

16.12.2025

# Änderungsantrag

der Fraktion der FDP

zu dem „**Gesetz zur Stärkung der Informationssicherheit des Landes Nordrhein-Westfalen (Informationssicherheitsgesetz Nordrhein-Westfalen – InfoSiG NRW)**“

Gesetzentwurf der Landesregierung

Drucksache 18/14581

Beschlussempfehlung des Ausschusses für Bauen, Wohnen und Digitalisierung

Drucksache 18/14943

1. In der Inhaltsübersicht wird die Angabe zu § 1 wie folgt gefasst:

„§ 1 Zweck des Gesetzes; Belastungsausgleich“

2. § 1 wird wie folgt geändert:

a) Die Überschrift wird wie folgt gefasst:

**„§ 1  
Zweck des Gesetzes; Belastungsausgleich“**

b) Nach den Wörtern „Landesverwaltung Nordrhein-Westfalen“ werden die Wörter „und der kommunalen Verwaltung“ eingefügt.

c) Folgender Satz 2 wird angefügt:

„Der Belastungsausgleich für die den Gemeinden und Gemeindeverbänden entstehenden notwendigen, durchschnittlichen Aufwendungen ist in einem Belastungsausgleichsgesetz zu diesem Gesetz geregelt.“

3. § 2 Absatz 1 wird wie folgt geändert:

a) In Nummer 4 wird der Punkt am Ende durch ein Komma ersetzt.

b) Folgende Nummer 5 wird angefügt:

„5. Gemeinde und Gemeindeverbände.“

4. § 3 wird wie folgt geändert:
- a) In Nummer 3 werden die Wörter „, die Nutzerinnen und Nutzer dieser Systeme und andere Personen schädigen,“ gestrichen.
  - b) Nummer 4 wird wie folgt gefasst:  
„4. eine erhebliche Cyberbedrohung eine Cyberbedrohung, die das Potenzial besitzt, die Netz- und Informationssysteme einer Behörde oder der Nutzerinnen und Nutzer solcher Systeme entweder aufgrund ihrer technischen Merkmale erheblich zu beeinträchtigen oder einen erheblichen materiellen oder immateriellen Schaden zu verursachen“
  - c) In Nummer 9 wird der Punkt am Ende durch ein Komma ersetzt.
  - d) Folgende Nummer 10 wird angefügt:  
„10. Sabotage eine vorsätzliche Handlung, die darauf abzielt, die Funktionsfähigkeit von Netzwerk- und Informationssystemen, deren Komponenten oder den darauf beruhenden Dienste zu stören, zu beschädigen oder zu zerstören, um deren Verfügbarkeit, Integrität oder Vertraulichkeit zu beeinträchtigen.“
5. § 4 Absatz 3 wird wie folgt gefasst:
- „(3) Die Landesregierung legt die nähere Ausgestaltung der Informationssicherheit in der Landesverwaltung in einer Verwaltungsvorschrift fest. Die Verwaltungsvorschrift wird dem Landtag zur Kenntnis gegeben.“
6. § 6 Absatz 2 wird wie folgt geändert:
- a) In Satz 1 wird das Wort „insbesondere“ gestrichen.
  - b) Nach Satz 2 wird folgender Satz 3 angefügt:  
„Die durch das CSIRT erhobenen Informationen dürfen ausschließlich zu Zwecken der Informationssicherheit verarbeitet werden und unterliegen einem besonderen Schutz der Vertraulichkeit.“
7. § 8 Absatz 1 wird wie folgt geändert:
- a) Nach Satz 1 wird folgender Satz eingefügt:  
„Die Maßnahmen nach Satz 1 umfassen auch Vorkehrungen zur Aufrechterhaltung wesentlicher Verwaltungsfunktionen im Not- und Krisenfall (Business-Continuity-Management).“
  - b) Nach dem neuen Satz 3 wird folgender Satz angefügt:  
„Dienste und Technologien, die nur dem Rechtsrahmen der Europäischen Union unterworfen sind, sind zu bevorzugen.“

8. Nach § 9 Absatz 6 wird folgender Absatz 7 angefügt:  
  
„(7) Für die Meldung von Schwachstellen, Beinahe-Vorfällen, Cyberbedrohungen, Sicherheitsvorfällen und Sabotage innerhalb der Landesverwaltung gelten die Absätze 1 bis 6 entsprechend.“
9. In § 11 wird das Wort „kann“ durch „spricht“ und das Wort „aussprechen“ durch „aus“ ersetzt.
10. § 19 wird wie folgt neu gefasst:  
  
