einen nicht sicherheitsrelevanten Bereich wird nur äußerst schwierig möglich sein.

Sollte wirklich eine Kündigung aus Sicherheitsgründen ausgesprochen werden, so ist mit Arbeitsschutzprozessen zu rechnen.

Auch hier läßt das angedachte SÜG Hessen die Arbeitgeber allein.



Prof. Dr.iur. Hansjörg Huber M.A.



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
Thomas Hering

Per E-Mail an:
H.Dransmann@ltg.hessen.de
C.Kehrein@ltg.hessen.de

Aktenzeichen 55.04:HSÜVG 2025-2026
*Bitte bei Antwort
angeben*

zuständig 14 08 - Frau Walburg
Durchwahl 157

Ihr Zeichen
Ihre Nachricht vom 30.06.2026

Datum 10.08.2026

Stellungnahme des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zum Entwurf eines Gesetzes zur Neufassung des Hessischen Sicherheitsüberprüfungs- und Verschlusssachengesetzes und zur Änderung einer weiteren Vorschrift, LT-Drs. 21/4531 vom 28.05.2026

Sehr geehrter Herr Vorsitzender,

für die Gelegenheit zur Stellungnahme zum Entwurf des Gesetzes zur Neufassung des Hessischen Sicherheitsüberprüfungs- und Verschlusssachengesetzes (HSÜVG) bedanke ich mich. Gerne nehme ich die Gelegenheit wahr, schriftlich zum o.g. Gesetzesentwurf Stellung zu nehmen. Ich hatte mich bereits im Rahmen der Evaluierung zum HSÜVG äußern können. Ich bedanke mich dafür, dass wesentliche Anmerkungen bereits umgesetzt wurden. Daher beschränkt sich diese Stellungnahme lediglich auf die im Rahmen der Evaluierung nicht aufgegriffenen datenschutzrechtlich relevanten Punkte.

Zu § 9 Abs. 1 Nr. 4 HSÜVG-E

Die Norm sieht vor, dass eine Sicherheitsprüfung für Personen durchzuführen ist, die eine Tätigkeit für das Landesamt für Verfassungsschutz Hessen wahrnehmen, die eine Überprüfung rechtfertigt. Im Gesetzestext wird diese Tätigkeit nicht näher konkretisiert.

Unsere derzeitige telefonische Erreichbarkeit: Mo. - Fr. von 09:00 - 12:00 Uhr sowie Mo. - Do. von 13:00 - 15:00 Uhr
Persönliche Termine bitte mit vorheriger Absprache

Laut der Gesetzesbegründung, sollen darunter Personen fallen, die zwar nicht selbst beim LfV tätig sind, aber Aufgaben wahrnehmen, die aufgrund ihrer Sensibilität dem Wissensstand entsprechen wie bei einer Tätigkeit im LfV Hessen selbst. Hierdurch sollten gleichwertige Verhältnisse geschaffen werden. Dies umfasse etwa Hilfspersonen aus anderen Behörden. Im Einzelfall sei dies aufgrund des konkreten Arbeitsgebietes, der dort erlangten Kenntnisse und der daraus resultierenden Folgen zu bewerten. Es seien stets das Sicherheitsbedürfnis des LfV Hessen mit den Persönlichkeitsrechten des Betroffenen gegeneinander abzuwägen.

Problematisch ist, dass der Gesetzeswortlaut den Kreis der betroffenen Personen nicht hinreichend bestimmt. Die maßgeblichen Voraussetzungen für die Sicherheitsüberprüfung ergeben sich im Wesentlichen erst aus der Gesetzesbegründung und einer einzelfallbezogenen Abwägung. Dadurch bleibt unklar, welche Tätigkeiten eine Überprüfung tatsächlich rechtfertigen. Dies eröffnet den Behörden einen erheblichen Beurteilungsspielraum und dürfte zulasten der Rechtssicherheit für die Betroffenen gehen.

