

§ 21 VSG NRW (Nordrhein-Westfalen) — Überwachung nicht öffentlicher Kommunikationsinhalte und weiterer Daten

Verfassungsschutzgesetz Nordrhein-Westfalen

Landesrecht Nordrhein-Westfalen

Stand: 26.08.2026 (konsolidierte Textfassung, kein amtliches Inkrafttretensdatum)

(1) Eine Maßnahme nach § 10 Absatz 1 Nummer 7 und 9 bis 12 Variante 2 und 3 ist nur dann zulässig, wenn

1. dies zur Aufklärung mindestens erheblich beobachtungsbedürftiger Bestrebungen oder Tätigkeiten erforderlich ist,
2. bestimmte Tatsachen die Annahme rechtfertigen, dass eine drohende Gefahr für die freiheitliche demokratische Grundordnung oder den Bestand oder die Sicherheit des Bundes oder eines Landes vorliegt und
3. tatsächliche Anhaltspunkte dafür bestehen, dass die in § 3 Absatz 1 genannten Bestrebungen und Tätigkeiten durch die Planung oder Begehung einer der folgenden Straftaten unterstützt werden:
 - a) Straftaten des Friedensverrats oder des Hochverrats nach den §§ 80a bis 83 des Strafgesetzbuches,
 - b) Straftaten der Gefährdung des demokratischen Rechtsstaates nach den §§ 84 bis 86, 87 bis 89b und 89c Absatz 1 bis 4 des Strafgesetzbuches,
 - c) Straftaten des Landesverrats und der Gefährdung der äußeren Sicherheit nach den §§ 94 bis 96, 97 Absatz 1 und den §§ 97a bis 100a des Strafgesetzbuches,
 - d) Straftaten gegen die Landesverteidigung nach den §§ 109e bis 109g des Strafgesetzbuches,
 - e) Straftaten gegen die Sicherheit der in der Bundesrepublik Deutschland stationierten Truppen der nichtdeutschen Vertragsstaaten des Nordatlantikvertrages nach den §§ 87, 89, 94 bis 96, 98 bis 100 und 109e bis 109g des Strafgesetzbuches in Verbindung mit § 1 des NATO-Truppen-Schutzgesetzes in der Fassung der Bekanntmachung vom 27. März 2008 (BGBl. I S. 490), das zuletzt durch Artikel 2 Absatz 1 des Gesetzes vom 23. Mai 2017 (BGBl. I S. 1226) geändert worden ist,
 - f) Straftaten nach den §§ 129a bis 130 des Strafgesetzbuches sowie den §§ 211, 212, 239a, 239b, 306 bis 306c, 308 Absatz 1 bis 3, § 315 Absatz 1 und 3, § 316b Absatz 3 und § 316c Absatz 1 und 3 des Strafgesetzbuches,
 - g) Straftaten nach § 303b Absatz 2 und 4 des Strafgesetzbuches oder
 - h) Straftaten nach § 13 des Völkerstrafgesetzbuches vom 26. Juni 2002 (BGBl. I S. 2254), das zuletzt durch Artikel 1 des Gesetzes vom 30. Juli 2024 (BGBl. 2024 I Nr. 255) geändert worden ist.

Anstelle der in Satz 1 Nummer 3 genannten Voraussetzung genügen auch tatsächliche Anhaltspunkte dafür, dass jemand Mitglied einer Vereinigung ist, deren Zwecke oder deren Tätigkeiten darauf gerichtet sind, Straftaten zu begehen, die gegen die freiheitliche demokratische Grundordnung oder den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind.

(2) Die Maßnahme darf sich nur gegen Personen nach § 11 Absatz 2 Satz 1 Nummer 1 oder gegen Personen richten, von denen aufgrund bestimmter Tatsachen anzunehmen ist, dass sie für die vorgenannten Personen bestimmte oder von ihnen herrührende Nachrichten entgegennehmen oder weitergeben oder dass diese Personen ihren Anschluss nutzen. Maßnahmen, die sich auf Sendungen beziehen, sind hinsichtlich solcher Sendungen zulässig, bei denen Tatsachen die Annahme rechtfertigen, dass sie von der Person, gegen die sich die Anordnung richtet, herrühren oder für sie bestimmt sind. Abgeordnetenpost eines Mitglieds des Europäischen Parlaments, des Bundestages oder eines Landesparlaments darf nicht in eine Maßnahme einbezogen werden, die sich gegen eine dritte Person richtet.

(3) Die Maßnahmen unterliegen der Vorabkontrolle durch die G 10-Kommission. Diese entscheidet auch über eine Verwendung von erhobenen Daten im Sinne des § 26 Absatz 6. Werden nach deren Entscheidung weitere Kennungen von Telekommunikationsanschlüssen der Person bekannt, gegen die sich die Anordnung richtet, darf die Durchführung der Maßnahme auch auf diese Kennungen erstreckt werden. Satz 3 findet keine Anwendung auf weitere Telekommunikationsanschlüsse von Personen, gegen die sich die Anordnung richtet, weil auf Grund bestimmter Tatsachen anzunehmen ist, dass die verdächtige Person ihren Telekommunikationsanschluss benutzt. Der G 10-Kommission ist in ihrer nächsten Sitzung über eine vorgenommene Erstreckung zu berichten.

