

**Anlage 4: Kernbereichsschutz**

- Bei **Wohnraumüberwachungen** hat der Gesetzgeber zwecks Kernbereichsschutz auf Erhebungsebene eine widerlegliche Vermutung vorzusehen.
- Auf Auswertungs-/Verwertungsebene ist die Vorlage sämtlicher aus der Maßnahme erlangter Kenntnisse an eine unabhängige Stelle vorzusehen. Sie hat zum einen zu prüfen, ob sich die Maßnahme in den Grenzen der richterlichen Anordnung gehalten hat. Zum anderen hat sie etwa erfasste Kernbereichsdaten unverzüglich zu löschen.
- Beim **Verdeckten Zugriff auf informationstechnische Systeme** ist eine gesetzliche Verpflichtung vorzusehen, wonach auf Erhebungsebene technisch sicherzustellen ist, dass die Erhebung von Kernbereichsinformationen, soweit möglich unterbleibt.
- Hier liegt der Fokus auf Vorkehrungen bei der Aus-/Verwertungsebene. Wie bei WRÜW hat eine Vorlage sämtlicher erlangter Erkenntnisse an eine unabhängige Stelle zu erfolgen (Prüfungsumfang wie oben). Hierbei ist eine technisch/fachliche Unterstützung durch die Verfassungsschutzbehörde möglich.

**Anforderung BVerfGE v. 26.4.2022:****1. Absoluter Kernbereichsschutz auch im Bereich des Verfassungsschutzes.**

Auch für eingriffsintensive Überwachungsmaßnahmen der Verfassungsschutzbehörden gelten besondere Anforderungen an den Schutz des Kernbereichs privater Lebensgestaltung. Dieser sichert einen absoluten Achtungsanspruch, der auch angesichts der hochrangigen Aufgaben des Verfassungsschutzes nicht relativierbar ist (Rdnr. 275), d. h. eine Abwägung mit den Sicherheitsinteressen nach Maßgabe des Verhältnismäßigkeitsgrundsatzes ist nicht zulässig (Rn. 277).

**2. Frage des Erfordernisses einer expliziten gesetzlichen KB-Regelung**

Der Kernbereichsschutz ist bei allen Überwachungsmaßnahmen zu beachten.

- a) Eine Verpflichtung des Gesetzgebers, den Schutz normenklar zu regeln, besteht jedoch nur bei Maßnahmen, die typischerweise tief in die Privatsphäre eindringen und mit einiger Wahrscheinlichkeit höchstvertrauliche Situationen erfassen können (Rn. 167).

In seiner BKAG-Entscheidung zählte das BVerfG zu solchen Maßnahmen die Befugnis zu längerfristigen Bildaufzeichnungen und zu einem auf lange Zeit

angelegten Abhören und Aufzeichnen des nichtöffentlich gesprochenen Worts (BVerfG 141, 220; Rn. 176).

- b) Außerhalb solch verletzungsgeneigter Befugnisse bedarf es keiner eigenständigen Regelungen – der Kernbereichsschutz ist bei deren Anwendung unmittelbar von Verfassungs wegen zu beachten (Rn. 278).

### 3. Kernbereichsschutz auf Erhebungs- und Auswertungsebene

Dem Kernbereichsschutz ist bei der Durchführung der relevanten Maßnahmen auf zwei Ebenen Rechnung zu tragen:

- a) Auf der Ebene der Datenerhebung sind Vorkehrungen zu treffen, die eine unbeabsichtigte Miterfassung von Kernbereichsinformationen möglichst ausschließen.
- b) Auf der Ebene der nachgelagerten Auswertung und Verwertung sind die Folgen eines dennoch nicht vermiedenen Eindringens in die Kernbereichssphäre strikt zu minimieren (Rn. 277).

### 4. Kernbereichsschutz bei Wohnraumüberwachungen

Die Anforderungen an den Kernbereichsschutz sind hier besonders streng (Rn. 279)

Erhebungsebene (Rn. 280 f., 305)

Auf Erhebungsebene hat der Gesetzgeber eine ausdrückliche Vermutungsregelung vorzusehen.

Es gilt die **Vermutung**, dass Gespräche, die

- in Privaträumen
- mit Personen des besonderen persönlichen Vertrauens geführt werden, dem Kernbereich privater Lebensgestaltung unterfallen und nicht überwacht werden dürfen.

Für Räume, in denen solche Gespräche zu erwarten sind, scheidet entsprechend auch eine automatische Dauerüberwachung aus.

Diese **Vermutung kann widerlegt** werden, sofern für bestimmte Gespräche konkrete Anhaltspunkte vorliegen, dass sie

- einen unmittelbaren Straftatenbezug – der auch vorliegt, wenn sie mit höchstpersönlichen Inhalten durchsetzt sind – aufweisen
- oder ihnen insgesamt ein höchstvertraulicher Charakter fehlen wird. Hierfür genügt jedoch nicht die Prognose, dass sich in einem Gespräch höchstvertrauliche und alltägliche Fragen mischen werden.

Bei Erfassung höchstvertraulicher Situationen sind die Maßnahmen unverzüglich abzubrechen. Bestehen in dieser Lage über den höchstvertraulichen Charakter – etwa aus sprachlichen Gründen – Zweifel oder gibt es konkrete Anhaltspunkte, dass im Zusammenhang mit dem Austausch höchstprivater Gedanken auch Straftaten besprochen werden, kann die Überwachung in Form einer automatischen Aufzeichnung fortgeführt werden (Rn. 281).

#### Auswertungs- und Verwertungsebene (Rn. 282 f., 306)

Auf Auswertungs- und Verwertungsebene ist eine **unabhängige Sichtung** der Ergebnisse der Überwachung durch eine unabhängige Stelle erforderlich.

Sie dient sowohl der Rechtmäßigkeitskontrolle als auch dem Herausfiltern höchstvertraulicher Daten. Zu diesem Zweck hat eine **vollständige Vorlage der Aufzeichnungen** aus der Wohnraumüberwachung zu erfolgen.

*Anmerkung: Da die gesamte Maßnahme bereits durch einen Richter anzuordnen ist, dürfte sich die o. g. vom BVerfG geforderte „Rechtmäßigkeitskontrolle“ der (unabhängigen Stelle) auf die Rechtmäßigkeit der von der Verfassungsschutzbehörde vorgenommenen konkreten Datenerhebung beschränken. Diese muss sich in den Grenzen der richterlichen Anordnung gehalten haben.*

*Daneben hat die (unabhängige Stelle) etwa erfasste Kernbereichsinhalte zu identifizieren und auch unverzüglich selber zu löschen. Zwar gesteht das BVerfG zu, dass es bei der Datenerhebung bei Wohnraumüberwachungen unvermeidbar zu einer Kenntnisnahme von Kernbereichsinhalten kommen kann.*

*Jedoch betont es zugleich, dass es gelte, eine (weitere) Kenntnisnahme der Verfassungsschutzbehörde bei der unabhängigen Sichtung auf Auswertungsebene zu vermeiden (Rdnr. 283). Hieraus kann geschlossen werden, dass die unabhängige Stelle die Löschung der von ihr identifizierten Kernbereichsinhalte selber vorzunehmen hat, da ansonsten eine „weitere Kenntnisnahme“ von Kernbereichsinhalten durch die Verfassungsschutzbehörde naheliegen würde.*

Für Ausnahmefälle sind hinsichtlich der umfassenden Kontrolle bei **Gefahr im Verzug** besondere Regelungen möglich (Rn. 282).

