

**Stellungnahme zu dem Beratungsgegenstand  
Erstes Thüringer Entlastungsgesetz  
Gesetzentwurf der Landesregierung  
- Drucksache 8/2487 -**

**dazu**

**Änderungsantrag  
der Fraktionen der CDU, des BSW und der SPD  
- Vorlage 8/1930 -**

**Auf einen Blick**

Der Antrag trägt der veränderten Sicherheitslage Rechnung, und vor diesem Hintergrund ist die Befassung mit der Problematik grundsätzlich begrüßenswert. Allerdings ist er an einigen Stellen zu unbestimmt und aus unserer Sicht etwas weit gefasst. Denn auch mit Blick auf die veränderte Sicherheitslage halten wir Transparenz, insbesondere staatlicher Stellen, für ein hohes Gut, dem bei der jeweiligen Einzelfallabwägung ein entsprechender Stellenwert zuzugestehen ist.

Dennoch sehen wir die Tendenz, dass der Bürokratieabbau bislang vor allem der Entlastung der öffentlichen Hand zu dienen scheint – etwa indem man Berichtspflichten öffentlicher Stellen streicht.

Anders sieht es bei der Privatwirtschaft aus: hier wird die Transparenz in der Regel über den Bürokratieabbau und die Sicherheitsbedenken gestellt. Wir müssen in diesem Zusammenhang darauf hinweisen, dass gerade auch privatwirtschaftlich organisierte Tätigkeit Grundlage für die gesamtgesellschaftliche Resilienz in Kernbereichen ist (z.B. Strom, Wasser, Transport, Nahrung, Gesundheit...).

Wirtschaft und Gesellschaft benötigen Schutz vor Spionage, Sabotage und Cyberangriffen. Schutzbedürftig sind vor allem Informationen über konkrete Schutzmaßnahmen, technische Ausgestaltung, Verwundbarkeiten, Betriebsabläufe, Lagerbestände und Stoffströme, Lieferketten oder Abhängigkeiten. Sie können eine operative Ausnutzung von Schwachstellen ermöglichen, Angriffe erleichtern und daher sicherheitsrelevant und schutzbedürftig sein.

Wir haben bereits in der Vergangenheit darauf hingewiesen, dass Informationen zu Mengenströmen, Lagerkapazitäten, technischen Verfahren, Schutzvorkehrungen und betrieblichen Abhängigkeiten unter Umständen sicherheits- bzw. missbrauchsrelevant sein können<sup>1</sup>. Dies betrifft insbesondere Konstellationen, in denen sich aus Einzelinformationen oder ihrer Zusammenführung Rückschlüsse auf die Verwundbarkeit von Anlagen oder auf die Möglichkeit von Sabotage, Diebstahl, missbräuchlicher Verwendung oder sonstigen Störungen ziehen lassen. Deren ungeschützte Online-Veröffentlichung diente in der Vergangenheit v. a. der Schaffung von Akzeptanz durch Transparenz für Maßnahmen der Energiewende und des Umweltschutzes. Unserer Erfahrung nach waren sie nur wenig von den theoretisch Betroffenen nachgefragt, bergen aber vor allem im Zusammenhang mit ungeschützter Veröffentlichung die o. g. Gefahrenpotentiale durch Dritte.

Angemessener Schutz dient nicht nur der Sicherheitsvorsorge, sondern auch der Entbürokratisierung: Wenn sensible Informationen eindeutig abgegrenzt und rechtssicher geschützt sind, werden aufwendige Einzelfallprüfungen, wiederholte Schwärzungen, Rechtsunsicherheiten und Streitigkeiten über Offenlegungspflichten verringert.

---

<sup>1</sup> So zum Beispiel im damaligen Anhörungsverfahren zum ThürUVPg 2017, in dem wir die weitgehend unbeschränkte digitale Veröffentlichung von Antragsunterlagen thematisiert hatten.

Zugleich benötigen Unternehmen, Investoren, kommunale Träger, Beschäftigte und Öffentlichkeit belastbare Informationen über die Funktionsfähigkeit öffentlicher Infrastruktur. Dazu gehören insbesondere Entscheidungen über Finanzierung, Planung, Vergabe, Betrieb, Kosten, Sanierung, Leistungsfähigkeit und vor allem die Aufsicht. Der Schutz konkret ausnutzbarer Sicherheitsdetails darf nicht zu einer pauschalen Abschirmung von Informationen über öffentliche Finanzierung, Vergabe, Wirtschaftlichkeit, Sanierungsbedarf, Leistungsfähigkeit, Kontrolle und Verantwortlichkeiten führen.