„Dieses Gesetz tritt vorbehaltlich § 2 Absatz 1 Nummer 5 am Tag nach der Verkündung in Kraft. § 2 Absatz 1 Nummer 5 tritt am 1. Juli 2026 in Kraft.“

## **Begründung**

### **Allgemeiner Teil**

Die IT-Sicherheit von Landesbehörden und Kommunen ist entscheidend als Fundament unserer staatlichen Ordnung. Das haben Cyberangriffe der jüngsten Vergangenheit eindrücklich bewiesen: Die Attacke auf die Südwestfalen-IT im November 2023 legte beispielsweise die IT-Infrastruktur von rund 70 Kommunen nahezu vollständig lahm samt zentraler Verwaltungsprozesse. Die massive Störung führte zu erheblichen wirtschaftlichen Schäden und hat das Vertrauen der Bürgerinnen und Bürger in den Staat erschüttert.

Die EU verfolgt mit der NIS-2-Richtlinie das Ziel, die IT-Sicherheit staatlicher Stellen europaweit zu erhöhen und verpflichtet die Mitgliedstaaten zur Einführung verbindlicher Sicherheitsstandards. Obwohl Nordrhein-Westfalen die Richtlinie bis Oktober 2024 hätte umgesetzt müssen, hat die Landesregierung den vorliegenden Gesetzesentwurf erst weit nach der Frist vorgelegt. Dieses Zögern birgt juristische Risiken für den deutschen Gesamtstaat, da die EU bei fehlender Umsetzung ein Vertragsverletzungsverfahren gegen Deutschland einleiten kann. In einer Anhörung im Ausschuss für Bauen, Wohnen und Digitalisierung vom 30. Oktober 2025 zum InfoSiG wurde deutlich, dass die EU-Kommission bereits den Umsetzungsstand abgefragt hat und eine Klage vor dem Europäischen Gerichtshof drohen könnte. Sachverständige warnten vor möglichen Strafzahlungen, deren Höhe sich an den enormen Schäden durch Cyberangriffe bemisst; allein 178,6 Mrd. Euro im vergangenen Jahr laut dem Branchenverband Bitkom.

In derselben Anhörung vom 30. Oktober 2025 haben Sachverständige deutlichen Änderungsbedarf am Gesetzesentwurf der Landesregierung angemeldet. Insbesondere wurde mehrfach bemängelt, dass die Kommunen vom Regelungsumfang ausgenommen sein sollen. Dabei sind sie als zentrale Akteure für die IT-Sicherheit des Staates von tragender Bedeutung. Deswegen müssen auch Städte und Gemeinden in das InfoSiG einbezogen werden. Die dadurch ausgelösten Konnexitätsfolgekosten muss das Land tragen. Ein unabhängiges Gutachten muss die Folgekosten bestimmen.

Ein weiterer Aspekt aus der Anhörung umfasst die Frage nach der digitalpolitischen Souveränität der Landesverwaltung. Mit dem InfoSiG soll das Digitalministerium für die Landesverwaltung Vorgaben machen können zu den in der Landesverwaltung genutzten Technologien. Das ist im Sinne einer Vereinheitlichung und Harmonisierung zu begrüßen. Sachverständige haben

in der Anhörung vorgeschlagen, innerhalb dieses Rahmens solche Technologien zu bevorzugen, die ausschließlich dem europäischen Recht unterliegen. Auf diese Weise kann Nordrhein-Westfalen an Unabhängigkeit von Unternehmen gewinnen, die auch der nationalen Regulierung außereuropäischer Staaten unterliegen. Dieser Vorschlag wird mit dem vorliegenden Änderungsantrag umgesetzt.

Schließlich schafft der Änderungsantrag Klarheit bei den Meldekettten. Laut dem Entwurf der Landesregierung sind nur erhebliche Sicherheitsvorfälle der zentralen Stelle zu melden. Die Anhörung hat ergeben, dass diese Meldepflicht auch auf Vorfälle unterhalb der Erheblichkeitsschwelle ausgeweitet werden soll. Zudem wird in dem Änderungsantrag erstmals „Sabotage“ als ein gesonderter sicherheitsrelevanter Vorfall normiert. Weiterhin stellt der Änderungsantrag verschiedene datenschutzrelevante Sachverhalte klar, so wie sie die Landesdatenschutzbeauftragte vorgetragen hat.