Die unabhängige Sichtung schließt nicht von vornherein die **Möglichkeit einer automatischen Sichtung** aus, sofern diese der überwachenden Behörde (künftig) technisch zuverlässig möglich sein sollte.

Entscheidend ist, der Behörde über die bei der Erhebung unvermeidbare Kenntnisnahme hinaus im Zuge der Sichtung nicht noch weiter kernbereichsrelevante Daten offenbar werden (Rn. 283).

## 5. Kernbereichsschutz beim Verdeckten Zugriff auf informationstechnische Systeme (Rn. 284ff.; 313ff.)

- Die Anforderungen auf der Erhebungsebene etwas geringer als bei Wohnraumüberwachung. Der Kernbereichsschutz ist zu einem großen Teil auf die Auswertungs-/Verwertungsebene verschoben. (Rn. 284)
- Genügend ist die in Art. 8a Absatz 1 Nr. 1 BayVSG vorgesehene (*und dem Absatz 1 der allgemeinen KB-Regelung unten S. 12 entsprechende*) allgemeine Vorgabe zum Kernbereichsschutz (Rn. 314)
- Jedoch muss zusätzlich sichergestellt werden, dass die Erhebung von Kernbereichsinformationen, soweit wie informationstechnisch und ermittlungstechnisch möglich unterbleibt. Einzusetzen sind verfügbare **informationstechnische Sicherungen**, mit deren Hilfe höchstvertrauliche Informationen aufgespürt und isoliert werden können. Auf diese Informationen darf nicht zugegriffen werden. (Rn. 285)
- Wenn jedoch kernbereichsrelevante Daten in der konkreten Anwendung vor oder bei der Datenerhebung nicht ausgesondert werden können, ist ein Zugriff auf das informationstechnische System auch dann zulässig, wenn hierbei eine Wahrscheinlichkeit besteht, dass am Rande auch höchstpersönliche Daten miterfasst werden (Rn. 286).
- Dem Schutzbedarf ist durch Sicherungen auf der Aus- und Verwertungsebene Rechnung zu tragen.  
Zum Zweck unabhängiger Kontrolle ist eine Verpflichtung vorzusehen, alle aus der Online-Durchsuchung gewonnenen Daten einer unabhängigen Stelle vorzulegen, die kernbereichsrelevante Informationen vor Kenntnisnahme und Nutzung durch die Behörde herausfiltert [Rn. 286 unter Verweis auf BVerfGE 141, 220, 306 f. (Rn. 218 ff.); BVerfGE 120, 274, 338 f.]

### Regelungsvorschläge

#### Anmerkung:

Die Rechtsprechung verlangt explizite Kernbereichsregelungen nur bei Befugnissen, die tief in die Privatsphäre eingreifen und bei denen die Erhebung höchstpersönlicher Informationen wahrscheinlich ist. Diese Situation sieht sie bei Wohnraumüberwachungen, Online-DS, aber auch bei längerfristigen Bild- und Tonaufzeichnungen gegeben (vgl. zu letzteren: BVerfGE „BKAG“ 141, 220 (Rn. 176).

Vor diesem Hintergrund werden nachfolgend verschiedene Regelungsalternativen vorgeschlagen:

1. **Alternative (Minimallösung):**

Jede der drei o. g. Befugnisse erhält eine eigene Kernbereichsregelung;

Vorteile:

- Minimallösung, d. h. es wird nicht mehr geregelt, als nötig
- maßgeschneiderte KB-Regelungen
- Lesbarkeit des Gesetzes (z. B. müssen für WRÜW nicht eigens Abweichungen von der vorne geregelten allgemeinen KB-Regelung geregelt werden)

Nachteil: textliche Redundanzen

2. **Alternative (Add on); vgl. ab S. 12:):**

Ähnlich wie im BayVSG wird eine allgemeine, im Grundsatz für alle ND-Mittel geltende KB-Regelung vor die Klammer gezogen (Standort: zu Beginn des Abschnitts „ND-Mittel“).

Die Besonderheiten des KB-Schutzes bei Wohnraumüberwachungen und Online-DS werden in den jeweiligen Befugnissen bzw. Verfahrensvorschriften geregelt.

Vorteile:

- (politische) Willensbekundung, dem KB-Schutz bei der nachrichtendienstlichen Tätigkeit insgesamt Beachtung zu schenken
- Vermeidung von Redundanzen

Nachteil:

- Lesbarkeit des Gesetzes, da man sowohl die allgemeine KB-Regelung als auch die (andernorts geregelten) KB-Besonderheiten für WRÜW/ODS im Blick haben muss.

## Erste Alternative:

### Regelungsvorschläge

#### Kernbereichsregelung für längerfristige Bild- und Tonaufzeichnungen

(vgl. BVerfGE „BKAG“141, 220 (Rn. 176))

*In die Befugnis für längerfristige Bild- und Tonaufzeichnungen sind an geeigneter Stelle folgende Absätze aufzunehmen:*

(x) Die Maßnahme ist unzulässig, soweit aufgrund hinreichend gewichtiger tatsächlicher Anhaltspunkte anzunehmen ist, dass durch sie allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung gewonnen würden.

(y) <sup>1</sup> Erfolgt während der Maßnahme eine unmittelbare Kenntnisnahme<sup>1</sup> und ergeben sich tatsächliche Anhaltspunkte dafür, dass allein Daten aus dem Kernbereich privater Lebensgestaltung erfasst werden, ist die Maßnahme unverzüglich zu unterbrechen, sobald dies ohne Gefährdung oder Enttarnung eingesetzter Personen möglich ist und solange anzunehmen ist, dass allein solche Daten erfasst würden.

<sup>2</sup>Bestehen Zweifel, ob oder wie lange die Voraussetzungen nach Satz 1 vorliegen, darf die Maßnahme ausschließlich als automatische Aufzeichnung fortgeführt werden.

<sup>3</sup>Diese ist unverzüglich der [einfügen: *Bezeichnung der unabhängigen Stelle*] vorzulegen.

<sup>4</sup>Diese entscheidet unverzüglich über die Verwendbarkeit oder Löschung der Daten.

<sup>5</sup>Erfasste Daten aus dem Kernbereich privater Lebensgestaltung dürfen nicht weiterverwendet werden und sind unverzüglich zu löschen.