Eine weit gefasste Ausnahme könnte deshalb nicht nur Sicherheitsdetails, sondern auch Informationen über erhebliche Kosten, Mängel, Sanierungsstau, unzureichende Leistungen oder Fehlsteuerungen verdecken.

Die Herausforderung besteht darin, die berechtigten Interessen Sicherheit und Transparenz in Einklang zu bringen. Für den Wirtschaftsstandort Thüringen und die Thüringer Gesellschaft sind sie Voraussetzungen für Vertrauen, Investitionsfähigkeit und resiliente Daseinsvorsorge.

Damit würde der notwendige Schutz präzise auf operative Sicherheitsinformationen konzentriert und die wirtschaftliche sowie demokratische Nachvollziehbarkeit öffentlicher Infrastrukturentscheidungen erhalten.

#### Schlussfolgerungen und abschließende Empfehlung

Wir unterstützen einen zielgenauen und wirksamen Schutz sicherheitsrelevanter Informationen über kritische Infrastruktur, Gefahrenabwehr sowie zivile Verteidigungsstrukturen. Die aktuelle Sicherheitslage rechtfertigt, konkrete Informationen über Schwachstellen, Schutzmaßnahmen, technische Ausgestaltung, Einsatzabläufe oder operative Abhängigkeiten wirksam vor Missbrauch zu schützen.

Der vorliegende Änderungsantrag ist dafür jedoch nachzubessern. Eine pauschal oder zu weit gefasste Herausnahme von Informationen aus dem Anwendungsbereich des Thüringer Transparenzgesetzes darf nicht dazu führen, dass Informationen über Kosten, Vergaben, Verträge, Sanierungsbedarf, Leistungsfähigkeit, Kontrolle und Verantwortlichkeiten kritischer Infrastruktur faktisch der öffentlichen und wirtschaftlichen Nachvollziehbarkeit entzogen werden.

Die Regelung nur sollte daher nur unter folgenden Bedingungen beschlossen werden:

1. Erhebliche, konkret prognostizierte Sicherheitsgefährdung als Voraussetzung des Ausschlusses.
2. Klarstellung, dass ein bloßer KRITIS- oder Sektorbezug nicht genügt.
3. Beschränkung auf konkret ausnutzbare Sicherheitsdetails.
4. Gesetzlicher Vorrang von Schwärzung, Abtrennung, Aggregation und Teilzugang.
5. Abwägung mit einem überwiegenden öffentlichen Interesse bei gravierenden Missständen.
6. Überprüfbare, zugleich sicherheitsgerechte Begründungspflicht.
7. Vollständige Kontrollmöglichkeiten des Landesbeauftragten und der Gerichte.
8. Befristete Evaluation der Vollzugspraxis.

Mit dieser Ausgestaltung kann Thüringen sowohl dem berechtigten Schutzbedürfnis kritischer Infrastruktur als auch den Interessen von Wirtschaft, Öffentlichkeit und rechtsstaatlicher Kontrolle gerecht werden.

## Zu den Fragen des Ausschusses im Einzelnen

### Zur Frage 1 „Begründungszusammenhang“

Der vorliegende Änderungsantrag verfolgt nach seiner Begründung vorrangig ein nachvollziehbares sicherheitspolitisches Ziel, damit ist der unmittelbare Begründungszusammenhang „Bürokratieabbau“ aus unserer Sicht weitgehend entfallen.

Die Regelung ist daher vor allem daran zu messen, ob sie einen wirksamen, verhältnismäßigen und rechtssicheren Ausgleich zwischen Sicherheitsinteressen und Transparenz herstellt. Für den VWT gehört dennoch auch die Frage, ob die Regelung mittelbar neue Verwaltungsaufwände erzeugt, etwa durch Abgrenzungsentscheidungen, Rechtsstreitigkeiten oder eine Zunahme individueller Informationsanträge.

Wir betonen nochmals: eine Wirtschaft, die unter Bürokratie leidet, kann auch keinen Beitrag zur gesamtgesellschaftlichen Resilienz leisten.