Zu § 10 Abs. 1a S. 3 HSÜVG-E

Die ursprüngliche Fassung des § 10 Abs. 1a S. 3 HSÜVG-E sah vor, dass die mitwirkende Behörde zur betroffenen Person in erforderlichem Maße Einsicht in allgemein zugänglich eigene Internetseiten und den öffentlich sichtbaren Teil sozialer Netzwerke nehmen kann. In der Neufassung wird nun das Wort „eigene“ gestrichen. Als Begründung wird angeführt, dass durch die Streichung des Wortes kein Eingriff in die Rechte der betroffenen Personen oder Dritter herbeigeführt werde, da der Betreiber der Internetseiten oder die einstellende Person bereit durch die Möglichkeit der öffentlichen Einsicht sich einverstanden erklärt habe. Die erweiterte Einsicht sei für die Bewertung des Sicherheitsrisikos sinnvoll. Aufgrund der stetig wachsenden Digitalisierung würden stetig mehr Informationen im Internet geteilt, die genutzt werden müssten, um Lücken im Rahmen des Sicherheitsüberprüfungsrechts zu vermeiden. Daten, die aus einem Datenleck oder Angriff stammten, seien nicht als ordnungsgemäß öffentlich zugänglich zu bewerten und würden daher nicht unter die Sicherheitsüberprüfung fallen.

Diese Änderung ist aus datenschutzrechtlicher Sicht kritisch zu sehen, da die Ausweitung auf jegliche zugängliche Internetseiten dazu führen kann, dass eine klare

Abgrenzung zur Individualkommunikation künftig nur schwer möglich ist, insbesondere bei fehlenden und fehlerhaften Konfigurationen und Datenlecks. Die Bewertung dieser Daten als „nicht ordnungsgemäß öffentlich zugängliche Daten“, findet sich nicht im Gesetzeswortlaut, sondern lediglich in der Gesetzesbegründung. Eine klare Regelung, welche Daten als öffentlich zugänglich verwendet werden dürfen und welche nicht, fehlt mithin im Gesetz und dürfte rechtssicher auch mithilfe der Begründung nicht möglich sein.

Zu § 11 Abs. 1 S. 2 HSÜVG-E

Durch die Anpassung der Norm soll zur besseren Identifizierung bei den Sicherheitsüberprüfungen nach §§ 8 und 9 HSÜVG nicht nur ein Lichtbild von der betroffenen, sondern auch von einbezogenen Personen vorgelegt werden müssen.

Dadurch wird ein grundrechtsintensiver Eingriff allein aufgrund des Näheverhältnisses zur betroffenen Person normiert, ohne Betrachtung der Frage der Erforderlichkeit für eine eindeutige Identifizierung im konkreten Einzelfall. Dies mag hinsichtlich der betroffenen Person noch hinnehmbar sein, ist aber als zwingende Vorgabe für die nur aufgrund des Näheverhältnisses einbezogene Person mit Blick auf ihre Grundrechte und den Grundsatz der Verhältnismäßigkeit problematisch.

Zu § 13 Abs. 3 Nr. 2 HSÜVG-E

Durch die Anpassung der Norm werden die persönlichen Angaben, welche die personalverwaltende Stelle bei Änderungen der zuständigen Stelle für die Sicherheitsüberprüfung mitteilt, erweitert. Demnach sollen nun auch Änderungen des Vornamens sowie des Geschlechtseintrages mitgeteilt werden. Laut der Gesetzesbegründung sei dies zur eindeutigen Identifikation der Person notwendig.

Dies ist mit Blick auf die Änderungen des Gesetzes über die Selbstbestimmung in Bezug auf den Geschlechtseintrag (SGBB) zum 01.11.2024 zur Erleichterung von Änderungen des Geschlechtseintrages und des Vornamens auf Bundesebene zwar nachvollziehbar, aber aus datenschutzrechtlicher Sicht durchaus kritisch zu betrachten. Die Änderung des Geschlechtseintrags kann ggf. Rückschlüsse auf die sexuelle Orientierung ermöglichen und damit zu den besonderen Kategorien personenbezogener Daten gehören, die einem erhöhten Schutz unterliegen. Aus der Gesetzesbegründung

ergibt sich nicht hinreichend, warum die Änderung des Geschlechtseintrags ein wesentlicher Faktor bei der eindeutigen Identifizierung im Hinblick auf sicherheitsrelevante Erkenntnisse nach Abschluss der Sicherheitsüberprüfung sein soll, wenn doch bereits bei der Sicherheitserklärung nach § 11 HSÜVG umfassende, auch unveränderbare (wie Geburtsort und Geburtsdatum) personenbezogene Daten angegeben werden müssen, um eine eindeutige Identifizierung zu ermöglichen.