<sup>6</sup>Die Tatsachen der Erfassung der Daten und der Löschung sind ausschließlich für Zwecke der Datenschutzkontrolle zu dokumentieren.<sup>2</sup>

---

<sup>1</sup> Damit wird klargestellt, dass eine unmittelbare Kenntnisnahme durch die Verfassungsschutzbehörde nicht obligatorisch vorausgesetzt wird (wie der Wortlaut des aktuellen Art. 8a Abs. 1 S. 2 BayVSG u. U. nahelegt).

<sup>2</sup> Die noch im BKAG-Urteil geforderten Fristen zur Aufbewahrung der Dokumente zur Erfassung/Löschung der KB-Daten (BVerfG 141, 220; Rdnr. 305) wurden im aktuellen BVerfG-Urteil nicht mehr angesprochen, obwohl sie im BayVSG fehlen.

## **Kernbereichsregelung für Wohnraumüberwachungen und Online-Durchsuchungen**

### **Anmerkung:**

*Beide Maßnahmen sind gleichermaßen eingriffstief und haben daher weitgehend identische Verfahrensvorschriften (vgl. in Anlage 5: gemeinsame Verfahrensvorschrift in §/Art. C für beide Befugnisse).*

*Aus diesem Grund wurden auch die Besonderheiten des KB-Schutzes für beide Befugnisse in die gemeinsame Verfahrensvorschrift eingearbeitet (vgl. unten §/Art. C Absatz 3 (WRÜW) und Absatz 4 (ODS)).*

### **§/Art. [A] – Verdeckter Einsatz technischer Mittel zur Wohnraumüberwachung**

(1) <sup>1</sup>Das Landesamt darf zur Abwehr einer dringenden Gefahr für

1. den Bestand oder die Sicherheit des Bundes oder eines Landes,
2. Leib, Leben oder Freiheit einer Person oder
3. Sachen, deren Erhaltung im besonderen öffentlichen Interesse geboten ist.

bei der Erhebung personenbezogener Daten im Schutzbereich von Art. 13 GG [und Art. XX der Landesverfassung] verdeckt technische Mittel einsetzen, um das nichtöffentlich gesprochene Wort abzuhören und aufzuzeichnen sowie Lichtbilder und Bildaufzeichnungen herzustellen.

**<sup>2</sup>Werden in Privaträumen Gespräche mit Personen des besonderen persönlichen Vertrauens geführt, ist die Maßnahme unzulässig.**

**<sup>3</sup>Dies gilt nicht, wenn tatsächliche Anhaltspunkte<sup>3</sup> die Annahme rechtfertigen, dass**

- 1. den Gesprächen insgesamt ein höchstvertraulicher Charakter fehlen wird oder**
- 2. die Gespräche unmittelbar die Besprechung oder Planung von Straftaten, die sich gegen die in Satz 1 genannten Rechtsgüter richten, zum Gegenstand haben werden.<sup>4</sup>**

---

<sup>3</sup> Das BVerfG spricht von „*konkreten Anhaltspunkten*“. Dem dürften im verfassungsschutzrechtlichen Fachjargon die „tatsächlichen Anhaltspunkte“ entsprechen. Durch diesen Begriff ist sichergestellt, dass nicht „ins Blaue hinein“ von einem Sachverhalt ausgegangen werden kann, der die ursprüngliche (Kernbereichs-)Vermutung widerlegt.

<sup>4</sup> Das BVerfG spricht im aktuellen Urteil nur allgemein davon, dass die Vermutung widerlegt werden kann, wenn ein „*unmittelbarer Straftatenbezug*“ vorliegt, ohne dass bestimmte Straftaten verlangt werden. Es erscheint jedoch sachgerecht, dass sich die Straftaten gegen diejenigen Schutzgüter richten müssen, für die bei Wohnraumüberwachungen eine dringende Gefahr vorliegen muss.

In BVerfG

<sup>4</sup>Zur Vorbereitung und Durchführung der Maßnahme darf die Wohnung auch ohne Wissen des Inhabers und der Bewohner betreten werden, wenn dies ausdrücklich angeordnet wurde.

<sup>5</sup>Die Maßnahme ist nur zulässig, wenn die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre und geeignete polizeiliche Hilfe für das betroffene Rechtsgut nicht rechtzeitig erlangt werden kann.

(2) <sup>1</sup>Die Maßnahme darf sich nur gegen eine Person richten, ...  
(weiter wie bei Anlage 5; dort §/Art. A Absatz 2)

(3) <sup>1</sup>Personenbezogene Daten, die durch eine Maßnahme ...  
(weiter wie bei Anlage 5; dort §/Art. A Absatz 3)

### **§/Art. [B] – Verdeckter Zugriff auf informationstechnische Systeme**

(1) (wie Anlage 5; dort §/Art. B Absatz 1)

(2) <sup>1</sup>Durch technische Maßnahmen ist sicherzustellen, dass

1. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind,
2. die vorgenommenen Veränderungen bei Beendigung der Maßnahme soweit technisch möglich automatisiert rückgängig gemacht werden und
- 3. Daten, die den Kernbereich privater Lebensgestaltung betreffen, soweit technisch möglich nicht erhoben werden.**

<sup>2</sup>Das eingesetzte Mittel ist (...)

(Sätze 2 und 3 wie bei Anlage 5; dort §/Art. B Absatz 1 S. 2 und 3)

(3) (Absatz 3 wie bei Anlage 5; dort §/Art. B Absatz 3)

(4) (Absatz 4 wie bei Anlage 5; dort §/Art. B Absatz 4)



## **§/Art. [C] – Verfahren bei den Maßnahmen nach [A - Wohnraumüberwachung] und [B – Online-DS]**

(1) <sup>1</sup>Der Einsatz technischer Mittel nach den [§/Art. A] und [B] bedarf einer richterlichen Anordnung.

<sup>2</sup>Bei Gefahr im Verzug kann die Behördenleitung oder ihre Vertretung die Anordnung treffen; eine richterliche Entscheidung ist unverzüglich nachzuholen.

(2) <sup>1</sup>Die Anordnung ist auf höchstens einen Monat zu befristen.

<sup>2</sup>Verlängerungen um jeweils nicht mehr als einen weiteren Monat sind zulässig, soweit die Voraussetzungen der Anordnung fortbestehen.

**(3) <sup>1</sup> Erfolgt während der Maßnahme nach §/Art. A (WRÜW) eine unmittelbare Kenntnisnahme<sup>5</sup> und ergeben sich hinreichend gewichtige Anhaltspunkte dafür, dass allein Daten aus dem Kernbereich privater Lebensgestaltung erfasst werden, ist die Maßnahme unverzüglich zu unterbrechen, sobald dies ohne Gefährdung oder Enttarnung eingesetzter Personen<sup>6</sup> möglich ist und solange anzunehmen ist, dass allein solche Daten erfasst würden.**

<sup>2</sup>Bestehen Zweifel, ob oder wie lange die Voraussetzungen nach Satz 1 vorliegen, darf die Maßnahme ausschließlich als automatische Aufzeichnung fortgeführt werden.