### Zur Frage 2 „Aktive Veröffentlichungspflichten“

Proaktive, strukturierte und digital zugängliche Veröffentlichung nicht sensibler Informationen vermeidet wiederholte Einzelanfragen, Rückfragen, Gebührenverfahren und individuelle Prüfungen. Werden Informationen nicht mehr aktiv veröffentlicht, müssen sie häufiger auf Antrag gesucht, rechtlich bewertet, gegebenenfalls geschwärzt und individuell beschieden werden.

Dies belastet sowohl die informationspflichtigen öffentlichen Stellen als auch Unternehmen und Verbände. Aus unserer Sicht ist aktive Veröffentlichung grundsätzlich ein Instrument der Verwaltungsmodernisierung.

Gleichwohl ist darauf zu achten, dass eine weit ausgelegte Sicherheitsausnahme nicht faktisch zu einem Rückgang proaktiver Veröffentlichungen in allen Bereichen führt.

### Zur Frage 3 „Reichweite der Ausnahme“

Der Schutzansatz ist sachlich nachvollziehbar, die Ausnahmen sind jedoch in ihrer derzeitigen Form nicht hinreichend eng und bestimmt. Es besteht die Gefahr eines zu weiten Transparenzausschlusses.

Problematisch sind insbesondere die Formulierungen „Sicherheit, Funktionsfähigkeit oder Resilienz“, „Systeme, Strukturen, Planungen, Verfahren, Abläufe oder Maßnahmen“ sowie die niedrige Eingriffsschwelle, wonach eine Beeinträchtigung lediglich möglich sein muss. Diese Begriffe können neben konkret ausnutzbaren Sicherheitsdetails auch allgemeine Informationen über Verwaltung, Finanzierung, Beschaffung, Betrieb und Kontrolle erfassen.

Erforderlich ist eine Begrenzung auf Informationen, bei denen konkrete tatsächliche Anhaltspunkte dafür bestehen, dass ihre Offenlegung eine erhebliche Beeinträchtigung eines geschützten Sicherheitsinteresses verursachen würde.

### Zur Frage 4 „Bereichsausnahme oder § 12 ThürTG“

eine Herausnahme aus dem Anwendungsbereich des Transparenzgesetzes halten wir grundsätzlich für weniger überzeugend als eine eng gefasste Regelung im bestehenden System der Ablehnungsgründe. Die geltende Systematik des § 12 ThürTG stellt den Informationszugang als Grundsatz voran und erlaubt dessen Einschränkung bei einem konkret darzulegenden Schutzinteresse. Dies stärkt Verhältnismäßigkeit, Teilzugang und Kontrolle.

Der Änderungsantrag verweist allerdings auf ein ernstzunehmendes praktisches Problem: Bei besonders sensiblen Informationen kann bereits eine detaillierte Begründung der Ablehnung Hinweise auf Sicherheitsarchitekturen, Schutzmaßnahmen oder Schwachstellen offenbaren. Dieses Problem rechtfertigt aber nicht ohne Weiteres eine umfassende Bereichsausnahme.

Vorzugswürdig wäre eine eng gefasste Ergänzung des § 12 ThürTG oder eine Sonderregelung, die erstens eine konkrete Gefahrenprognose verlangt, zweitens eine abstrakte, sicherheitsgerechte Begründung zulässt, drittens Teilzugang vorrangig anordnet und viertens die vertrauliche Kontrolle sowie die volle gerichtliche Überprüfbarkeit sicherstellt.

Falls der Gesetzgeber an einer Regelung in § 2 ThürTG festhält, muss diese durch eine strikte Tatbestandsbegrenzung, den Vorrang milderer Mittel und eindeutige Kontrollvorschriften abgesichert werden.

#### Zur Frage 5 „Folgen für Kontrolle“

Eine Herausnahme aus dem Anwendungsbereich kann Begründungspflichten, Teilzugang und Kontrollmöglichkeiten schwächen. Sie birgt insbesondere die Gefahr, dass Behörden eine Anfrage insgesamt als nicht vom Gesetz erfasst behandeln, anstatt den Informationszugang einzelfallbezogen zu prüfen und nur einzelne sicherheitsrelevante Details auszunehmen.

