



Gesetz- und Verordnungsblatt für das Land Nordrhein-Westfalen

Ausgabe: [GV. NRW. 2026 Nr. 1](#)
Veröffentlichungsdatum: 15.01.2026
Seite: 6

Gesetz zur Stärkung der Informationssicherheit des Landes Nordrhein-Westfalen (Informationssicherheitsgesetz Nordrhein-Westfalen – InfoSiG NRW)

Der Landtag hat das folgende Gesetz beschlossen, das hiermit verkündet wird:

Gesetz zur Stärkung der Informationssicherheit des Landes Nordrhein-Westfalen (Informationssicherheitsgesetz Nordrhein-Westfalen – InfoSiG NRW)

Vom 18. Dezember 2025

Inhaltsübersicht

Abschnitt 1 Allgemeine Vorschriften

- § 1 Zweck des Gesetzes
- § 2 Geltungsbereich
- § 3 Begriffsbestimmungen

Abschnitt 2 Organisation

- § 4 Informationssicherheit in der Landesverwaltung
- § 5 Zuständige Behörde im Sinne der NIS-2-Richtlinie
- § 6 [Computer-Notfallteam \(CSIRT\)](#)

Abschnitt 3 Maßnahmen, Informations- und Dokumentationspflichten

- § 7 Identifizierung und Registrierung
- § 8 [Risikomanagementmaßnahmen](#)
- § 9 [Berichtspflichten](#)
- § 10 [Freiwillige Meldung von relevanten Informationen](#)
- § 11 Empfehlungen für den Nachweis über Risikomanagementmaßnahmen sowie die Anwendung technischer Spezifikationen
- § 12 Aufsichts- und Durchsetzungsmaßnahmen gegenüber wichtigen Behörden
- § 13 [Zusammenarbeit mit anderen Behörden](#)

Abschnitt 4 Abwehr von Gefahren für die Informationstechnik, Datenerhebung und -auswertung

- § 14 [Abwehr von Gefahren für die Informationstechnik](#)
- § 15 Datenerhebung und -auswertung zur Abwehr von Gefahren für die Informationstechnik

Abschnitt 5 Datenschutz

- § 16 [Datenverarbeitung](#)
- § 17 [Datenübermittlung](#)

Abschnitt 6

Schlussvorschriften

§ 18 [Einschränkung von Grundrechten](#)

§ 19 Inkrafttreten

Abschnitt 1

Allgemeine Vorschriften

§ 1

Zweck des Gesetzes

Zweck dieses Gesetzes ist, die Netz- und Informationssicherheit in der Landesverwaltung Nordrhein-Westfalen zu erhöhen, Gefahren für informationstechnische Systeme abzuwehren und die Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (ABl. L 333 vom 27.12.2022, S. 80; L, 2023/90206, 22.12.2023), im Folgenden NIS-2-Richtlinie, umzusetzen, soweit hierfür die Zuständigkeit im Land Nordrhein-Westfalen liegt.

§ 2

Geltungsbereich

(1) Dieses Gesetz gilt für

1. Landesbehörden im Sinne des § 2 des Landesorganisationsgesetzes vom 10. Juli 1962 ([GV. NRW. S. 421](#)) in der jeweils geltenden Fassung,
2. Einrichtungen des Landes im Sinne des § 14 des Landesorganisationsgesetzes, soweit diese an das Landesverwaltungsnetz angeschlossen sind,
3. den Landtag Nordrhein-Westfalen, unabhängig von einer Anbindung an das Landesverwaltungsnetz,
4. Landesbetriebe im Sinne des § 14a des Landesorganisationsgesetzes und

5. Organe der Rechtspflege im Sinne des § 1 Absatz 2 Buchstabe c des Landesorganisationsgesetzes (Behörden).

(2) Der Landtag gewährleistet die ihn betreffende Informationssicherheit durch den Beschluss einer für ihn, seine Gremien, seine Mitglieder und deren Beschäftigte, seine Fraktionen und deren Beschäftigte sowie für die Landtagsverwaltung geltenden Informationssicherheitsleitlinie. Die §§ 4 bis 18 dieses Gesetzes gelten nach Maßgabe der Informationssicherheitsleitlinie.

(3) Dieses Gesetz gilt nicht für Behörden, soweit diese in den Bereichen nationale Sicherheit, öffentliche Sicherheit, Verteidigung oder Strafverfolgung, einschließlich der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten, tätig werden.

(4) Die in diesem Gesetz festgelegten Verpflichtungen umfassen nicht die Bereitstellung von Informationen, deren Offenlegung wesentlichen Interessen der Mitgliedstaaten im Bereich der nationalen Sicherheit, der öffentlichen Sicherheit oder der Verteidigung zuwiderlaufen würde.