<sup>3</sup>Die (*einfügen: Verfassungsschutzbehörde*) darf erfasste Daten aus dem Kernbereich privater Lebensgestaltung nicht weiterverwenden und hat sie unverzüglich zu löschen<sup>7</sup>.

<sup>4</sup>Die Tatsachen der Erfassung der Daten und der Löschung sind ausschließlich für Zwecke der Datenschutzkontrolle zu dokumentieren.<sup>8</sup>

<sup>5</sup>Sämtliche durch die Maßnahmen nach §/Art. A (WRÜW) erlangten Daten sind unverzüglich der/dem [*einfügen: Bezeichnung der unabhängigen Stelle*] vorzulegen.

<sup>6</sup>Diese entscheidet unverzüglich, ob die Maßnahme der Anordnung entsprechend durchgeführt wurde.

---

<sup>5</sup> Damit wird klargestellt, dass eine unmittelbare Kenntnisnahme durch die Verfassungsschutzbehörde nicht obligatorisch vorausgesetzt wird (wie der Wortlaut des Art. 8a Abs. 1 S. 2 BayVSG nahelegt).

<sup>6</sup> Dieser Halbsatz ist auch für WRÜW relevant, da Verfassungsschutzbedienstete auch während der WRÜW-Maßnahme in der Wohnung anwesend sein dürfen (vgl. §/Art. A Absatz 1 Satz 2).

<sup>7</sup> Das BVerfG geht selber davon aus, dass es trotz der Vorkehrungen auf Erhebungsebene bei WRÜW zur Erhebung von KB-Daten kommen kann (vgl. Rdnr.: 283 „über bei der Erhebung unvermeidbare Kenntnisnahmen hinaus...“)

<sup>8</sup> Die noch im BKAG-Urteil geforderten Fristen zur Aufbewahrung der Dokumente zur Erfassung/Löschung der KB-Daten (BVerfG 141, 220; Rdnr. 305) wurden im aktuellen BVerfG-Urteil nicht mehr angesprochen, obwohl sie im BayVSG fehlen.

**<sup>7</sup>Sind Daten aus dem Kernbereich privater Lebensgestaltung erfasst worden, so nimmt sie unverzüglich deren Löschung vor; Satz 4 gilt entsprechend.<sup>9</sup>**

**(4) <sup>1</sup>Die Anwendung der Maßnahme nach §/Art. B (Online-DS) ist unzulässig, soweit aufgrund hinreichend gewichtiger tatsächlicher Anhaltspunkte anzunehmen ist, dass durch sie allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung gewonnen würden<sup>10</sup>.**

**<sup>2</sup>Absatz 3 Satz 5 bis 7 gilt entsprechend<sup>11</sup>.**

**<sup>3</sup>Sofern es für die Sichtung der erlangten Daten aus technischen oder fachlichen Gründen erforderlich ist, kann die (einfügen: unabhängige Stelle)**

- 1. Bedienstete des/der (einfügen: Bezeichnung der Verfassungsschutzbehörde) zur Unterstützung heranziehen,**
- 2. technische Unterstützung durch (einfügen: Bezeichnung der Verfassungsschutzbehörde) in Anspruch nehmen.**

**<sup>4</sup>Die zur Unterstützung herangezogenen Bediensteten dürfen von erfassten Daten aus dem Kernbereich privater Lebensgestaltung nur insoweit Kenntnis erlangen, als dies für die Unterstützung unvermeidbar ist.**

**<sup>5</sup>Über den Inhalt dieser Daten haben sie Stillschweigen zu bewahren.<sup>12</sup>**

**(5)<sup>1</sup> § 4 Absatz 1 und 2 Satz 2 sowie ... zu ermitteln ist. (vgl. bei Anlage 5; §/Art. C)**

**(6)<sup>1</sup> Dient der Einsatz technischer Mittel ... (vgl. bei Anlage 5; §/Art. C)**

**(7) Zuständig für richterliche Entscheidungen ... (vgl. bei Anlage 5; §/Art. C)**

---

<sup>9</sup> Dass die unabhängige Stelle die Löschung selber vornehmen muss (und nicht die Verfassungsschutzbehörde), ergibt sich aus Rdnr. 283: „Entscheidend ist, dass der überwachenden Behörde über bei der Erhebung unvermeidbare Kenntnisnahmen hinaus, nicht noch weitere kernbereichsrelevante Daten offenbar werden. Es darf also bei der dem Kernbereichsschutz dienenden Sichtung auf Auswertungsebene nicht zu einer (weiteren) Kenntnisnahme durch die Behörde kommen.“

<sup>10</sup> Das BVerfG hat für die Vorkehrungen auf Erhebungsebene bei ODS den Inhalt der allgemeinen KB-Regelung (Art. 8a Abs. 1 BayVSG) für ausreichend erachtet, vgl. Rdnr. 314). Ergänzend hinzukommen muss jedoch die technische Vorkehrung; vgl. unten in §/Art. B Absatz 1 S. 2 Nr. 3)

<sup>11</sup> Eine Regelung, wonach die Verfassungsschutzbehörde die Kernbereichsdaten nicht verwenden darf und sie diese unverzüglich zu löschen hat, erscheint hier entbehrlich, da die Behörde in die digitalen Daten überhaupt erst dann Einsicht nehmen kann, wenn diese durch die unabhängige Stelle bereits um die Kernbereichsdaten bereinigt wurden.

<sup>12</sup>vgl. hierzu Rdnr. 315 sowie BVerfG 141, 220, Rdnr. 218 ff und BVerfG 120, 274 (338f)

## **Zweite Alternative (Add on):**

### **I. Allgemeine KB-Regelung für sämtliche Befugnisse;**

#### **§/Art. (...)**

#### **Schutz des Kernbereichs privater Lebensgestaltung**

(1) Die Anwendung nachrichtendienstlicher Mittel ist unzulässig, soweit aufgrund hinreichend gewichtiger tatsächlicher Anhaltspunkte anzunehmen ist, dass durch sie allein Daten aus dem Kernbereich privater Lebensgestaltung gewonnen würden.

(2) <sup>1</sup> Erfolgt während der Anwendung nachrichtendienstlicher Mittel eine unmittelbare Kenntnisnahme<sup>13</sup> und treten die Voraussetzungen des Absatzes 1 ein, ist die Maßnahme unverzüglich zu unterbrechen, sobald dies ohne Gefährdung oder Enttarnung eingesetzter Personen möglich ist und solange anzunehmen ist, dass diese Voraussetzungen vorliegen.

<sup>2</sup>Bestehen Zweifel, ob oder wie lange die Voraussetzungen des Absatzes 1 vorliegen, darf die Maßnahme ausschließlich als automatische Aufzeichnung fortgeführt werden.