### **Besonderer Teil**

Zu Nr. 1:

Es handelt sich um eine redaktionelle Folgeänderung zu Nr. 2a und 2c.

Zu Nr. 2 und 3

Mit diesen Änderungen wird das Informationssicherheitsgesetz auf Gemeinden und Gemeindeverbände ausgeweitet.

Nach Art. 2 Abs. 5 NIS-2-RL können die Mitgliedstaaten der EU vorsehen, dass die Richtlinie auf Einrichtungen der öffentlichen Verwaltung auf lokaler Ebene Anwendung findet. Die Erreichung des Anwendungsbereichs auch auf Gemeinden und Gemeindeverbände ist für eine funktionierende gesamtstaatliche Struktur von wesentlicher Bedeutung. Auch hier existieren kritische Infrastrukturen, die besonders zu schützen sind, wie z.B. im Bereich der zivilen Verteidigung oder der Versorgung. Zudem hüten die Städte und Gemeinden im Rahmen ihrer Registerhoheit wertvolle Datensätze über die Bürgerinnen und Bürger, Betriebe und staatliche Informationen, die für Cyberangriffe eine lohnende Beute darstellen.

Ein notwendiger Einbezug der Gemeinden und Gemeindeverbände ergibt sich auch aus der Logik des föderalen Aufbaus von Nordrhein-Westfalen. Nach § 2 Abs. 1 Nr. 1 InfoSiG gilt das Gesetz für die Landesbehörden im Sinne des § 2 Landesorganisationsgesetz. Hierzu zählen auch die unteren Landesbehörden. Nach § 9 Landesorganisationsgesetz gehören dazu auch die Landrätinnen und Landräte in ihrer Funktion als untere staatliche Verwaltungsbehörden.

Da die Ausweitung des InfoSiG auf die Kommunen eine Veränderung bestehender Aufgaben darstellt, löst das Vorhaben gemäß § 1 Abs. 1 KonnexAG zwingend Kostenfolgen aus. In der Praxis wird sich dies zeigen, insbesondere durch neue Personalaufwände sowie den Betrieb zusätzlicher Sicherheitsinfrastrukturen. Hinzu kommen materielle Aufwendungen für Hard- und Software sowie laufende Kosten für Pflege, Support und Abnutzung, die nach § 3 Abs. 3 KonnexAG im Rahmen einer Kostenfolgeabschätzung systematisch zu erfassen sind. Satz 2 bestimmt, dass der Belastungsausgleich gemäß § 6 Satz 3 KonnexAG in einem gesonderten Belastungsausgleichsgesetz geregelt wird.

Zu Nr. 4:

Die Definition von Cyberbedrohungen beschränkt sich bisher auf Vorfälle in IT-Systemen, die Personen schädigen könnten. Mit dem Änderungsantrag wird präzisiert, dass auch mögliche Sachschäden als konstituierende Folge einbezogen werden, die keine oder nur mittelbare Schädigung von Personen verursachen können.

Mit dem Änderungsantrag wird zudem ein Konstruktionsfehler bei der Erheblichkeit von Cyberbedrohungen gelöst. Bisher sieht die Definition eine doppelte Vorbedingung vor, nämlich Lahmlegen der IT und Schadensfolge zusammen. Hier muss es jedoch genügen, dass eine der beiden Bedingungen vorliegen. Damit werden auch Angriffe unter den Erheblichkeit-Begriff gefasst, die zwar nur eine geringfügige IT-Beeinträchtigungen auslösen, aber erhebliche Schäden bewirken, und umgekehrt.

Zudem wird der Fall der Sabotage als neuer gesonderter sicherheitsrelevanter Vorfall normiert, als eine vorsätzliche Handlung, die darauf abzielt, die Funktionsfähigkeit von Netzwerk- und Informationssystemen, deren Komponenten oder den darauf beruhenden Dienste zu stören, zu beschädigen oder zu zerstören, um deren Verfügbarkeit, Integrität oder Vertraulichkeit zu beeinträchtigen.

Zu Nr. 5:

Die Änderung legt fest, dass die Landesregierung verpflichtet ist, eine ausführende Verwaltungsvorschrift zu erarbeiten. Die bisherige Kann-Vorschrift wird ersetzt.