§ 3

Begriffsbestimmungen

Im Sinne dieses Gesetzes ist:

1. eine wichtige Behörde eine Behörde, die die Voraussetzungen des Artikel 3 Absatz 2 der NIS-2-Richtlinie erfüllt,
2. ein Beinahe-Vorfall ein Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über Netz- und Informationssysteme angeboten werden oder zugänglich sind, beeinträchtigt haben könnte, dessen Eintritt jedoch erfolgreich verhindert wurde oder das nicht eingetreten ist,
3. eine Cyberbedrohung ein möglicher Umstand, ein mögliches Ereignis oder eine mögliche Handlung, die informationstechnische Systeme, Komponenten und Prozesse, die Nutzerinnen und Nutzer dieser Systeme und andere Personen schädigen, stören oder anderweitig beeinträchtigen könnte,
4. eine erhebliche Cyberbedrohung eine Cyberbedrohung, die das Potenzial besitzt, die Netz- und Informationssysteme einer Behörde oder der Nutzerinnen und Nutzer solcher Systeme aufgrund ihrer technischen Merkmale erheblich zu beeinträchtigen, indem sie erheblichen materiellen oder immateriellen Schaden verursacht,
5. ein Dienst jeder Vorgang innerhalb einer Behörde, durch den öffentliche Aufgaben wie zum Beispiel Verwaltungsakte, Datenbereitstellung, Vollzug von Meldepflichten sowie verwaltungsinterne Dienstleistungen erfüllt werden,
6. ein Netz- und Informationssystem:

- a) ein Übertragungssystem, ungeachtet dessen, ob es auf einer permanenten Infrastruktur oder zentralen Verwaltungskapazität basiert, und gegebenenfalls eine Vermittlungs- und Leitweeinrichtung sowie anderweitige Ressourcen, einschließlich der nicht aktiven Netzbestandteile, die die Übertragung von Signalen über Kabel, Funk, optische oder andere elektromagnetische Einrichtungen ermöglichen, einschließlich Satellitennetze, feste (leitungs- und paketvermittelt, einschließlich Internet) und mobile Netze, Stromleitungssysteme, soweit sie zur Signalübertragung genutzt werden, Netze für Hör- und Fernsehfunk sowie Kabelfernsehnetze, unabhängig von der Art der übertragenen Informationen,
 - b) ein Gerät oder eine Gruppe miteinander verbundener oder zusammenhängender Geräte, die einzeln oder zu mehreren auf der Grundlage eines Programms die automatische Verarbeitung digitaler Daten durchführen, oder
 - c) digitale Daten, die von den in den Buchstaben a und b genannten Elementen zum Zwecke ihres Betriebs, ihrer Nutzung, ihres Schutzes und ihrer Pflege gespeichert, verarbeitet, abgerufen oder übertragen werden,
7. eine Schwachstelle eine Schwäche, Anfälligkeit oder Fehlfunktion von Produkten oder Diensten im Bereich der Informations- und Kommunikationstechnologien, die bei einer Cyberbedrohung ausgenutzt werden kann,
8. ein Sicherheitsvorfall ein Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über Netz- und Informationssysteme angeboten werden oder zugänglich sind, beeinträchtigt und
9. ein erheblicher Sicherheitsvorfall ein solcher, wenn
- a) er schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die Behörde verursacht hat oder verursachen kann,
 - b) er andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann oder
 - c) er im Sinne eines von der Europäischen Kommission erlassenen Durchführungsrechtsaktes als solcher anzusehen ist.

Abschnitt 2 Organisation

§ 4 Informationssicherheit in der Landesverwaltung

(1) Das für Digitalisierung zuständige Ministerium hat

1. Gefahren für die Sicherheit der Informationstechnik an den Schnittstellen zwischen Landesverwaltungsnetz und anderen Netzen abzuwehren,
 2. die an das Landesverwaltungsnetz angeschlossenen Behörden bei der Abwehr von Gefahren für die Sicherheit in der Informationstechnik zu unterstützen und
 3. alle für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik, die Erkennung von Sicherheitsrisiken und die Bewertung von Sicherheitsvorkehrungen erforderlichen Informationen zu sammeln und auszuwerten sowie die an das Landesverwaltungsnetz angeschlossenen Behörden unverzüglich über die sie betreffenden Informationen zu unterrichten.
- (2) Es kann sich zur Erfüllung seiner Aufgaben des Landesbetriebes Information und Technik Nordrhein-Westfalen, im Folgenden IT. NRW, oder anderer geeigneter Dritter bedienen.
- (3) Die Landesregierung kann die nähere Ausgestaltung der Informationssicherheit in der Landesverwaltung in einer Verwaltungsvorschrift festlegen. Die Verwaltungsvorschrift wird dem Landtag zur Kenntnis gegeben.

§ 5

Zuständige Behörde im Sinne der NIS-2-Richtlinie

- (1) Im für Digitalisierung zuständigen Ministerium wird eine zuständige Stelle als zuständige Behörde im Sinne des Artikel 8 Absatz 1 der NIS-2-Richtlinie eingerichtet. Sie überwacht die Anwendung dieses Gesetzes, sofern es die Anforderungen der NIS-2-Richtlinie auf Ebene des Landes Nordrhein-Westfalen umsetzt. Sie ist in der Erfüllung ihrer Aufgaben operativ unabhängig und weisungsfrei. Sie hat ein direktes Vortragsrecht in der IT-Steuerungsgruppe.
- (2) Die zuständige Behörde meldet der nationalen zentralen Anlaufstelle die wichtigen Behörden.
- (3) Zur Unterstützung der Risikomanagementmaßnahmen nach § 8 soll sie Muster oder zentrale Leistungen im Bereich der Informations- und Kommunikationstechnologien zur Verfügung stellen.
- (4) Die zuständige Behörde übermittelt dem zuständigen Bundesministerium insbesondere
1. ihre Identität und Aufgabe als zuständige Behörde und
 2. die Identität und die Aufgaben des CSIRT nach § 6.
- (5) Sie kann sich zur Erfüllung der Aufgaben geeigneter Dritter bedienen. Diese Dritten sind bei der Erfüllung der Aufgaben operativ unabhängig und ausschließlich an die Weisungen der zuständigen Stelle gebunden.