<sup>3</sup>Diese ist unverzüglich der [einfügen: Bezeichnung der jeweils zu bestimmenden unabhängigen Stelle] vorzulegen.

<sup>4</sup>Diese entscheidet unverzüglich über die Verwendbarkeit oder Löschung der Daten.

<sup>5</sup>Erfasste Daten nach Absatz 1 dürfen nicht weiterverwendet werden und sind unverzüglich zu löschen.

<sup>6</sup>Die Tatsachen der Erfassung der Daten und der Löschung sind ausschließlich für Zwecke der Datenschutzkontrolle zu dokumentieren.<sup>14</sup>

---

<sup>13</sup> Damit wird klargestellt, dass eine begleitende Live-Kenntnisnahme durch die Verfassungsschutzbehörde nicht obligatorisch vorausgesetzt wird (wie der Wortlaut des Art. 8a Abs. 1 S. 2 BayVSG nahelegt).

<sup>14</sup> Die noch im BKAG-Urteil geforderten Fristen zur Aufbewahrung der Dokumente zur Erfassung/ Löschung der KB-Daten (BVerfG 141, 220; Rdnr. 305) wurden im aktuellen BVerfG-Urteil nicht mehr angesprochen, obwohl sie im BayVSG fehlen.

## II. Ergänzend:

### Regelung der Besonderheiten des KB-Schutzes in den besonderen Befugnis-/Verfahrensnormen

#### Anmerkung zum KB-Schutz bei längerfristigen Bild- und Tonaufzeichnungen:

Für das ND-Mittel der längerfristigen Bild- und Tonaufzeichnungen genügt die allgemeine KB-Regelung oben Ziffer I. Es bedarf hier keiner Sonderregelungen in der speziellen Befugnisnorm. Dies ist deswegen anzunehmen, weil das BVerfG bei der Bayer. Befugnis zu längerfristigen Observationen nicht das Fehlen einer ausreichenden KB-Schutzregelung moniert hat.

#### Anmerkung zum KB-Schutz bei WRÜW<sup>15</sup>:

Standort der Sonderregelung zur „widerleglichen Vermutung“ (Erhebungsebene):

→ in der Befugnisnorm, vgl. nachfolgend §/Art. A Absatz 1 Satz 2 und 3

Standort der Sonderregelung „Vorlage sämtlicher Erkenntnisse an unabhängige Stelle“ (Auswertungsebene):

→ in der Verfahrensregelung vgl. nachfolgend §/Art. C Absatz 3

#### Anmerkung zum KB-Schutz bei Online-DS:

Für die Vorkehrungen auf Erhebungsebene genügt Absatz 1 der allgemeinen Kernbereichsregelung oben;

jedoch ergänzt durch die technische Sicherstellungspflicht unten in §/Art. B Absatz 2 Satz 1 Nr. 3.

Für die Vorkehrungen auf Auswertungsebene gelten die Verfahrensregelungen in §/Art. C Absatz 4 (unten).

---

<sup>15</sup> Die vom BMI angeregte Übernahme der KB-Regelung für WRÜW in § 42 Abs. 7 BKAG wird nicht für sachgerecht gehalten. Sie enthält

- keine explizite widerlegliche Vermutung,
- keine Regelung, wonach die Maßnahme bei Zweifelsfällen (wenigstens noch) als automatische Aufzeichnung fortgeführt werden darf,
- keine Pflicht der unabhängigen Stelle, neben dem Kernbereichsdaten-Check auch eine (zumindest eingeschränkte) Rechtmäßigkeitskontrolle durchzuführen.

## §/Art. [A]

### **Verdeckter Einsatz technischer Mittel zur Wohnraumüberwachung**

- (1) <sup>1</sup>Das Landesamt darf zur Abwehr einer dringenden Gefahr für
1. den Bestand oder die Sicherheit des Bundes oder eines Landes,
  2. Leib, Leben oder Freiheit einer Person oder
  3. Sachen, deren Erhaltung im besonderen öffentlichen Interesse geboten ist.

bei der Erhebung personenbezogener Daten im Schutzbereich von Art. 13 GG [und Art. XX der Landesverfassung] verdeckt technische Mittel einsetzen, um das nichtöffentlich gesprochene Wort abzuhören und aufzuzeichnen sowie Lichtbilder und Bildaufzeichnungen herzustellen.

**<sup>2</sup>Werden in Privaträumen Gespräche mit Personen des besonderen persönlichen Vertrauens geführt, ist die Maßnahme abweichend von §/Art. (*einfügen: Bezeichnung der allg. Kernbereichsregelung*) Absatz 1 unzulässig.**

**<sup>3</sup>Dies gilt nicht, wenn tatsächliche Anhaltspunkte<sup>16</sup> die Annahme rechtfertigen, dass**

- 1. den Gesprächen insgesamt ein höchstvertraulicher Charakter fehlen wird oder**
- 2. die Gespräche unmittelbar die Besprechung oder Planung von Straftaten, die sich gegen die in Satz 1 genannten Rechtsgüter richten, zum Gegenstand haben werden.<sup>17</sup>**

<sup>4</sup> Zur Vorbereitung und Durchführung der Maßnahme darf die Wohnung auch ohne Wissen des Inhabers und der Bewohner betreten werden, wenn dies ausdrücklich angeordnet wurde.

<sup>5</sup>Die Maßnahme ist nur zulässig, wenn die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre und geeignete polizeiliche Hilfe für das betroffene Rechtsgut nicht rechtzeitig erlangt werden kann.

- (2) <sup>1</sup>Die Maßnahme darf sich nur gegen eine Person richten, ... (weiter wie bei Anlage 5)

---

<sup>16</sup> Das BVerfG spricht von „*konkreten Anhaltspunkten*“. Dem dürften im verfassungsschutzrechtlichen Fachjargon die „tatsächlichen Anhaltspunkte“ entsprechen. Durch diesen Begriff ist sichergestellt, dass nicht „ins Blaue hinein“ von einem Sachverhalt ausgegangen werden kann, der die ursprüngliche (Kernbereichs-)Vermutung widerlegt.

<sup>17</sup> Das BVerfG spricht im aktuellen Urteil nur allgemein davon, dass die Vermutung widerlegt werden kann, wenn ein „*unmittelbarer Straftatenbezug*“ vorliegt, ohne dass bestimmte Straftaten verlangt werden. Es erscheint jedoch sachgerecht, dass sich die Straftaten gegen diejenigen Schutzgüter richten müssen, für die bei Wohnraumüberwachungen eine dringende Gefahr vorliegen muss.