In der Gesetzesbegründung wird angeführt, dass ein Rückschluss auf die sexuelle Orientierung durch die Angabe eines geänderten Geschlechtseintrages nicht direkt möglich sei, da die Veränderung des Geschlechts nicht automatisch mit einer Veränderung oder Beibehaltung der sexuellen Orientierung verbunden sei. Es muss zwar kein zwingender Zusammenhang zwischen Geschlechtsidentität und sexueller Orientierung bestehen, aber ein geänderter Geschlechtseintrag im Zusammenspiel kann insbesondere im Zusammenhang mit weiteren bekannten Umständen, wie einer bestehenden Ehe oder Partnerschaft, Rückschlüsse auf die sexuelle Orientierung ermöglichen.

Zu § 28 Abs. 1 Nr. 2 HSÜVG-E

Die Norm regelt ebenfalls, dass eine Änderung des Geschlechtseintrages mitgeteilt werden muss. Es wird hierzu auf die Ausführungen zu § 13 Abs. 3 Nr. 2 HSÜVG-E verwiesen.

Zu § 29 Satz 3 HSÜVG-E

Der neu eingefügte Satz 3 sieht vor, dass die Sicherheitsakte dem oder der internen Datenschutzbeauftragten einer nicht öffentlichen Stelle nicht zugänglich zu machen ist. Aus der Gesetzesbegründung geht jedoch nicht hervor, warum der Ausschluss des oder der internen Datenschutzbeauftragten erforderlich ist.

Die Regelung ist vergleichbar mit § 30 Sicherheitsüberprüfungsgesetz des Bundes (SÜG). Diese sieht vor, dass die Sicherheitsakte der nichtöffentlichen Stelle dem oder der Datenschutzbeauftragten nicht zugänglich gemacht werden darf. Aus der Gesetzesbegründung zu § 30 SÜG (BT-Drs. 21/1926 Gesetzentwurf der Bundesregierung zur Modernisierung des Sicherheitsüberprüfungsgesetzes und zur Änderung beamtenrechtlicher Vorschriften vom 01.10.2025, Seite 4) ergibt sich, dass die Aufnahme

des Ausschlusses des Datenschutzbeauftragten der Rechtsklarheit dienen sollte. Zur Begründung wird auf Ziffer 6.4 der Vorbemerkungen der Allgemeinen Verwaltungsvorschrift des BMI zur Ausführung des Sicherheitsüberprüfungsgesetzes (Allgemeine Verwaltungsvorschrift zum personellen Geheimschutz und zum vorbeugenden personellen Sabotageschutz SÜG-Ausführungsvorschrift (SÜG-AVV) vom 15. Februar 2018 (GMBI. S. 270) i. d. F. der mit Rundschreiben des Bundesministeriums des Innern und für Heimat vom 8. Juni 2022, Seite 8) verwiesen. Dort wird ausgeführt, dass die Erhebung, Verarbeitung und Nutzung personenbezogener Daten im Rahmen der Sicherheitsüberprüfung bei nichtöffentlichen Stellen abweichend von den Vorschriften im Bundesdatenschutzgesetz (BDSG) durch die oder den Bundesbeauftragte(n) für den Datenschutz und die Informationsfreiheit geprüft wird, da die Sicherheitsüberprüfung im staatlichen Interesse erfolgt und insoweit die für den öffentlichen Bereich geltenden Vorschriften nach dem BDSG gelten sollen. Damit wird von der allgemeinen Zuständigkeitsregelung des § 40 BDSG abgewichen, wonach für die Datenschutzaufsicht über nichtöffentliche Stellen grundsätzlich die Landesdatenschutzaufsichtsbehörden zuständig sind.

Diese Erwägungen lassen sich auf das Hessische Sicherheitsüberprüfungsgesetz nicht ohne Weiteres übertragen. Anders als auf Bundesebene bedarf es im hessischen Landesrecht keiner entsprechenden Regelung im Hinblick auf die Aufsichtszuständigkeit. Der Ausschluss des oder der internen Datenschutzbeauftragten vom Zugang zur Sicherheitsakte ist in diesem Zusammenhang ebenfalls nicht nachvollziehbar.