§ 6

Computer-Notfallteam (CSIRT)

(1) Das Computer-Notfallteam, im Folgenden CSIRT, nach Artikel 10 Absatz 1 der NIS-2-Richtlinie für das Land Nordrhein-Westfalen wird beim für Digitalisierung zuständigen Ministerium eingerichtet. Es kann sich zur Erfüllung seiner Aufgaben IT. NRW oder anderer geeigneter Dritter bedienen.

(2) Das CSIRT hat insbesondere folgende Aufgaben:

1. Überwachung und Analyse von Cyberbedrohungen, Schwachstellen und Sicherheitsvorfällen auf Landesebene und auf Anfrage Bereitstellung von Unterstützung für wichtige Behörden hinsichtlich der Überwachung ihrer Netz- und Informationssysteme in Echtzeit oder nahezu in Echtzeit,
2. Ausgabe von Frühwarnungen und Alarmmeldungen sowie Bekanntmachung und Weitergabe von Informationen über Cyberbedrohungen, Schwachstellen und Sicherheitsvorfälle an die wichtigen Behörden sowie an die zuständige Stelle und andere einschlägige Interessenträger, möglichst echtzeitnah,
3. Reaktion auf Sicherheitsvorfälle und gegebenenfalls Unterstützung der wichtigen Behörden,
4. Erhebung und Analyse forensischer Daten sowie dynamische Analyse von Risiken und Sicherheitsvorfällen sowie Lagebeurteilung im Hinblick auf die Netz- und Informationssicherheit,
5. auf Ersuchen einer wichtigen Behörde eine proaktive Überprüfung der informationstechnischen Systeme, Komponenten und Prozesse der wichtigen Behörde auf Schwachstellen mit potenziell signifikanten Auswirkungen (Schwachstellenscan),
6. Beteiligung am CSIRTs-Netzwerk und im Rahmen seiner Kapazitäten und Kompetenzen auf Gegenseitigkeit beruhende Unterstützung anderer Mitglieder des CSIRTs-Netzwerks auf deren Ersuchen und
7. Beitrag zum Einsatz sicherer Instrumente für den Informationsaustausch nach Artikel 10 Absatz 3 der NIS-2-Richtlinie.

Bei der Durchführung dieser Aufgaben kann das CSIRT auf der Grundlage eines risikobasierten Ansatzes bestimmten Aufgaben Vorrang einräumen.

(3) Das CSIRT nimmt nach Artikel 19 der NIS-2-Richtlinie an organisierten Peer Reviews teil.

Abschnitt 3

Maßnahmen, Informations- und Dokumentationspflichten

§ 7

Identifizierung und Registrierung

(1) Die Ministerpräsidentin oder der Ministerpräsident und die Ministerien ermitteln und erstellen spätestens einen Monat nach dem 16. Januar 2026 auf der Grundlage des Identifizierungskonzeptes jeweils für ihren Geschäftsbereich eine Liste der wichtigen Behörden. Diese Liste ist durch die Ministerpräsidentin oder den Ministerpräsidenten und die Ministerien alle zwei Jahre einer Überprüfung auf Richtigkeit und Vollständigkeit zu unterziehen und gegebenenfalls zu aktualisieren.

(2) Die Ministerpräsidentin oder der Ministerpräsident und die Ministerien übermitteln der zuständigen Behörde nach § 5 spätestens nach einem Monat, nachdem sie erstmals oder erneut die Identifizierung nach Absatz 1 durchgeführt haben, jeweils die folgenden Angaben:

1. den Namen der wichtigen Behörde und
2. die Anschrift und die aktuellen Kontaktdaten, einschließlich der E-Mail-Adressen, IP-Adressbereiche und Telefonnummern.

(3) Ergeben sich Änderungen im Hinblick auf die übermittelten Angaben, so ist die zuständige Behörde nach § 5 hierüber unverzüglich, in jedem Fall jedoch innerhalb von zwei Wochen ab dem Zeitpunkt der Änderung, zu unterrichten.

(4) Die Angaben nach Absatz 2 sind **in geeigneter Weise aufzubewahren und unter Berücksichtigung der Sensibilität der Daten zu übermitteln.**

(5) Sofern die Europäische Kommission Leitlinien und Vorlagen für die Verpflichtung nach Artikel 3 Absatz 4 der NIS-2-Richtlinie bereitstellt, sind diese zu berücksichtigen.

§ 8

Risikomanagementmaßnahmen

(1) Die wichtigen Behörden müssen sicherstellen, dass geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen ergriffen werden, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die diese Behörden für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, zu beherrschen und die Auswirkungen von Sicherheitsvorfällen auf die Empfängerinnen und Empfänger ihrer Dienste und auf andere Dienste zu verhindern oder möglichst gering zu halten. Die in Satz 1 genannten Maßnahmen müssen unter Berücksichtigung des Stands der Technik und gegebenenfalls der einschlägigen internationalen, europäischen und nationalen Normen sowie der Kosten der Umsetzung ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist. Bei der Bewertung der Verhältnismäßigkeit dieser Maßnahmen sind das Ausmaß der Risikoexposition der wichtigen Behörde, die Größe der wichtigen Behörde und die Wahrscheinlichkeit des Eintretens von Sicherheitsvorfällen und deren Schwere, einschließlich ihrer gesellschaftlichen und wirtschaftlichen Auswirkungen, gebührend zu berücksichtigen.