(3) <sup>1</sup>Personenbezogene Daten, die durch eine Maßnahme ... (weiter wie bei Anlage 5)

## §/Art. [B]

### Verdeckter Zugriff auf informationstechnische Systeme

(1) (wie bei Anlage 5)

(2) <sup>1</sup>Durch technische Maßnahmen ist sicherzustellen, dass

1. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind,
2. die vorgenommenen Veränderungen bei Beendigung der Maßnahme soweit technisch möglich automatisiert rückgängig gemacht werden und
- 3. Daten, die den Kernbereich privater Lebensgestaltung betreffen, soweit technisch möglich nicht erhoben werden.**

<sup>2</sup>Das eingesetzte Mittel ist (... Satz 2 und 3 weiter wie bei Anlage 5)

(3) (Absatz 3 wie bei Anlage 5)

(4) (Absatz 4 wie bei Anlage 5)

## §/Art. [C]

### Verfahren bei den Maßnahmen nach [A - Wohnraumüberwachung] und [B – Online-DS]

(1) <sup>1</sup>Der Einsatz technischer Mittel nach den [§/Art. A] und [B] bedarf einer richterlichen Anordnung.

<sup>2</sup>Bei Gefahr im Verzug kann die Behördenleitung oder ihre Vertretung die Anordnung treffen; eine richterliche Entscheidung ist unverzüglich nachzuholen.

(2) <sup>1</sup>Die Anordnung ist auf höchstens einen Monat zu befristen.

<sup>2</sup>Verlängerungen um jeweils nicht mehr als einen weiteren Monat sind zulässig, soweit die Voraussetzungen der Anordnung fortbestehen.

(3) <sup>1</sup>Abweichend von §/Art. (einfügen: *Bezeichnung der allgemeinen Kernbereichsvorschrift; vgl. oben S. 12*) Absatz 2 Satz 3 und 4 sind sämtliche durch eine Maßnahme nach [§/Art. A - Wohnraumüberwachung] erlangten Daten unverzüglich der [einfügen: *Bezeichnung der unabhängigen Stelle*] vorzulegen.

<sup>2</sup>Diese entscheidet unverzüglich, ob die Maßnahme der Anordnung entsprechend durchgeführt wurde.

<sup>3</sup>Sind Daten aus dem Kernbereich privater Lebensgestaltung erfasst worden, so nimmt sie unverzüglich deren Löschung vor.<sup>18</sup>

(4) <sup>1</sup>Abweichend von §/Art. (*allgemeine Kernbereichs-Regelung auf S. 12*) Absatz 2 Satz 1 bis 4<sup>19</sup> sind sämtliche durch eine Maßnahme nach [§/Art. B – Online-DS] erlangten Daten unverzüglich der [einfügen: *Bezeichnung der unabhängigen Stelle*] vorzulegen.<sup>20</sup>

<sup>2</sup> Absatz 3 Satz 2 und 3 gilt entsprechend.

---

<sup>18</sup> Dass die unabhängige Stelle bei Wohnraumüberwachungen selbst löschen muss (und nicht die Verfassungsschutzbehörde), ergibt sich aus Rdnr. 283: „Entscheidend ist, dass der überwachenden Behörde über bei der Erhebung unvermeidbare Kenntnisnahmen hinaus, nicht noch weiter kernbereichsrelevante Daten offenbar werden. Es darf also bei der dem Kernbereichsschutz dienenden Sichtung auf Auswertungsebene nicht zu einer (weiteren) Kenntnisnahme durch die Behörde kommen.“

<sup>19</sup> Absatz 2 S. 1 bis 4 der allg. KB-Regelung (→ Unterbrechung; Zweifelsfall-Aufzeichnung; deren Vorlage an unabhängige Stelle) sind für die Auswertungsebene bei Online-DS unpassend und werden daher hier (anders als in Abs. 3 bei WRÜW) für nicht anwendbar erklärt.

Absatz 2 S. 5 und 6 der allg. KB-Regelung gelten hingegen auch bei ODS, denn durch die einzurichtenden „technischen Sicherungen“ (§/Art. B Abs. 2 S. 1 Nr. 3) kann es bei der ODS-Datenerhebung zur Isolierung von KB-Inhalten kommen, die sodann von der Verfassungsschutzbehörde zu löschen sind.

<sup>20</sup> Für Online-Durchsuchungen genügt als Vorkehrung auf Erhebungsebene der Absatz 1 der allgemeinen Kernbereichsregelung (vgl. S. 12), jedoch verbunden mit einer Verpflichtung zur Vornahme entsprechender technischer Sicherungen (vgl. Rdnr. 313 und §/Art. B Abs. 2 S. 1 Nr. 3).

<sup>3</sup> Sofern es für die Sichtung der erlangten Daten aus technischen oder fachlichen Gründen erforderlich ist, kann die (*einfügen: Bezeichnung der unabhängigen Stelle*)

1. Bedienstete des/der (*einfügen: Bezeichnung der Verfassungsschutzbehörde*) zur Unterstützung heranziehen und
2. technische Unterstützung durch (*einfügen: Bezeichnung der Verfassungsschutzbehörde*) in Anspruch nehmen.

<sup>4</sup>Die zur Unterstützung herangezogenen Bediensteten dürfen von erfassten Daten aus dem Kernbereich privater Lebensgestaltung nur insoweit Kenntnis erlangen, als dies für die Unterstützung unvermeidbar ist.

<sup>5</sup>Über den Inhalt dieser Daten haben sie Stillschweigen zu bewahren.<sup>21</sup>

(5) bis (7)

(Absätze 5 bis 7 wie bei Anlage 5)

---

<sup>21</sup>vgl. hierzu Rdnr. 315 sowie BVerfG 141, 220, Rdnr. 218 ff und BVerfG 120, 274 (338f)



## **Begründung**

### Anmerkung:

*Zur Vermeidung von Redundanzen wird darauf verzichtet, sowohl für die 1. Alternative (=spezielle KB-Regelungen nur dort, wo zwingend notwendig) als auch für die 2. Alternative (Add on: Allgemeine KB-Regelung plus KB-Besonderheiten in einzelnen Befugnissen) gesonderte Begründungen zu erstellen.*

*Die nachfolgende Begründung bezieht sich daher nur auf das vom BayVSG verfolgte Modell der 2. Alternative.*

### **Begründung für die allgemeine KB-Regelung (oben S. 12)**

Das Bundesverfassungsgericht (BVerfG) stellte zuletzt in seinem Urteil zum Bayerischen Verfassungsschutzgesetz fest, dass der Gesetzgeber für Überwachungsmaßnahmen, die typischerweise zur Erhebung kernbereichsrelevanter Daten führen können, Regelungen schaffen muss, die einen wirksamen Schutz des Kernbereichs privater Lebensgestaltung normenklar gewährleisten (vgl. BVerfG, Ur. vom 26. April 2022, Az: 1 BvR 1619/17, Rdnr. 167).