Mit freundlichen Grüßen



Prof. Dr. Alexander Roßnagel



HESSEN

Landesamt für Verfassungsschutz Hessen
Postfach 39 05 • 65029 Wiesbaden

E-Mail

Hessischer Landtag
Schlossplatz 1-3
65183 Wiesbaden

nachrichtlich:
HMdI/Abt. II

c.kehrein@ltg.hessen.de
h.dransmann@ltg.hessen.de

Aktenzeichen: 037-S-470000-0002/2026
Tel.: (0611) 720 - 08235
E-Mail: poststelle@lfv.hessen.de
Ihr Zeichen: Ihre Nachricht: 30.06.2026
Datum: 7. August 2026

Schriftliche Anhörung des Innenausschusses des Hessischen Landtags
Gesetz zur Neufassung des Hessischen Sicherheitsüberprüfungs- und
Verschlusssachengesetzes und zur Änderung einer weiteren Vorschrift
– Drucks. 21/4531 –
Stellungnahme des Landesamtes für Verfassungsschutz Hessen

Sehr geehrte Frau Kehrein,
sehr geehrter Herr Dransmann,

für die Benachrichtigung von der schriftlichen Anhörung des Innenausschusses des Hessischen Landtags (HLT) sowie für die Aufnahme in den Kreis der Anzuhörenden bedanke ich mich. Namens des LfV Hessen darf ich zu dem Gesetz zur Neufassung des Hessischen

65187 Wiesbaden, Konrad-Adenauer-Ring 49
Telefon: (0611) 720-0
E-Mail: poststelle@lfv.hessen.de
Internet: www.verfassungsschutz.hessen.de



Sicherheitsüberprüfungs- und Verschlusssachengesetzes und zur Änderung einer weiteren Vorschrift wie folgt Stellung nehmen.

Die Zeitenwende hat längst auch in Hessen ihren Einzug erhalten. Damit einher geht ein erhöhtes Sicherheitsinteresse des Landes, dem mit verschiedenen Maßnahmen Rechnung getragen werden muss. Die Neufassung bzw. Überarbeitung der bestehenden Gesetze in Hessen ist dabei ein Baustein. Insofern wird die Neufassung des Hessischen Sicherheitsüberprüfungs- und Verschlusssachengesetzes (HSÜVG) sowie die Änderung weiterer Vorschriften vollumfänglich begrüßt.

Soweit in dem Gesetzesentwurf der Landesregierung zu dem HSÜVG Konkretisierungen und Klarstellungen des aktuellen Gesetzestextes vorgeschlagen werden, um damit die Anwendbarkeit der Normen auf konkrete Sachverhalte zu vereinfachen bzw. zu erleichtern, werden diese Änderungsvorschläge vollumfänglich begrüßt und in einem zweiten Schritt auch befürwortet. Insofern wird im weiteren Verlauf der Stellungnahme zu diesen Änderungen nur im Einzelfall gesondert Stellung genommen.

Ebenso begrüßt und befürwortet werden alle Änderungen in dem Gesetzesvorschlag, die zum Schutz der Mitarbeitenden des Landesamtes für Verfassungsschutz (LfV) aufgenommen bzw. angepasst wurden. Die Mitarbeitenden stehen im Zusammenhang mit ihrer Tätigkeit für den Verfassungsschutz seit jeher in einem besonderen Fokus von ausländischen Nachrichtendiensten. Dies hat sich mit dem Beginn der Zeitenwende noch einmal zum Nachteil der Mitarbeitenden verstärkt. Insofern gilt es, die Mitarbeitenden unter einen besonderen Schutz zu stellen. Die entsprechenden Änderungen sind ein Schritt in die richtige Richtung.

Unter Berücksichtigung der einleitenden Worte nehme ich zu folgenden Änderungsvorschlägen wie folgt Stellung:

1. Artikel 1: Hessisches Sicherheitsüberprüfungs- und Verschlusssachengesetz (HSÜVG)

Änderung in § 1

Die Einfügung des § 1 Abs. 1 S. 5 (im Entwurf der Gesetzesbegründung nach hiesiger Auffassung irrtümlich als S. 4 zitiert) erfüllt den Zweck der Klarstellung des Ziels des vorbeugenden personellen Sabotageschutzes und konkretisiert damit den Zweck und das Ziel des Gesetzes und wird insofern ausdrücklich befürwortet.

Besonders begrüßt wird -wie bereits in der Einleitung dieser Stellungnahme erwähnt- die Ergänzung in Abs. 2 Nr. 6, die zum Schutz der Mitarbeiterinnen und Mitarbeiter LfV eingefügt

wurde. Im Zuge der Zeitenwende stehen diese Personen in einem besonderen Fokus von ausländischen Nachrichtendiensten. Es gilt, diesen Personenkreis besonders zu schützen. Die Überprüfung der Personen, die aufgrund des Zugangs zu Personalinformationen Kenntnis der Mitarbeitenden des LfV oder deren Tätigkeit erlangen können, ist eine erste Maßnahme, um die Sicherheit der Mitarbeitenden des LfV zu erhöhen.