Die Begründung darf keine Informationen preisgeben, deren Schutz gerade bezweckt wird. Sie muss dennoch ausreichen, um eine effektive Rechtskontrolle zu ermöglichen.

#### Zur Frage 6 „Bestehender § 12 ThürTG“

Uns ist kein Fall bekannt, in dem der geltende § 12 ThürTG nachweislich nicht ausgereicht hätte, tatsächlich gefährliche Informationen zurückzuhalten. Es sollte Aufgabe des Gesetzgebers sein, für eine neue Bereichsausnahme konkrete Vollzugsfälle, Schutzlücken oder gerichtliche Entscheidungen zu benennen, aus denen sich ein Regelungsbedarf ergibt.

Denkbar ist eine besondere Problemlage bei Informationen, bei denen bereits die Darlegung der konkreten Gefahr sicherheitsrelevante Rückschlüsse ermöglicht. Dies kann etwa bei hochdetaillierten Lageplänen, konkreten Zugangsdaten, technischen Sicherheitskonfigurationen, tatsächlichen Verwundbarkeiten, Alarmierungs- und Einsatzstrukturen sowie kombinierten Datensätzen über verschiedene Abhängigkeiten und Notfallprozesse der Fall sein.

Eine besonders prüfbedürftige Fallgruppe betrifft private Betreiber und Zulieferer kritischer Leistungen. Beispielsweise können detaillierte Informationen über die technische Auslegung von Energie- oder Wasseranlagen, kritische Transportketten, Lieferabhängigkeiten im Gesundheitswesen oder Lager- und Verarbeitungsprozesse der chemischen Industrie eine missbräuchliche Nutzung erleichtern.

Auch in diesen Konstellationen sollte zunächst geprüft werden, ob die bestehenden Instrumente – insbesondere die Ablehnung nach § 12 ThürTG, Verschlussachen- und Geheimschutzvorschriften, der Schutz von Betriebs- und Geschäftsgeheimnissen sowie Teilzugang durch Schwärzung oder Abtrennung – ausreichen. Eine neue Ausnahme sollte nur für eine konkret belegte verbleibende Schutzlücke geschaffen werden.

#### Zur Frage 8 „Gefahrenschwelle“

Die Schwelle „beeinträchtigen kann“ ist zu niedrig und zu unbestimmt. Sie eröffnet ein weites Ermessen und kann dazu führen, dass bereits abstrakte Risikobefürchtungen den Ausschluss des Informationszugangs rechtfertigen.

Eine konkrete, nachvollziehbare und auf tatsächliche Anhaltspunkte gestützte Gefahrenprognose scheint uns daher zielführender. Es sollte verlangt werden, dass die Offenlegung die Sicherheit, Funktionsfähigkeit oder Resilienz des Schutzguts erheblich beeinträchtigen würde oder dass dies nach den Umständen ernsthaft zu erwarten ist.

#### Zur Frage 9 „Vor- und Nachteile der Zugänglichkeit“

Die Zugänglichkeit von Informationen über Infrastruktur hat erhebliche Vorteile, sofern keine konkret ausnutzbaren Sicherheitsdetails offenbart werden.

Vorteile sind:

1. Nachvollziehbarkeit öffentlicher Investitions-, Vergabe- und Betreiberentscheidungen.
2. Transparenz über Kosten, Gebühren, Fördermittel und wirtschaftliche Auswirkungen.
3. Frühzeitige Sichtbarkeit von Sanierungsbedarf, Kapazitätsengpässen und strukturellen Risiken.
4. Stärkung von Vertrauen in öffentliche Daseinsvorsorge und Infrastrukturbetreiber.
5. Verbesserte Planbarkeit für Unternehmen, Investoren, Kommunen und Beschäftigte.
6. Förderung von Wettbewerb und Korruptionsprävention bei öffentlichen Beschaffungen.

## 7. Möglichkeit öffentlicher und fachlicher Debatte über Resilienz, Prioritäten und Infrastrukturpolitik.

Nachteile entstehen dann, wenn Informationen konkrete Angriffe erleichtern. Dies gilt insbesondere für detaillierte Lage-, Zugangs- und Sicherheitsinformationen, technische Verwundbarkeiten, konkrete Schutzmaßnahmen, Alarmierungs- und Einsatzabläufe oder operative Abhängigkeiten.