(2) Die in Absatz 1 genannten Maßnahmen müssen auf einem gefahrenübergreifenden Ansatz beruhen, der darauf abzielt, die Netz- und Informationssysteme und die physische Umwelt dieser Systeme vor Sicherheitsvorfällen zu schützen, und zumindest Folgendes umfassen:

1. Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme,
2. die Bewältigung von Sicherheitsvorfällen,
3. die Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement,
4. die Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Behörden und ihren unmittelbaren Anbieterinnen und Anbietern oder Diensteanbietern,
5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen,
6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Netz- und Informationssicherheit,
7. grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Netz- und Informationssicherheit,
8. Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung,
9. die Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen und
10. die Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der wichtigen Behörde.

(3) Die wichtigen Behörden haben bei der Erwägung geeigneter Maßnahmen nach Absatz 2 Nummer 4 die spezifischen Schwachstellen der einzelnen unmittelbaren Anbieterinnen oder Anbieter und Diensteanbieter sowie die Gesamtqualität der Produkte und der Sicherheitspraxis ihrer Anbieterinnen oder Anbieter und Diensteanbieter, einschließlich der Sicherheit ihrer Entwicklungsprozesse, zu berücksichtigen. Sie müssen bei der Erwägung geeigneter Maßnahmen nach Absatz 2 Nummer 4 die Ergebnisse der durchgeführten koordinierten Risikobewertungen in Bezug auf die Sicherheit kritischer Lieferketten berücksichtigen.

(4) Sofern eine wichtige Behörde feststellt, dass sie den in Absatz 1 genannten Maßnahmen nicht nachkommt, hat sie unverzüglich alle erforderlichen, angemessenen und verhältnismäßigen Korrekturmaßnahmen zu ergreifen.

(5) Sofern die Europäische Kommission Durchführungsrechtsakte zur Festlegung der technischen und methodischen Anforderungen an die in Absatz 2 genannten Maßnahmen erlässt, sind diese zu beachten.

(6) Die Leitungsorgane der wichtigen Behörden haben die nach Absatz 2 ergriffenen Risikomanagementmaßnahmen zu billigen und ihre Umsetzung zu überwachen. [Die für die wichtigen Behörden geltenden Haftungsregelungen bleiben, wie die Haftung von öffentlichen Bediensteten](#)

und gewählten oder ernannten Amtsträgerinnen und -trägern, unberührt. Die Leitungsorgane nach Satz 1 müssen an Schulungen teilnehmen und bieten ihren Beschäftigten regelmäßig entsprechende Schulungen an, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Netz- und Informationssicherheit und deren Auswirkungen auf die von der wichtigen Behörde erbrachten Dienste zu erwerben.

§ 9

Berichtspflichten

(1) Die wichtigen Behörden unterrichten das CSIRT unverzüglich über jeden erheblichen Sicherheitsvorfall nach § 3 Nummer 9. Die wichtigen Behörden sollen die Empfängerinnen und Empfänger ihrer Dienste unverzüglich über den erheblichen Sicherheitsvorfall unterrichten, der die Erbringung des jeweiligen Dienstes beeinträchtigen kann. Melden sie der zuständigen Behörde einen erheblichen Sicherheitsvorfall, leitet die zuständige Behörde nach § 5 die Meldung nach Eingang an das CSIRT weiter. Sofern die Europäische Kommission Durchführungsrechtsakte über die Art der Angaben, das Format und das Verfahren der Meldung nach Absatz 1 oder für die Mitteilung nach diesem Absatz erlässt, sind diese zu beachten.

(2) Die wichtigen Behörden sollen den potenziell von einer erheblichen Cyberbedrohung betroffenen Empfängerinnen und Empfängern ihrer Dienste unverzüglich alle Maßnahmen oder Abhilfemaßnahmen mitteilen, die diese Empfängerinnen und Empfänger als Reaktion auf diese Bedrohung ergreifen können.

(3) Eine von einem erheblichen Sicherheitsvorfall betroffene wichtige Behörde übermittelt dem CSIRT für die Zwecke der Meldung nach Absatz 1 das Folgende:

1. unverzüglich, in jedem Fall aber innerhalb von 24 Stunden nach Kenntnisnahme des erheblichen Sicherheitsvorfalls, eine Frühwarnung, in der gegebenenfalls angegeben wird, ob der Verdacht besteht, dass der erhebliche Sicherheitsvorfall auf rechtswidrige oder böswillige Handlungen zurückzuführen ist oder über das Land Nordrhein-Westfalen hinaus übergreifende Auswirkungen haben könnte,
2. unverzüglich, in jedem Fall aber innerhalb von 72 Stunden nach Kenntnisnahme des erheblichen Sicherheitsvorfalls, eine Meldung über den Sicherheitsvorfall, in der gegebenenfalls die unter Nummer 1 genannten Informationen aktualisiert werden und eine erste Bewertung des erheblichen Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen, sowie gegebenenfalls die Kompromittierungsindikatoren angegeben werden,
3. auf Ersuchen eines CSIRT oder gegebenenfalls der zuständigen Behörde einen Zwischenbericht über relevante Statusaktualisierungen,
4. spätestens einen Monat nach Übermittlung der Meldung des Sicherheitsvorfalls nach Nummer 2 einen Abschlussbericht, der Folgendes enthält:

- a) eine ausführliche Beschreibung des Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen,
 - b) Angaben zur Art der Bedrohung oder der zugrundeliegenden Ursache, die wahrscheinlich den Sicherheitsvorfall ausgelöst hat,
 - c) Angaben zu den getroffenen und laufenden Abhilfemaßnahmen und
 - d) gegebenenfalls die über das Land Nordrhein-Westfalen hinausgreifenden Auswirkungen des Sicherheitsvorfalls und
5. im Falle eines andauernden Sicherheitsvorfalls zum Zeitpunkt der Vorlage des Abschlussberichts nach Nummer 4 einen Fortschrittsbericht zu diesem Zeitpunkt und einen Abschlussbericht innerhalb eines Monats nach Behandlung des Sicherheitsvorfalls.

(4) Das CSIRT oder die zuständige Behörde nach § 5 übermitteln der meldenden Behörde unverzüglich und nach Möglichkeit innerhalb von 24 Stunden nach Eingang der Frühwarnung nach Absatz 3 Nummer 1 eine Antwort, einschließlich einer ersten Rückmeldung zu dem erheblichen Sicherheitsvorfall und, auf Ersuchen der Behörde, Orientierungshilfen oder eine operative Beratung für die Durchführung möglicher Abhilfemaßnahmen. Sofern die betroffene Behörde zusätzliche technische Unterstützung ersucht, ist die zuständige Behörde nach § 5 durch das CSIRT unverzüglich zu beteiligen. Wird bei dem erheblichen Sicherheitsvorfall ein krimineller Hintergrund vermutet, gibt das CSIRT ferner Orientierungshilfen für die Meldung des Sicherheitsvorfalls an die Strafverfolgungsbehörden.

(5) Wenn der erhebliche Sicherheitsvorfall weitere Länder, den Bund oder einen anderen Mitgliedstaat betrifft, unterrichtet das CSIRT unverzüglich die zentrale Anlaufstelle des Bundes für Sicherheit in der Informationstechnik. Die zu übermittelnden Informationen umfassen die Art der nach Absatz 3 erhaltenen Informationen.

(6) Ist eine Sensibilisierung der Öffentlichkeit erforderlich, um einen erheblichen Sicherheitsvorfall zu verhindern oder einen laufenden erheblichen Sicherheitsvorfall zu bewältigen oder liegt die Offenlegung des erheblichen Sicherheitsvorfalls anderweitig im öffentlichen Interesse, so kann das CSIRT nach Zustimmung der zuständigen Behörde nach § 5 und nach Anhörung der betreffenden Behörde die Öffentlichkeit über den erheblichen Sicherheitsvorfall auf geeignetem Wege informieren oder die Behörde auffordern, dies zu tun.

§ 10

Freiwillige Meldung von relevanten Informationen

(1) Die wichtigen Behörden können dem CSIRT oder der zuständigen Behörde Sicherheitsvorfälle, Bedrohungslagen und Beinahe-Vorfälle melden. Jede Behörde kann dem CSIRT oder der zuständigen Behörde erhebliche Sicherheitsvorfälle, Bedrohungslagen und Beinahe-Vorfälle melden. Das in § 9 vorgesehene Verfahren gilt entsprechend. Pflichtmeldungen nach § 9 können vor freiwilligen Meldungen bearbeitet werden.

(2) Unbeschadet der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten dürfen die freiwilligen Meldungen nicht dazu führen, dass der meldenden Behörde zusätzliche Verpflichtungen auferlegt werden, die nicht für sie gegolten hätten, wenn sie die Meldung nicht übermittelt hätte.

§ 11

Empfehlungen für den Nachweis über Risikomanagementmaßnahmen sowie die Anwendung technischer Spezifikationen

Das für Digitalisierung zuständige Ministerium kann für wichtige Behörden Empfehlungen

1. zur Verwendung spezieller Produkte, Dienste und Prozesse im Bereich der Informations- und Kommunikationstechnologien, um die in § 8 genannten Anforderungen an das Risikomanagement nachzuweisen, und
 2. zur Verwendung internationaler, europäischer oder nationaler Normen sowie technischer Spezifikationen für die Sicherheit von Netz- und Informationsdiensten, um eine einheitliche Anwendung des § 8 zu gewährleisten,
- ausprechen.

§ 12

Aufsichts- und Durchsetzungsmaßnahmen gegenüber wichtigen Behörden

(1) Die zuständige Behörde kann die erforderlichen Auskünfte und Unterlagen von wichtigen Behörden anfordern, um die Einhaltung der Vorgaben aus den §§ 8 und 9 zu überprüfen.

(2) Rechtfertigen Tatsachen nach einer Überprüfung der Auskünfte und Unterlagen aus Absatz 1 die Annahme, dass ein Verstoß gegen dieses Gesetz vorliegt, informiert die zuständige Behörde hierüber die betroffene wichtige Behörde und die jeweils zuständige oberste Landesbehörde. Wenn die betroffene wichtige Behörde nicht in angemessener Zeit Abhilfe schafft, kann die zuständige Behörde im Benehmen mit der jeweils zuständigen obersten Landesbehörde die erforderlichen Maßnahmen zur Abhilfe festlegen. Gegenüber einer obersten Landesbehörde kann die zuständige Behörde die erforderlichen Maßnahmen nach Satz 2 nur im Einvernehmen mit dieser festlegen.