Änderung in § 2

Neben den Neufassungen des Abs. 7, Satz 1 Nr. 2 Buchstabe c sowie der Einfügung des neuen Satz 3 wird insbesondere die Ergänzung in § 2 Abs. 7 S. 3 ausdrücklich begrüßt. In der Praxis zeigt es sich immer wieder, dass im Rahmen einer Ü 1 Erkenntnisse zu Personen nach § 3 Abs. 3 Satz 1 (einzubeziehende Personen) auftreten können, die bei einer sicherheitsmäßigen Bewertung zu sicherheitserheblichen Erkenntnissen führen kann und im Fall einer Ü 2 oder Ü 3 zur Feststellung eines Sicherheitsrisikos führen würde. Hierunter können beispielsweise (kompromittierende) veröffentlichte Fotos des Ehepartners in den Sozialen Medien der zu überprüfenden Person fallen. Hier ist dem Gesetzgeber zuzustimmen, dass die größtmögliche Wirksamkeit und Sicherheit der Sicherheitsüberprüfung nur zu gewährleisten ist, wenn jede zulässigerweise erlangte Kenntnis eines Sicherheitsrisikos einzubeziehen ist. Anderenfalls bestünde eine Wertungswiderspruch. Insofern ist auch die daraus resultierende Änderung in § 6 konsequent und folgerichtig.

Änderung in § 3

Die Klarstellung der in Absatz 3 benannten Personen ist nachvollziehbar und dient der Klarheit.

Änderung in § 4

Sofern in Absatz 1 nach Satz 3 die Anwendbarkeit des § 3a Abs. 4 des hessischen Verwaltungsverfahrensgesetzes ausgeschlossen wird und damit die Einwilligung in die Sicherheitsüberprüfung auch weiterhin in Schriftform erteilt werden muss, ist der Gesetzesbegründung zuzustimmen. Der Eingriff in die Persönlichkeitsrechte des Betroffenen durch eine Sicherheitsüberprüfung ist so erheblich, dass die notwendige Sensibilität für dieses Verfahren unter anderem durch die Fortführung des Erfordernisses in Schriftform erreicht werden kann.

Änderung in § 5

Auch die Regelung zur unverzüglichen Unterrichtung der für die Sicherheitsüberprüfung zuständigen Stelle durch die personalverwaltende Stelle über die beabsichtigte Verwendung ist insbesondere deshalb zu befürworten, weil so eine zeitliche Verzögerung im Sicherheitsüberprüfungsverfahren vermieden kann.

Änderung in §§ 6 und 7

Die Änderungen in 6 und 7 sind unter Berücksichtigung der Begründung in den §§ 1 und 2 konsequent. Hier wird ausdrücklich Bezug auf die Ausführungen zu den Änderungen in § 1 und 2 genommen.

Änderung in § 9

Bislang war es für das LfV als zuständige Stelle nur möglich, Sicherheitsüberprüfungen nach Ü 3 für Personen durchzuführen, die auch bei dem LfV tätig sind. Durch die Neuregelung wird der Personenkreis nun auf gleichgestellte Personen erweitert. Die Regelung wird unter Berücksichtigung des erhöhten Sicherheitsinteresses -auch gegenüber den Mitarbeitenden- aus Sicht des LfV ausdrücklich begrüßt. Es ist unerheblich, ob Wissen und Kenntnisse über den Aufbau, die Prozesse oder Vorgänge innerhalb des LfVs von Personen erlangt werden, die bei dem LfV tätig sind oder aber in einer anderen Behörde. Es geht ausschließlich um den Schutz dieses Wissens bzw. der Kenntnisse.

Auch die Einfügung des Satz 2 wird besonders mit Blick auf die derzeit schwierige Situation im Bereich der Personalgewinnung ausdrücklich begrüßt. Alle Mitarbeitenden des LfV müssen sich einer Sicherheitsüberprüfung nach Ü 3 unterziehen. Die Neuerungen ermöglicht es dem LfV nunmehr in ausgewählten Einzelfällen -beispielsweise bei besonders qualifizierten Bewerbern- unter Berücksichtigung der Voraussetzung in Satz 2 flexibel reagieren zu können, um so für einen Bewerber attraktiv zu bleiben.