Auch wenn das BVerfG eine eigene gesetzliche Regelung nur für tief in die Privatsphäre eingreifende Befugnisse fordert, die „typischerweise zur Erhebung kernbereichsrelevanter Daten führen“, soll – im Hinblick auf die generell höhere Schutzbedürftigkeit solcher sensiblen Daten – nun mit §/Art. (*Bezeichnung allgemeine KB-Regelung*) eine allgemeine Regelung für den Schutz dieser Daten beim Einsatz sämtlicher nachrichtendienstlicher Mittel geschaffen werden. Sie gilt, soweit nicht spezielle Regelungen für besondere nachrichtendienstlichen Mittel getroffen wurden.

Dem Kernbereichsschutz ist auf zwei Ebenen Rechnung zu tragen. Zum einen sind auf der Ebene der Datenerhebung Vorkehrungen zu treffen, die eine unbeabsichtigte Miterfassung von Kernbereichsinformationen nach Möglichkeit ausschließen (Absatz 1). Zum anderen sind auf der Ebene der nachgelagerten Auswertung und Verwertung die Folgen eines dennoch nicht vermiedenen Eindringens in den Kernbereich privater Lebensgestaltung strikt zu minimieren (Absatz 2; BVerfG, a. a. O., Rdnr. 277).

Auf der Ebene der Datenerhebung ist bei verletzungsgeneigten Maßnahmen durch eine vorgelagerte Prüfung sicherzustellen, dass die Erfassung von kernbereichsrelevanten Situationen oder Gesprächen jedenfalls insoweit ausgeschlossen ist, als sich diese mit praktisch zu bewältigendem Aufwand im Vorfeld vermeiden lässt.

#### Zu Absatz 1

Eine Datenerhebung ist bereits dann unzulässig, wenn hinreichend gewichtige tatsächliche Anhaltspunkte für die Annahme vorliegen, dass durch sie allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erfasst würden. Solche Anhaltspunkte können sich insbesondere aus dem Verhältnis der erfassten Personen zueinander und der Art der zu überwachenden Räumlichkeiten ergeben. Es ist daher bereits vor der Durchführung der Maßnahme eine Prognose dahingehend zu treffen, dass mit der Maßnahme nicht allein Kernbereichsinhalte erfasst werden. Eine Kommunikation über Höchstvertrauliches fällt dabei nicht schon deshalb aus dem strikt zu schützenden Kernbereich heraus, weil sich in ihr höchstvertrauliche mit alltäglichen Informationen mischen (vgl. BVerfGE 109, 279, 330).

Schützenswert ist insbesondere die nichtöffentliche Kommunikation mit Personen des besonderen persönlichen Vertrauens. Zu diesen Personen gehören insbesondere Ehe- oder Lebenspartner, Geschwister und Verwandte in gerader Linie, vor allem, wenn sie im selben Haushalt leben, und können Strafverteidiger, Ärzte, Geistliche und enge persönliche Freunde zählen (BVerfGE 141, 220, Rn. 121).

#### Zu Absatz 2

Erfolgt während der Anwendung nachrichtendienstlicher Mittel eine unmittelbare Kenntnisnahme durch Bedienstete und treten die Voraussetzungen des Absatzes 1 ein, ist die Maßnahme nach Satz 1 unverzüglich zu unterbrechen. Eine Unterbrechung unterbleibt jedoch, wenn durch sie eine unmittelbare, konkrete Gefahr für Leib oder Leben eingesetzter Personen oder deren Enttarnung zu befürchten ist. Die Unterbrechung dauert an, solange anzunehmen ist, dass die Voraussetzungen des Absatzes 1 vorliegen.

Wenn Zweifel darüber bestehen, ob im Einzelfall die Voraussetzungen des Absatzes 1 vorliegen oder ob sie noch fort dauern, darf die Maßnahme – sofern nach Art der Maßnahme möglich – nur in Form einer automatischen Aufzeichnung fortgeführt werden, d. h. eine etwaige unmittelbare Kenntnisnahme durch Bedienstete des Verfassungsschutzes ist abubrechen (Satz 2).

Zweifel, *ob* Kernbereichsinhalte erfasst werden, können neben sprachlichen Verständnisproblemen z. B. dann bestehen, wenn unklar ist, ob dem Gespräch im konkreten Fall ein insgesamt höchstpersönlicher Charakter fehlt oder ob höchstpersönliche Inhalte tatsächlich derart mit unmittelbaren Straftatbezügen durchmischt sind, dass dieser Gesprächsteil wegen des Sozialbezugs insgesamt aus dem Kernbereichsschutz herausfällt.

Bei bestehenden Zweifeln ist eine unmittelbare Kenntnisnahme durch Bedienstete einzustellen. Eine etwaige – dann allein noch zulässige – automatische „Zweifelsfall“-Aufzeichnung ist nach Satz 3 unverzüglich (*der unabhängigen Stelle*) vorzulegen, welche wiederum unverzüglich über die Verwendbarkeit oder Löschung der Daten zu entscheiden hat (Satz 4).

Da nicht ausgeschlossen werden kann, dass trotz aller Sicherheitsvorkehrungen auf der Erhebungsebene Daten erfasst werden, die den Kernbereich betreffen, wird ein Verbot der weiteren Verwendung sowie ein Gebot zur sofortigen Löschung dieser Daten normiert. Die Tatsachen der Erfassung und Löschung von geschützten Kernbereichsdaten sind zur Ermöglichung einer Datenschutzkontrolle zu dokumentieren (Satz 5 und 6).

### **Begründung der Regelung zur widerleglichen Vermutung in der Befugnisnorm für Wohnraum-Überwachungen**

#### **§/Art. A Absatz 1 S. 2 und 3:**

Da Wohnraumüberwachungen besonders tief in die Privatsphäre und den persönlichen, zur Wahrung der Menschenwürde besonders wichtigen Rückzugsraum des Einzelnen eindringen können, sind bei ihnen die Anforderungen an den Kernbereichsschutz besonders streng (BVerfG, Urt. vom 26. April 2022, 1 BvR 1619/17, Rn. 279). Spezifische verfassungsrechtliche Anforderungen ergeben sich zum einen auf der Datenerhebungsebene - erste Stufe -, zum anderen aber auch auf der Auswertungs- und Verwertungsebene - zweite Stufe - (BVerfG, a. a. O., Rn. 280f., 282f.).

Auf Erhebungsebene gilt eine besondere Vermutungsregelung. So gilt die widerlegliche Vermutung, dass Gespräche, die in Privaträumen mit Personen des besonderen persönlichen Vertrauens geführt werden, dem Kernbereich privater Lebensgestaltung unterfallen und nicht überwacht werden dürfen (Satz 2). Für Räume, in denen solche Gespräche zu erwarten sind, scheidet entsprechend auch eine automatische Dauerüberwachung aus (BVerfG, a. a. O., Rn. 280, 305).