Die sachgerechte Konsequenz lautet nicht „Transparenz oder Sicherheit“, sondern eine differenzierte Veröffentlichung: Allgemeine Informationen über Finanzierung, Zustand, Leistung und Steuerung müssen zugänglich bleiben; konkret ausnutzbare Details sind wirksam zu schützen.

### Zur Frage 10 „Angemessenheit der Regelung“

Die Regelung ist in ihrer derzeitigen Fassung zu stark. Sie ist nicht deshalb problematisch, weil sie sicherheitsrelevante Details schützt; dies ist erforderlich. Sie ist problematisch, weil die Begriffe des Schutzbereichs und der Informationen weit gefasst sind, die Eingriffsschwelle niedrig ist und ausdrückliche Sicherungen für Teilzugang, Begründung, Kontrolle und das öffentliche Interesse fehlen.

Eine angemessene Regelung müsste daher:

1. eine erhebliche, konkret begründete Gefährdung verlangen;
2. den Ausschluss auf konkret ausnutzbare Sicherheitsdetails beschränken;
3. klarstellen, dass ein bloßer KRITIS-Bezug nicht ausreicht;
4. Teilzugang verbindlich vorrangig machen;
5. eine überprüfbare, sicherheitsgerechte Begründung verlangen;
6. die vertrauliche Kontrolle durch den Landesbeauftragten und die gerichtliche Überprüfbarkeit absichern;
7. eine Evaluierung der Anwendung vorsehen.

### Zur Frage 11 „Herauslösung einzelner KRITIS-Sektoren“

Eine pauschale Herauslösung ganzer Sektoren ist nicht zwingend erforderlich und wäre wegen der unterschiedlichen tatsächlichen Schutzbedarfe innerhalb jedes Sektors nur begrenzt sachgerecht. Auch innerhalb eines nicht klassisch sicherheitsnahen Sektors können konkret schutzbedürftige Informationen vorkommen; umgekehrt sind in jedem KRITIS-Sektor zahlreiche allgemeine Informationen nicht sicherheitsrelevant.

Entscheidend sollte daher nicht der Sektor, sondern die konkrete Information sein. Der Gesetzgeber sollte allerdings ausdrücklich festlegen, dass bestimmte Kategorien allgemeiner Informationen auch in KRITIS-Sektoren grundsätzlich zugänglich bleiben. Dazu gehören insbesondere Haushalts- und Förderinformationen, Vergaben, allgemeine Betreiberverträge, Gebühren- und Kostenstrukturen, Investitions- und Sanierungsstände, nicht operative Kontrollberichte und allgemeine Leistungsdaten.

Eine sektorübergreifende informationsbezogene Begrenzung ist aus Sicht des VWT rechtssicherer und wirtschaftlich praktikabler als eine sektorweise Herausnahme.

### Zur Frage 12 und 13 „Abwägungsklausel und Sektorbezug“

Eine ausdrückliche Abwägungsklausel schützt nicht nur demokratische Kontrolle, sondern auch die wirtschaftlichen Interessen von Gebührenzahlern, Unternehmen, Investoren und öffentlichen Auftraggebern an einer nachvollziehbaren und leistungsfähigen Daseinsvorsorge.

Die Klausel muss jedoch so ausgestaltet sein, dass sie nicht zur Offenlegung konkret ausnutzbarer Sicherheitsdetails führt. Sie sollte den Zugang zu allgemeinen Informationen, zu aggregierten Daten, zu geschwätzten Unterlagen oder zu nicht sicherheitskritischen Teilen von Prüf- und Kontrollberichten ermöglichen.

Damit würde der notwendige Schutz präzise auf operative Sicherheitsinformationen konzentriert und die wirtschaftliche sowie demokratische Nachvollziehbarkeit öffentlicher Infrastrukturentscheidungen erhalten.

#### Zur Frage 14 „Demokratie und Daseinsvorsorge“

Ja. Diese Gefahr besteht. Infrastrukturen in den Bereichen Energie, Wasser, Verkehr, Gesundheit, IT, Telekommunikation, Abfallwirtschaft und Finanzwesen sind vielfach mit öffentlichen Aufgaben, kommunalen Entscheidungen, Gebühren, Vergaben, Förderungen und Betreiberstrukturen verbunden. Eine weit gefasste Ausnahme könnte deshalb nicht nur Sicherheitsdetails, sondern auch Informationen über erhebliche Kosten, Mängel, Sanierungsstau, unzureichende Leistungen oder Fehlsteuerungen verdecken.