Änderung in § 10

Den Ausführungen in der Gesetzesbegründung zu der neu eingefügten Nr. 5 wird ausdrücklich befürwortet. Die Verifizierung von Daten, die im Sicherheitsüberprüfungsbogen angegeben werden, sind die Basis für eine belastbare Bewertung innerhalb der Sicherheitsüberprüfung. Darüber hinaus wird die Streichung des Wortes „eigene“ in Abs. 1a Satz 3 sehr begrüßt. Die Internetrecherche stellt im Rahmen des Sicherheitsüberprüfungsverfahrens einen wesentlichen Baustein für die Gewinnung von Informationen dar. Die Streichung des Wortes „eigene“ stellt unmissverständlich klar, dass jegliche allgemein zugängliche und öffentlich sichtbare Internetseiten eingesehen werden dürfen.

Auch die Änderungen in Absatz 3 werden ausdrücklich begrüßt. Die Befragungen von Referenzpersonen sind zeitaufwändig. In Einzelfällen hat sich gezeigt, dass schon nach der Befragung der ersten Referenzperson abgesehen werden kann, dass kein

Sicherheitsrisiko vorliegt und deshalb die Befragung der weiteren Referenzpersonen das Verfahren insgesamt nur in die Länge zieht. In solchen Fällen muss die Möglichkeit bestehen, bereits nach der

Befragung der ersten Referenzpersonen einen Abschluss ohne Sicherheitsrisiko zu ermöglichen. Die Dokumentation dieser Entscheidung stellt sicher, dass aus dieser Möglichkeit kein Regelverfahren abgeleitet werden kann.

Änderung in § 11

Soweit in Satz 2 für die Überprüfung der einbezogenen Person nunmehr auch die Vorlage eines Lichtbildes gefordert wird, ist diese Regelung mehr als nachvollziehbar. Die Vorlage eines Lichtbildes dient der Identifikation einer Person, unabhängig davon, ob es die betroffene oder die einzubeziehende Person ist.

Änderung in § 12

Soweit in Absatz 3 klargestellt wird, dass die zuständige Stelle zur Vermeidung der Feststellung von Sicherheitsrisiken Auflagen erlassen kann, wird dies sehr begrüßt. Diese Möglichkeit besteht zwar seit jeher, nunmehr ist sie aber auch ausdrücklich normiert und kann von den zuständigen Stellen zur Entscheidungsbegründungen herangezogen werden.

Die Erweiterung des Absatz 4 um die Regelung aus Satz 6 kann nachvollzogen werden und ist insofern sinnvoll, als dass damit nicht nur den Interessen des Betroffenen Rechnung getragen wird, sondern auch der Frage, ab wann ein erheblicher Nachteil für die Interessen des Bundes oder des Landes vorliegen, die eine Anhörung bisher gänzlich ausgeschlossen haben.

Änderung in § 13

Die Regelung im neuen Absatz 4 entspricht der Regelung des Bundes. Sie überzeugt insofern, als das bei sicherheitserheblichen Erkenntnissen von besonderer Bedeutung die (vorläufige) Untersagung zu Gunsten der Sicherheit grundsätzlich keinen Aufschub dulden darf.

Änderungen in §§ 17, 18 sowie §§ 26-29 und §§ 32 a und 32 b

Gegen die Änderungen bzw. Einfügungen in den §§ 17, 18 sowie 26-29 und 32a, 32 b bestehen keine Einwände.

Diese erfolgen zur Klarstellung bzw. Schließung von Gesetzeslücken und sind nachvollziehbar.

2. Artikel 2: Änderung des Verfassungsschutzkontrollgesetzes

Artikel 2 des genannten Änderungsgesetzes befasst sich mit einer Änderung des Verfassungsschutzkontrollgesetzes vom 25. Juni 2018 (GVBl. 302, 317), zuletzt geändert durch Gesetz vom 10. Dezember 2025 (GVBl. 2025 Nr. 97). § 1 Abs. 5 des Verfassungsschutzkontrollgesetzes (VerfSchKontG) soll demnach um die folgenden Sätze ergänzt werden:

„Für den Fall des Satz 3 gilt für die Mitglieder der Parlamentarischen Kontrollkommission, die nicht dem neu gewählten Landtag angehören, § 3 Abs. 4 Nr. 1 des Hessischen Sicherheitsüberprüfungs-

und Verschlussachengesetzes vom [Datum und Fundstelle des Gesetzes zur Neufassung des Hessischen Sicherheitsüberprüfungs- und Verschlussachengesetzes und zur Änderung weiterer Vorschriften], bis zum Ausscheiden aus der Parlamentarischen Kontrollkommission für die Ausübung dieser Tätigkeit weiter. Sofern nicht innerhalb eines Jahres nach Durchführung der Neuwahlen des Landtags die neuen Mitglieder der Parlamentarischen Kontrollkommission gewählt wurden, gilt Satz 5 nicht mehr."