Zu Nr. 6:

Die Streichung des Wortes „insbesondere“ dient der Klarstellung, dass die im Entwurf vorgesehenen Befugnisse zur Datenverarbeitung eindeutig und abschließend an die Aufgaben gebunden sind, die dem CSIRT gesetzlich im Rahmen des InfoSiG übertragen werden. Der Begriff hätte eine unbestimmte Erweiterung der Befugnisse nahegelegt und damit den Eindruck erweckt, dass Datenverarbeitung auch für außerhalb des gesetzlichen Aufgabenkreises liegende Tätigkeiten zulässig wäre. Durch die sprachliche Präzisierung wird sichergestellt, dass zusätzliche Aufgaben, die dem CSIRT gegebenenfalls lediglich durch Verwaltungsvorschriften übertragen werden, keine Datenverarbeitungsbefugnis ohne ausdrückliche gesetzliche Grundlage auslösen.

Zudem erfolgt eine Klarstellung über die Schutzdimension der gewonnenen Daten. Denn § 6 listet umfassende Überwachungs-, Analyse- und Forensikbefugnisse auf, enthält jedoch keine ausreichende Regelung zur Zweckbindung oder Vertraulichkeit der hierbei gewonnenen Daten. Angesichts dieser weitreichenden Informationsflüsse wird zur Wahrung von Vertrauensschutz, Meldebereitschaft und Rechtsklarheit ausdrücklich klargestellt, dass die durch das CSIRT erhobenen und weitergegebenen Informationen ausschließlich zu Zwecken der Informationssicherheit verwendet werden dürfen.

Zu Nr. 7:

§ 8 regelt das Risikomanagement, enthält bisher jedoch keine Pflicht zur Aufrechterhaltung eines Notbetriebs (Business Continuity Managements). § 8 Abs. 2 Nr. 3 regelt lediglich die technische Aufrechterhaltung des IT-Betriebs im Rahmen eines Backup-Managements, der Wiederherstellung und des Krisenmanagements. Die hier gemachten Änderungen normieren zusätzlich die Verpflichtung zur Aufrechterhaltung wesentlicher Verwaltungsfunktionen im Sinne eines „Business Continuity Managements“, darunter fallen Notbetrieb, Ersatzverfahren und die Priorisierung staatlicher Aufgaben.

Der Änderungsantrag führt weiterhin ein, dass bei der Festsetzung und Empfehlung von Technologien innerhalb der Landesverwaltung solche Anbieter bevorzugt werden, die ausschließlich dem europäischen Rechtsrahmen unterliegen. Auf diese Weise stärkt die Landesverwaltung ihre digitalpolitische Autonomie. Besonders europäische Anbieter von Open-Source-Software bieten eine hinlängliche Alternative zu außereuropäischen Technologien mit höchstem Nutzungsniveau und IT-Sicherheitsstandards.

Zu Nr. 8:

Innerhalb der Landesverwaltung wird die Meldekette für wichtige Behörden um Schwachstellen, Beinahe-Vorfällen, Cyberbedrohungen, Sicherheitsvorfällen und Sabotage erweitert. Informativ wird hier klargestellt, dass Meldungen ausschließlich zur Verbesserung der Informationssicherheit verwendet werden dürfen und eine Weitergabe zur Ausnutzung gemeldeter Sicherheitslücken durch Polizeien oder deutsche Nachrichtendienste nicht stattfindet.

Zu Nr. 9:

Die Änderung legt fest, dass die Landesregierung verpflichtet ist für die Anwendungen technischer Spezifikationen Empfehlungen auszusprechen. Die bisherige Kann-Vorschrift wird ersetzt.

Zu Nr. 10:

Um sicherzustellen, dass die Belastungsausgleichsregelung für die Gemeinden und Gemeindeverbände nach § 1 Satz 2 in unmittelbarem zeitlichen Zusammenhang mit der Aufgabenübertragung steht (vgl. VerfGH NRW, Urteil vom 10.01.2017 – VerfGH 8/15 -, NVwZ 2017, 780 (781) Rn. 33), wird die Geltung des Gesetzes für die Gemeinden und Gemeindeverbände auf den 1. Juli 2026 hinausgeschoben. Dies ermöglicht ein gleichzeitiges Inkrafttreten von Aufgabenübertragung und Belastungsausgleichsregelung.

Henning Höne  
Marcel Hafke  
Angela Freimuth  
Dirk Wedel

und Fraktion