Zur Sicherung von Schutz und Transparenz sind aus Sicht des VWT erforderlich:

1. Ersatz der Schwelle „beeinträchtigen kann“ durch eine erhebliche und konkret begründete Gefährdung.
2. Ausdrückliche Beschränkung auf konkret ausnutzbare Sicherheitsdetails.
3. Klarstellung, dass ein KRITIS- oder Sektorbezug allein nicht genügt.
4. Gesetzlicher Vorrang von Schwärzung, Abtrennung, Aggregation und sonstigem Teilzugang.
5. Sicherung des Zugangs zu Finanzierungs-, Vergabe-, Kosten-, Leistungs- und Kontrollinformationen.
6. Abwägungsklausel für ein überwiegendes öffentliches Interesse.
7. Abstrakte, aber überprüfbare Begründungspflicht.
8. Vertraulicher Informationszugang des Landesbeauftragten und volle gerichtliche Kontrolle.
9. Gesetzliche Evaluation nach spätestens drei Jahren.

#### Zur Frage 15 „Konkrete Änderungen“

Erforderlich sind insbesondere folgende Änderungen:

1. Der Anwendungsbereich muss auf Informationen mit konkret ausnutzbarem Sicherheitsgehalt begrenzt werden.
2. Die Eingriffsschwelle muss eine erhebliche Beeinträchtigung auf Grundlage konkreter tatsächlicher Anhaltspunkte verlangen.
3. Die gesetzliche Regelung muss ausdrücklich klarstellen, dass der bloße Bezug zu einem KRITIS-Sektor oder Betreiber keine Ausnahme begründet.
4. Die aktive Veröffentlichung allgemeiner, nicht sicherheitskritischer Informationen darf unberührt bleiben.
5. Vor einem vollständigen Ausschluss müssen Schwärzung, Abtrennung, Aggregation, Generalisierung und zeitliche Zurückstellung geprüft werden.
6. Die Behörde muss den Ausschluss abstrakt, aber prüffähig begründen.
7. Der Landesbeauftragte für Informationsfreiheit benötigt vertraulichen Zugang zu allen entscheidungserheblichen Unterlagen.
8. Es sollte eine Abwägungsklausel für überwiegende öffentliche Interessen sowie eine Evaluierungs- und Berichtspflicht vorgesehen werden.
9. Die Regelung muss private Unternehmen einbeziehen, soweit diese kritische Leistungen für die Daseinsvorsorge oder im Krisen-, Katastrophen-, Spannungs- beziehungsweise Verteidigungsfall erbringen. Schutzbedürftig sind jedoch nur konkret ausnutzbare Sicherheitsinformationen. Dies gilt beispielsweise für Details zu Energie- und Wasseranlagen, kritischen Logistik- und Lieferketten, Gesundheitseinrichtungen sowie für Angaben zu Mengen, Lagerung, Verarbeitung und Transport sicherheitsrelevanter Stoffe in chemischen Betrieben.

Diese Elemente ermöglichen die proaktive Veröffentlichung allgemeiner Informationen und bewahren den Informationszugang auf Antrag, ohne operative Sicherheitsinteressen zu gefährden.

#### Zur Frage 16 „Definition sicherheitsrelevanter Informationen“

Die vorgesehene Definition reicht nicht aus, um eine überdehnte Anwendung zuverlässig zu verhindern. Die Begriffe „Systeme, Strukturen, Planungen, Verfahren, Abläufe oder Maßnahmen“ sind in ihrer Allgemeinheit sehr weit und können nahezu sämtliche Verwaltungs- und Betriebsinformationen in den genannten Bereichen erfassen.

Für den Schutz konkret sensibler Informationen sind diese Begriffe zwar relevant, etwa bei Einsatzplänen, Alarmierungswegen, Lagebildern, Leitstellenstrukturen, technischen Sicherheitskonfigurationen oder konkreten Wiederanlaufprozessen. Ohne weitere Begrenzung können sie aber auch Haushaltsplanungen, organisatorische Zuständigkeiten, allgemeine Beschaffungsabläufe, nicht operative Konzepte oder gewöhnliche Verträge erfassen.