§ 1 Abs. 5 VerfSchKontG n.F. hieße dann:

„Scheidet ein Mitglied aus dem Landtag oder seiner Fraktion aus oder wird es Mitglied der Landesregierung, so verliert es seine Mitgliedschaft in der Parlamentarischen Kontrollkommission. Für dieses Mitglied ist unverzüglich ein neues Mitglied zu wählen; das Gleiche gilt, wenn ein Mitglied aus der Parlamentarischen Kontrollkommission ausscheidet. Die Mitglieder der Parlamentarischen Kontrollkommission bleiben nach Ablauf der Wahlperiode oder der Auflösung des Landtags bis zur Wahl einer neuen Parlamentarischen Kontrollkommission im Amt. Für den Fall des Satz 3 gilt für die Mitglieder der Parlamentarischen Kontrollkommission, die nicht dem neu gewählten Landtag angehören, § 3 Abs. 4 Nr. 1 des Hessischen Sicherheitsüberprüfungs- und Verschlussachengesetzes vom [Datum und Fundstelle des Gesetzes zur Neufassung des Hessischen Sicherheitsüberprüfungs- und Verschlussachengesetzes und zur Änderung weiterer Vorschriften], bis zum Ausscheiden aus der Parlamentarischen Kontrollkommission für die Ausübung dieser Tätigkeit weiter. Sofern nicht innerhalb eines Jahres nach Durchführung der Neuwahlen des Landtags die neuen Mitglieder der Parlamentarischen Kontrollkommission gewählt wurden, gilt Satz 5 nicht mehr."

Aus obiger Darstellung ist ersichtlich, dass § 1 Abs. 5 S. 3 VerfSchKontG in der aktuellen Fassung lediglich den Umstand regelt, dass Mitglieder der Parlamentarischen Kontrollkommission (PKV) nach Ablauf der Wahlperiode oder der Auflösung des Landtags bis hin zur Wahl einer neuen PKV im Amt bleiben. Dass PKV-Mitglieder in genannter Konstellation jedoch trotz Umgang mit sicherheitssensiblen Sachverhalten grundsätzlich nicht mehr unter die Ausnahme des § 3 Abs. 4 Nr. 1 HSÜVG fallen, wonach eine Sicherheitsüberprüfung für die Mitglieder des Hessischen Landtages nicht durchzuführen ist, berücksichtigt die bisherige Fassung nicht. Vor diesem Hintergrund wird es von hieraus begrüßt, dass mit der Ergänzung des § 1 Abs. 5 VerfSchKontG durch eine zeitlich auf ein Jahr beschränkte Ausdehnung der Ausnahme nach § 3 Abs. 4 Nr. 1 HSÜVG nunmehr Rechtssicherheit für PKV-Mitglieder geschaffen wird, die nicht mehr dem Hessischen Landtag angehören. Für eine solche Ausdehnung sprechen nicht nur Praktikabilitätsgesichtspunkte, sondern insbesondere auch das Bedürfnis nach Sicherstellung der Arbeitsfähigkeit der PKV nach Ablauf der Wahlperiode oder der Auflösung des Landtags.

Bei Rückfragen stehe ich gerne zur Verfügung.

gez. Neumann



Hessischer Landkreistag

Hessischer Landkreistag · Frankfurter Str. 2 · 65189 Wiesbaden

Hessischer Landtag
Herrn Thomas Hering
Vorsitzender des Innenausschusses
Schlossplatz 1-3
65183 Wiesbaden

Frankfurter Str. 2
65189 Wiesbaden
Telefon (0611) 17 06 - 0
Durchwahl (0611) 17 06- 12
Telefax-Zentrale (0611) 17 06- 27

e-mail-Zentrale: info@hlt.de
e-mail-direkt: bebensee-biederer@hlt.de
www.HLT.de

Datum: 10.08.2026
Az. : Be/We/052.13

Ausschließlich per Mail an: h.dransmann@ltg.hessen.de
c.kehrein@ltg.hessen.de
ausschussdienst@ltg.hessen.de

Gesetzentwurf Landesregierung Gesetz zur Neufassung des Hessischen Sicherheitsüberprüfungs- und Verschlusssachengesetzes und zur Änderung einer weiteren Vorschrift – Drucks. 21/4531 –

Ihr Schreiben vom 30. Juni 2026

Sehr geehrter Herr Vorsitzender,

eingangs bedanken wir uns für die Möglichkeit, zum Gesetzentwurf der Landesregierung zur Neufassung des Hessischen Sicherheitsüberprüfungs- und Verschlusssachengesetzes Stellung nehmen zu können. Gern möchten wir die Gelegenheit nutzen und auf einige Probleme hinweisen, die uns aus den hessischen Landkreisen mitgeteilt wurden.