§ 13

Zusammenarbeit mit anderen Behörden

(1) Die zuständige Behörde nach § 5 arbeitet zur Erfüllung ihrer Aufgaben und Pflichten

1. mit den zuständigen Behörden anderer Länder und des Bundes, mit der zentralen Anlaufstelle des Bundes, CSIRTs, den Strafverfolgungsbehörden, den Datenschutzbehörden und den nationalen Behörden nach

a) Verordnung (EG) Nr. 300/2008 des Europäischen Parlaments und des Rates vom 11. März 2008 über gemeinsame Vorschriften für die Sicherheit in der Zivilluftfahrt und zur Aufhebung der Verordnung (EG) Nr. 2320/2002 (ABl. L 97 vom 9.4.2008, S. 72; L 164 vom 23.6.2012, S. 18), die durch die Verordnung (EU) Nr. 18/2010 (ABl. L 7 vom 12.1.2010, S. 3) geändert worden ist, und

b) Verordnung (EU) 2018/1139 des Europäischen Parlaments und des Rates vom 4. Juli 2018 zur Festlegung gemeinsamer Vorschriften für die Zivilluftfahrt und zur Errichtung einer Agentur der Europäischen Union für Flugsicherheit sowie zur Änderung der Verordnungen (EG) Nr. 2111/2005, (EG) Nr. 1008/2008, (EU) Nr. 996/2010, (EU) Nr. 376/2014 und der Richtlinien 2014/30/EU und 2014/53/EU des Europäischen Parlaments und des Rates und zur Aufhebung der Verordnungen (EG) Nr. 552/2004 und (EG) Nr. 216/2008 des Europäischen Parlaments und des Rates und der Verordnung (EWG) Nr. 3922/91 des Rates (ABl. L 212 vom 22.8.2018, S. 1; L 296 vom 22.11.2018, S. 41), die zuletzt durch die Verordnung (EU) 2024/2803 (ABl. L, 2024/2803, 11.11.2024) geändert worden ist,

2. den Aufsichtsstellen nach der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (ABl. 257 vom 28.8.2014, S. 73; L 23 vom 29.1.2015, S. 19; L 155 vom 14.6.2016, S. 44), die zuletzt durch die Verordnung (EU) 2024/1183 (ABl. L, 2024/1183, 30.4.2024) geändert worden ist,

3. den nach der [Verordnung \(EU\) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen \(EG\) Nr. 1060/2009, \(EU\) Nr. 648/2012, \(EU\) Nr. 600/2014, \(EU\) Nr. 909/2014 und \(EU\) 2016/1011 \(ABl. L 333 vom 27.12.2022, S. 1; L 2024/90822, 19.12.2024\)](#) zuständigen Behörden,

4. den nationalen Regulierungsbehörden nach der [Richtlinie \(EU\) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation \(Neufassung\) \(ABl. L 321 vom 17.12.2018, S. 36; L 334 vom 27.12.2019, S. 164\)](#), die durch die Richtlinie (EU) 2022/2555 geändert worden ist,

5. den nach der Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates (ABl. L 333 vom 27.12.2022, S. 164) zuständigen Behörden sowie

6. [im Rahmen anderer sektorspezifischer Rechtsakte der Union innerhalb des jeweiligen Mitgliedstaats mit den zuständigen Behörden](#)

zusammen.

(2) Stellt die zuständige Behörde nach § 5 fest, dass der Verstoß einer wichtigen Behörde gegen eine Verpflichtung nach den §§ 8 und 9 eine Verletzung des Schutzes personenbezogener Daten im Sinne von Artikel 4 Nummer 12 der Verordnung (EU) 2016/679 des Europäischen Parlaments

und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72; L 127 vom 23.5.2018, S. 2; L 74 vom 4.3.2021, S. 35), im Folgenden Datenschutz-Grundverordnung, zur Folge haben kann, die nach Artikel 33 der Datenschutz-Grundverordnung zu melden ist, unterrichtet sie unverzüglich die Beauftragte oder den Beauftragten für Datenschutz und Informationsfreiheit.

Abschnitt 4

Abwehr von Gefahren für die Informationstechnik, Datenerhebung und -auswertung

§ 14

Abwehr von Gefahren für die Informationstechnik

Das für Digitalisierung zuständige Ministerium kann zur Erfüllung seiner Aufgaben nach § 4 gegenüber den an das Landesverwaltungsnetz angeschlossenen Behörden die erforderlichen Anordnungen treffen oder Maßnahmen ergreifen, um Gefahren für die Informationstechnik abzuwehren. Es trifft Anordnungen und ergreift Maßnahmen zur Beseitigung der Gefahr erst nach Ablauf einer zuvor gesetzten, angemessenen Frist. Es darf nur im Einvernehmen mit der jeweils fachlich zuständigen obersten Landesbehörde Anordnungen treffen oder Maßnahmen vornehmen. Von der Einhaltung der Vorgaben der Sätze 2 und 3 kann das für Digitalisierung zuständige Ministerium absehen, wenn zur Gefahrenabwehr unverzügliches Handeln erforderlich ist.