Diese Vermutung kann jedoch widerlegt werden, sofern für ein bestimmtes Gespräch konkrete Anhaltspunkte vorliegen, dass es

- einen unmittelbaren Straftatenbezug aufweist – der auch vorliegt, wenn das Gespräch dabei auch mit höchstpersönlichen Inhalten durchsetzt ist –  
oder
- ihm insgesamt ein höchstvertraulicher Charakter fehlen wird (Satz 3).  
Hierfür genügt jedoch nicht die Prognose, dass sich in einem Gespräch

höchstvertrauliche und alltägliche Fragen mischen werden (vgl. BVerfG, a.a.O., Rn. 280):

Besteht danach die Wahrscheinlichkeit, dass eine Überwachungsmaßnahme in den Kernbereich privater Lebensgestaltung eindringt, ist die Maßnahme zu unterlassen. Bestehen dagegen Anhaltspunkte dafür, dass bestimmten Gesprächen ein höchstvertraulicher Charakter fehlen wird, dürfen die Maßnahmen durchgeführt werden.

**Begründung** der Regelung in der Online-DS-Befugnis für eine „**technische Sicherstellung, dass Daten, die den KB privater Lebensgestaltung betreffen, soweit technisch möglich nicht erhoben werden**“

**§/Art. B Absatz 2 S. 1 Nr. 3:**

Für den Kernbereichsschutz bei Online-DS verlangt das BVerfG als Vorkehrung auf Erhebungsebene, dass die Erhebung von Informationen, die dem Kernbereich zuzuordnen sind, soweit wie informationstechnisch und ermittlungstechnisch möglich unterbleibt. Insbesondere seien verfügbare informationstechnische Sicherungen einzusetzen. Können mit deren Hilfe höchstvertrauliche Informationen aufgespürt und isoliert werden, ist der Zugriff auf diese untersagt (BVerfG, a.a.O., Rdnr. 285).

Nummer 3 sieht dementsprechend eine Verpflichtung für die Einrichtung einer solchen technischen Sicherstellung vor.

**Begründung** der Regelung „**Vorlage aller Erkenntnisse an unabhängige Stelle**“ bei **Wohnraum-Überwachungen**

**§/Art. C Absatz 3:**

Wenn sich im Zuge einer unmittelbaren „Live-Kennntnisnahme“ einer Wohnraum-Überwachung – trotz der ursprünglich für widerlegt erachteten Vermutung nach §/Art. A Absatz 1 S. 2 und 3 – nunmehr hinreichend gewichtige tatsächliche Anhaltspunkte dafür ergeben sollten, dass allein Kernbereichsinhalte erfasst werden, so ist die Maßnahme unverzüglich abubrechen. Bestehen in dieser Lage über den höchstvertraulichen Charakter – etwa aus sprachlichen Gründen – Zweifel oder gibt es konkrete Anhaltspunkte, dass im Zusammenhang mit dem Austausch höchstprivater Gedanken auch Straftaten besprochen werden, kann die Überwachung in Form einer automatischen Aufzeichnung fortgeführt werden (BVerfG, a.a.O., Rn. 281). Es gilt die allgemeine Regelung in §/Art. (*allg. Kernbereichsregelung*) Absatz 2 Satz 1 und 2.

Abweichend von (*allg. Kernbereichsregelung*) Absatz 2 Satz 3 und 4 sind jedoch nicht nur derartige „Zweifelsfall-Aufzeichnungen“ einer unabhängigen Stelle vorzulegen. Vielmehr bedarf es der Vorlage sämtlicher Erkenntnisse, die aus der Maßnahme gewonnen wurden. Die (*unabhängige Stelle*) hat sodann zum einen zu prüfen, ob die Maßnahme insgesamt entsprechend den Vorgaben der richterlichen Anordnung durchgeführt wurde. Zum anderen hat sie möglicherweise erfasste Kernbereichsinhalte zu identifizieren und unverzüglich auch selbst zu löschen. Laut BVerfG ist es unbedingt zu vermeiden, dass es – über eine etwaige bei der Erhebung unvermeidbar gewesene Kenntnisnahme von Kernbereichsinhalten durch Verfassungsschutzbedienstete hinaus – zu einer (weiteren) Kenntnisnahme im Zuge der unabhängigen Sichtung kommt (BVerfG a.a.O., Rdnr. 283). Für die Dokumentation der vorgenommenen Löschung gilt §/Art. (*allg. KB-Regelung*) Absatz 2 S. 6.

### **Begründung der Regelung „Vorlage aller Erkenntnisse an unabhängige Stelle“ bei ODS**

#### **§/Art. C Absatz 4:**

Beim heimlichen Zugriff auf informationstechnische Systeme ist der Kernbereichsschutz zu einem großen Teil auf die Auswertungs-/Verwertungsebene verschoben (BVerfG, a.a.O., Rn. 284). Können kernbereichsrelevante Daten in der konkreten Anwendung vor oder bei der Datenerhebung nicht ausgesondert werden (vgl. §/Art. B Absatz 2 S. 1 Nr. 3), ist ein Zugriff auf das informationstechnische System auch dann zulässig, wenn hierbei eine Wahrscheinlichkeit besteht, dass am Rande auch höchstpersönliche Daten miterfasst werden. (BVerfG, a.a.O., Rn. 286).

Dem Schutzbedarf muss durch Sicherungen auf der Aus- und Verwertungsebene Rechnung getragen werden. Zum Zweck unabhängiger Kontrolle sind sämtliche aus der Online-Durchsuchung gewonnenen Daten der (*unabhängigen Stelle*) vorzulegen. Zum Prüfungsumfang der (*unabhängigen Stelle*) gelten die Ausführungen zu Absatz 3 Satz 2 und 3.

Sofern die externe Sichtung an technische und fachliche Grenzen stößt, kann (*die unabhängige Stelle*) Bedienstete (*der Verfassungsschutzbehörde*) zur Gewährleistung ermittlungsspezifischen Sachverstands hinzuziehen. Auch eine technische Unterstützung durch (*die Verfassungsschutzbehörde*) ist möglich. Die Bediensteten dürfen jedoch nur in dem für die Sichtung unvermeidbaren Maße von Kernbereichsdaten Kenntnis erlangen. Über den Inhalt dieser Daten haben sie Stillschweigen zu bewahren (Sätze 4 und 5; vgl. hierzu BVerfG, a.a.O., Rdnr. 315 sowie BVerfG 141, 220, Rdnr. 218 ff und BVerfG 120, 274 (338f)).

### **Hinweise:**

- Ein Querbezug besteht zum Teilprojekt zu institutionellen Anforderungen an unabhängige Kontrolle (Anlage 3) und zum Teilprojekt zu besonderen Vorgaben für die Intensiveingriffe (Anlage 5).
- Zum Kernbereichsschutz bei Wohnraumüberwachungen:  
Hier können bei der im Grundsatz umfassenden Kontrollbefugnis der unabhängigen Stelle zusätzlich für Ausnahmefälle besondere Regeln für eine Gefahr im Verzug vorgesehen werden.