Die vorliegende Modifikation des HSÜVG ist ein wichtiger Schritt, um gegen bestehende Gefahren weiterhin Schutz bieten zu können. Um eine zukünftige Sicherheitsarchitektur langfristig resilient gegen moderne hybride und gesellschaftliche Dynamiken aufzustellen, bedarf es allerdings weiterer Erfordernisse:

1. Digitale Lebensrealität und Cyber-Radikalisierung:
Die Beschränkung auf „öffentlich zugängliche“ Internetpräsenzen in der Sicherheitserklärung verkennt die aktuelle digitale Radikalisierungsdynamik. Relevante Prozesse finden heute in geschlossenen Ökosystemen (Telegram, Discord, Darknet) statt. Nötig erscheinen rechtssichere Kriterien für den Umgang mit verschlüsselter Kommunikation und KI-gestützten Bedrohungen (z.B. Deepfakes als Erpressungsgrundlage). Es bedarf weiterer Regelungen zur digitalen Resilienz der überprüften Personen.
2. Transformation der Bedrohungsakteure:

Der Fokus auf klassische ausländische Nachrichtendienste oder die Stasi-Vergangenheit ist für die kommenden Generationen (Gen Z/Alpha) kaum noch biographisch relevant. Ein blinder Fleck dürften die nicht-staatlichen, aber staatlich geduldeten Akteure (z.B. staatliche Hacker-Kollektive, Desinformations-Netzwerke) sein. Es fehlen dynamische Mechanismen und Prüfkriterien für moderne hybride Bedrohungen und systemische Rivalen jenseits formaler Strukturen.

3. Dynamischer Extremismus:

Das Feststellen von persönlichen Sicherheitsrisiken erfolgt u.a. bei Zweifeln am Bekenntnis zur "freiheitlichen demokratischen Grundordnung" oder bei Kontakten zu "verfassungsfeindlichen Organisationen" (Statistischer Organisationsbegriff).

Moderne Staatsfeindlichkeit agiert jedoch oft „führerlos“, dezentral und unterhalb der Schwelle zur offenen Gewalt (z. B. subtile Delegitimierung, Reichsbürger-Ideologien). Das Gesetz sollte Instrumente zur Bewertung informeller Netzwerkstrukturen, um „weiche“, aber systemgefährdende Verfassungsfeindlichkeit rechtssicher greifbar zu machen, beinhalten.

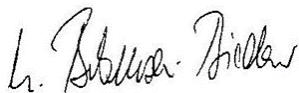
4. Gesellschaftlicher Wandel und Diversität:

In die erweiterte Überprüfung sollen volljährige Ehegatten, Lebenspartner oder Personen in einer "eheähnlichen oder gleichgeschlechtlichen Gemeinschaft (Lebensgemeinschaft)" einbezogen werden. Die Beschränkung auf klassische Partnerschaftsmodelle spiegelt nicht die Realität wider. Mitarbeitende in modernen Lebensformen (Polyamorie, nicht-binäre Identitäten) könnten sich zur Geheimhaltung gezwungen sehen, was ein Sicherheitsrisiko durch Erpressbarkeit darstellt. Eine lebensnahe Formulierung schützt vor Diskriminierung und eliminiert Angriffsflächen.

5. Erweiterung des Begriffs der Kritischen Infrastruktur (KRITIS):

Das Gesetz definiert "lebenswichtige" und "verteidigungswichtige" Einrichtungen stark über die gesundheitliche Gefährdung der Bevölkerung und die Unterstützung der Bundeswehr. Hier wäre zu überlegen, den Begriff des vorbeugenden personellen Sabotageschutzes auf digitale Infrastrukturen (Rechenzentren, Cloud-Anbieter für Behörden) und ökologische kritische Infrastrukturen auszuweiten. Zukünftige Konflikte dürften sich auch um Ressourcen und Daten drehen.

Mit freundlichen Grüßen



Ute Bebensee-Biederer
Referatsleiterin