§ 15

Datenerhebung und -auswertung zur Abwehr von Gefahren für die Informationstechnik

(1) Das CSIRT kann zur Abwehr von Gefahren für die Informationstechnik und zur Erfüllung seiner Aufgaben nach § 6, soweit dies erforderlich ist,

1. Protokolldaten erheben und automatisiert auswerten, die beim Betrieb von Informationstechnik des Landes oder der an das Landesverwaltungsnetz angeschlossenen Behörden anfallen,
2. Daten erheben und automatisiert auswerten, die an den Schnittstellen zwischen dem Landesverwaltungsnetz und anderen Netzen und an vergleichbaren Schnittstellen innerhalb des Landesverwaltungsnetzes anfallen,
3. Daten aus öffentlich zugänglichen Quellen, die Informationen mit Auswirkungen auf die Sicherheit der Informationstechnik des Landes oder der an das Landesverwaltungsnetz angeschlossenen Behörden haben können, erheben und automatisiert auswerten und
4. bei der Untersuchung von Informationstechnik des Landes oder der an das Landesverwaltungsnetz angeschlossenen Behörden, soweit ein Sicherheitsvorfall auf die Informationstechnik

anzunehmen ist, zur Bearbeitung und Aufarbeitung des Sicherheitsvorfalls die dort gespeicherten Daten verarbeiten.

(2) Jede Behörde kann zur Vermeidung oder Aufarbeitung eines Sicherheitsvorfalls in ihrem Zuständigkeitsbereich die Datenverarbeitung nach Absatz 1 Nummer 4 auch in eigener Zuständigkeit durchführen und dabei das CSIRT um Unterstützung bitten.

(3) Eine Datenerhebung und Datenauswertung zur Abwehr von Gefahren für die Informationstechnik nach Absatz 1 kann ergänzend und in Abstimmung mit dem CSIRT auch in bestehenden Fachrechenzentren oberster Landesbehörden für deren jeweiligen Geschäftsbereich erfolgen.

(4) Daten, die dem richterlichen, staatsanwaltschaftlichen oder rechtspflegerischen Arbeitsprozess oder dem Arbeitsprozess von Behörden mit Sicherheitsaufgaben zuzurechnen sind, dürfen nur im Einvernehmen mit der jeweils zuständigen obersten Landesbehörde erhoben, gespeichert, ausgewertet, genutzt oder sonst verarbeitet werden.

Abschnitt 5 Datenschutz

§ 16 Datenverarbeitung

(1) Eine automatisierte Auswertung der nach § 14 oder § 15 erlangten Daten durch Behörden muss unverzüglich erfolgen. Die Daten müssen nach erfolgtem Abgleich sofort und spurlos gelöscht werden, sofern nicht die nachfolgenden Absätze eine weitere Verarbeitung gestatten. Daten, die weder dem Fernmeldegeheimnis unterliegen noch Personenbezug aufweisen, sind von den Verarbeitungseinschränkungen dieser Vorschrift ausgenommen.

(2) Protokolldaten nach § 15 Absatz 1 Nummer 1 dürfen über den für die automatisierte Auswertung erforderlichen Zeitraum hinaus, längstens jedoch für 18 Monate, gespeichert werden, soweit tatsächliche Anhaltspunkte bestehen, dass die Daten erforderlich sein können

1. für den Fall der Bestätigung eines Verdachts nach Absatz 4 Satz 1 Nummer 2 zur Abwehr von Gefahren für die Informationstechnik oder
2. zur Verhütung, Unterbindung oder Verfolgung damit zusammenhängender Straftaten.

Die Daten sind im Gebiet der Europäischen Union zu speichern. Durch organisatorische und technische Maßnahmen nach dem Stand der Technik ist sicherzustellen, dass eine Auswertung der nach diesem Absatz gespeicherten Daten nur automatisiert erfolgt. **Die Daten sind zu pseudonymisieren, soweit dies automatisiert möglich ist.** Eine nicht automatisierte Auswertung oder eine personenbezogene Verarbeitung ist nur nach Maßgabe der nachfolgenden Absätze zulässig. Soweit es hierzu erforderlich ist, pseudonymisierte Daten durch Heranziehung zusätzlicher Informationen einer natürlichen Person zuzuordnen, muss dies durch die Behördenleitung angeordnet werden. Die Entscheidung ist zu dokumentieren.

(3) Für die Datenverarbeitung von Inhaltsdaten gilt Absatz 2 mit der Maßgabe, dass eine Speicherung für höchstens zwei Monate zulässig ist, die Speicherung und Auswertung von der Behördenleitung und einer oder einem weiteren Bediensteten mit der Befähigung zum Richteramt angeordnet sind und dies zum Schutz der technischen Systeme unerlässlich ist. Die Anordnung gilt längstens für zwei Monate; sie kann verlängert werden.

(4) Eine über die Absätze 2 und 3 hinausgehende Verarbeitung der Daten ist nur zulässig,

1. wenn bestimmte Tatsachen den Verdacht begründen, dass die Daten Gefahren für die Informationstechnik, etwa durch Schadprogramme, programmtechnische Sicherheitslücken oder unbefugte Datenverarbeitung, enthalten, oder Hinweise auf solche Gefahren geben können und soweit die Datenverarbeitung erforderlich ist, um den Verdacht zu bestätigen oder zu widerlegen,
2. wenn sich der Verdacht nach Nummer 1 bestätigt und soweit dies zur Abwehr von Gefahren für die Informationstechnik erforderlich ist oder
3. wenn bei einer Verarbeitung der Daten ein nach § 17 Absatz 2 zu übermittelndes Datum festgestellt wird.