Der Gesetzestext sollte deshalb beispielhaft und abschließend klarstellen, dass sicherheitsrelevante Informationen nur solche Informationen sind, die konkrete Rückschlüsse auf ausnutzbare Schwachstellen, Schutzmaßnahmen, Lage- und Zugangsdaten, technische Sicherheitsarchitekturen, Einsatz- und Alarmierungsstrukturen oder operative Abhängigkeiten zulassen. Außerdem sollte ein unmittelbarer und erheblicher Bezug zur möglichen Sicherheitsbeeinträchtigung verlangt werden.

#### Zur Frage 17 „Teilzugang“

Es sollte eine ausdrückliche Teilzugangspflicht geschaffen werden. Diese sollte den vollständigen Ausschluss als letztes Mittel ausweisen.

Die Behörde sollte dokumentieren müssen, welche Teilzugangsoptionen geprüft und weshalb sie gegebenenfalls verworfen wurden. Dies stärkt die Kontrolle durch den Landesbeauftragten und die Gerichte. Es verbessert zugleich die Akzeptanz der Entscheidung bei Unternehmen, Antragstellern und Öffentlichkeit.

#### Zur Frage 18 „Schutz durch Resilienzmaßnahmen“

Der wirksamste Schutz kritischer Infrastruktur entsteht vorrangig durch konkrete Schutz- und Resilienzmaßnahmen an den Anlagen und in den Betriebsprozessen. Informationsschutz ist ein notwendiger Baustein, kann aber technische, organisatorische und personelle Schutzmaßnahmen nicht ersetzen.

Dies gilt gleichermaßen für staatliche, kommunale und private Betreiber. In Thüringen werden zahlreiche kritische Leistungen durch Unternehmen erbracht, insbesondere in den Bereichen Energie, Wasser, Ernährung, Transport und Verkehr sowie Gesundheit. Die Resilienz dieser Unternehmen ist ein Bestandteil der öffentlichen Sicherheitsvorsorge und zugleich ein Standortfaktor.

Für chemische Betriebe bedeutet dies unter anderem: Sicherheitsrelevante Stoffe, Lagerkapazitäten und Verarbeitungsprozesse müssen durch angemessene technische, organisatorische und personelle Maßnahmen geschützt werden. Transparenzrechtlich müssen konkrete Angaben, die eine missbräuchliche Nutzung, Sabotage oder gezielte Störung erleichtern könnten, geschützt bleiben. Dies ersetzt jedoch nicht die Notwendigkeit, konkrete Risiken durch Anlagensicherheit, Zugangsschutz, Sicherheitsmanagement, Notfallkonzepte und belastbare Lieferketten tatsächlich zu reduzieren.

Aus Sicht des VWT gehören zu einer wirksamen Resilienzstrategie insbesondere:

1. Redundanzen und Ersatzkapazitäten in Versorgung, Kommunikation und Logistik.
2. Notstromversorgung, Notfalllager und belastbare Wiederanlaufkonzepte.
3. Physische Sicherung besonders schutzbedürftiger Anlagen.
4. Cybersicherheitsmaßnahmen, segmentierte Systeme und sichere Kommunikationswege.
5. Regelmäßige Risiko- und Schwachstellenanalysen.
6. Krisenübungen, qualifiziertes Personal und klare Meldewege.
7. Belastbare Lieferketten und alternative Bezugsquellen.
8. Abgestimmte Zusammenarbeit von Betreibern, Kommunen, Sicherheitsbehörden und Aufsicht.

9. Gezielte Investitionen zur Beseitigung tatsächlich festgestellter Schwachstellen. Eine weitreichende Herausnahme von Informationen kann Angriffe nicht verhindern, wenn Anlagen und Systeme tatsächlich unzureichend geschützt sind. Sie kann zudem die öffentliche und fachliche Kontrolle über Investitionsbedarf, Sanierungsstau, Fehlsteuerungen und mangelnde Resilienz erschweren.

Wir befürworten deshalb einen zielgenauen Informationsschutz für konkret ausnutzbare Sicherheitsdetails, verbunden mit einer konsequenten Stärkung der tatsächlichen Resilienz kritischer Infrastrukturen.

Erfurt, 31.08.2026

Johannes Bräun  
Leiter Wirtschafts- und Umweltpolitik