Wenn das CSIRT nach diesem Absatz Daten verarbeitet, welche die richterliche Unabhängigkeit berühren, ist dies der jeweils zuständigen obersten Landesbehörde unverzüglich zu berichten. Berührt die Datenverarbeitung die Aufgabenwahrnehmung anderer unabhängiger Stellen oder ein Berufs- oder besonderes Amtsgeheimnis, ist die betroffene Stelle unverzüglich zu unterrichten. Die jeweiligen Stellen nach den Sätzen 2 und 3 können Auskunft über die Verarbeitung von Daten nach diesem Absatz verlangen.

(5) Eine Verarbeitung von besonderen Kategorien personenbezogener Daten durch Behörden ist abweichend von Artikel 9 Absatz 1 der Datenschutz-Grundverordnung und unbeschadet des § 15 des Datenschutzgesetzes Nordrhein-Westfalen vom 17. Mai 2018 ([GV. NRW. S. 244](#), ber. S. 278 und S. 404) in der jeweils geltenden Fassung zulässig, wenn

1. diese Verarbeitung zur Abwehr einer erheblichen Gefahr für die Informationssicherheit erforderlich ist,
2. ein Ausschluss dieser Daten die Verarbeitung zur Abwehr einer erheblichen Gefahr für die Informationstechnik unmöglich machen oder erheblich gefährden würde und
3. kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss dieser Daten von der Verarbeitung überwiegt.

(6) Bei der Datenverarbeitung ist, soweit möglich, technisch sicherzustellen, dass Daten nicht erhoben werden, die den Kernbereich privater Lebensgestaltung betreffen. Werden Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt, dürfen diese nicht verwendet werden und sind unverzüglich zu löschen. Die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren. Dies gilt auch in Zweifelsfällen.

§ 17

Datenübermittlung

(1) Das CSIRT übermittelt Daten nach § 16 Absatz 2 bis 4 an die für den Betrieb der Informations- und Kommunikationstechnik verantwortlichen Stellen, wenn und soweit dies zur Abwehr oder Beseitigung von Gefahren für die Vertraulichkeit, Verfügbarkeit und Integrität der Daten in der Informations- und Kommunikationsinfrastruktur erforderlich ist.

(2) Das CSIRT soll Daten nach § 16 Absatz 2 bis 4 unverzüglich übermitteln

1. an die Polizei und sonstigen Sicherheitsbehörden zur Verhütung und Unterbindung von in Nummer 2 genannten Straftaten sowie zur Abwehr von Gefahren für Leib, Leben oder Freiheit einer Person; § 16 des Verfassungsschutzgesetzes Nordrhein-Westfalen vom 20. Dezember 1994 ([GV. NRW. 1995 S. 28](#)), das zuletzt durch Artikel 9 des Gesetzes vom 17. Mai 2018 ([GV. NRW. S. 244](#)) geändert worden ist, bleibt unberührt; und

2. an die Strafverfolgungsbehörden zur Verfolgung einer Straftat,

a) soweit die Tatsachen, aus denen sich eine Gefahr für die Informationstechnik oder der diesbezügliche Verdacht ergibt, den Verdacht einer Straftat begründen oder

b) soweit bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Absatz 2 der Strafprozeßordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch Artikel 1 des Gesetzes vom 8. Dezember 2025 (BGBl. 2025 I Nr. 319) geändert worden ist, bezeichnete Straftat, begangen hat, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht oder durch eine Straftat vorbereitet hat.

Abschnitt 6

Schlussvorschriften

§ 18

Einschränkung von Grundrechten

Das Fernmeldegeheimnis (Artikel 10 des Grundgesetzes für die Bundesrepublik Deutschland) wird durch die §§ 12, 14, 15, 16 und 17 eingeschränkt.

§ 19

Inkrafttreten

Dieses Gesetz tritt am Tag nach der Verkündung in Kraft.

Düsseldorf, den 18. Dezember 2025

Die Landesregierung Nordrhein-Westfalen

Der Ministerpräsident

Hendrik W ü s t

Die Ministerin für Wirtschaft, Industrie, Klimaschutz und Energie

Mona N e u b a u r

Der Minister der Finanzen

Dr. Marcus O p t e n d r e n k

Der Minister des Innern

Herbert R e u l

Die Ministerin für Kinder, Jugend, Familie, Gleichstellung, Flucht und Integration

Josefine P a u l

Der Minister für Arbeit, Gesundheit und Soziales

Karl-Josef L a u m a n n

Die Ministerin für Heimat, Kommunales, Bau und Digitalisierung

Ina S c h a r r e n b a c h

Der Minister für Umwelt, Naturschutz und Verkehr

Zugleich für den Minister der Justiz

Oliver K r i s c h e r

Die Ministerin für Landwirtschaft und Verbraucherschutz

Zugleich für die Ministerin für Schule und Bildung

Silke G o r i ß e n

Die Ministerin für Kultur und Wissenschaft

Ina B r a n d e s

Der Minister für Bundes- und Europaangelegenheiten, Internationales sowie Medien und

Chef der Staatskanzlei

Nathanael L i m i n s k i

[GV. NRW. 2026 S. 6](#)