(4) Personenbezogene Daten Dritter dürfen bei einer Maßnahme nach § 10 Absatz 1 Nummer 12 Variante 3 nur erhoben werden, wenn dies aus technischen Gründen unvermeidbar ist. Sie dürfen nicht ausgewertet werden und sind nach Beendigung der Maßnahme unverzüglich zu löschen. Anderes gilt nur, wenn bezüglich der Dritten ebenfalls die Voraussetzungen des Absatzes 1 vorliegen. Vor einer Weiterverarbeitung der Daten, die über die reine Identifizierung hinausgeht, auch im Sinne des § 26 Absatz 6, ist das Einverständnis der G 10-Kommission einzuholen.

(5) Die Überwachung und Aufzeichnung der laufenden Telekommunikation, die nach dem Zeitpunkt der Anordnung übertragen worden ist, darf auch in der Art und Weise erfolgen, dass in ein von der betroffenen Person genutztes informationstechnisches System eingegriffen wird, wenn dies notwendig ist, um die Überwachung und Aufzeichnung insbesondere in unverschlüsselter Form zu ermöglichen. In diesen Fällen gilt Absatz 1 Satz 1 Nummer 3 mit der Maßgabe, dass anstelle tatsächlicher Anhaltspunkte bestimmte Tatsachen vorliegen müssen und die Maßnahme nicht in Bezug auf Delikte gemäß § 85 Absatz 2, den §§ 86, 89b, 109g Absatz 4 und § 130 Absatz 2, 4 und 5 des Strafgesetzbuches zulässig ist. Auf dem informationstechnischen System ab dem Zeitpunkt der Anordnung gespeicherte Inhalte und Umstände der Kommunikation dürfen überwacht und aufgezeichnet werden, wenn sie auch während des laufenden Übertragungs-vorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können. Bei den Maßnahmen nach den Sätzen 1 und 3 ist technisch sicherzustellen, dass

1. ausschließlich überwacht und aufgezeichnet werden können:

a) in den Fällen des Satzes 1 die laufende Kommunikation und

b) in den Fällen des Satzes 3 Inhalte und Umstände der Kommunikation, die auch während des laufenden Kommunikationsvorgangs ab dem Zeitpunkt der Anordnung im öffentlichen Telekommunikationsnetz hätten überwacht und aufgezeichnet werden können,

2. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und

3. die vorgenommenen Veränderungen bei Beendigung der Maßnahme, soweit technisch möglich, automatisiert rückgängig gemacht werden.

Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. Kopierte Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen. Bei jedem Einsatz sind zu protokollieren:

1. die Bezeichnung des technischen Mittels und der Zeitpunkt seines Einsatzes,

2. die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen,

3. die Angaben, die die Feststellung der erhobenen Daten ermöglichen, und

4. die Organisationseinheit, die die Maßnahme durchführt.

(6) Die Pflichten der Anbieter von Post- und Telekommunikationsdiensten ergeben sich aus den §§ 2 und 17 bis 19 des Artikel 10-Gesetzes. Postsendungen, die zur Öffnung und Einsichtnahme ausgehändigt

worden sind, sind dem Postverkehr unverzüglich wieder zuzuführen. Telegramme dürfen dem Postverkehr nicht entzogen werden. Der zur Einsichtnahme berechtigten Stelle ist eine Abschrift des Telegramms zu übergeben.

(7) Die Maßnahmen sind unter Aufsicht einer oder eines von der Auswertung unabhängigen und besonders bestellten Bediensteten vorzunehmen, die oder der die Befähigung zum Richteramt hat. Sie oder er entscheidet über die Übermittlung von auf diese Weise gewonnenen Daten und beaufsichtigt deren Löschung.

(8) Die erhebende Stelle prüft unverzüglich und sodann in Abständen von höchstens sechs Monaten, ob die erhobenen personenbezogenen Daten allein oder zusammen mit bereits vorliegenden Daten für die Zwecke, zu denen sie erhoben wurden, erforderlich sind. Soweit die Daten für diese Zwecke nicht erforderlich sind und nicht für eine Übermittlung an andere Stellen benötigt werden, sind sie unverzüglich zu löschen. Die Löschung ist zu protokollieren. Die Protokolldaten dürfen ausschließlich zur Durchführung der Datenschutzkontrolle verwendet werden. Die Protokolldaten sind am Ende des Kalenderjahres, das dem Jahr der Protokollierung folgt, zu löschen. Die Löschung unterbleibt, soweit die Daten für eine Mitteilung nach § 12 oder für eine Überprüfung der Rechtmäßigkeit der Beschränkungsmaßnahme von Bedeutung sein können. In diesen Fällen ist die Verarbeitung der Daten einzuschränken; sie dürfen nur zu diesen Zwecken verwendet werden. Die verbleibenden Daten sind zu kennzeichnen.

(9) Die Maßnahmen sind nach ihrer Beendigung gemäß § 12 mitzuteilen.

Zitiervorschlag: § 21 VSG NRW (Nordrhein-Westfalen)

Quelle: nrwrecht, abgerufen 26.08.2026

Nicht-amtliche Lesefassung — verbindlich ist die Papierfassung des Gesetz- und Verordnungsblattes für das Land

Nordrhein-Westfalen (recht.nrw.de — Verkündungsblätter: <https://recht.nrw.de/suche/vbl>)

Provided by nu:legal (<https://recht.nulegal.eu>), the leading open legal database: AI-first, expanding daily, German and European law and case law in full text, free, with an open API for AI agents. Text and data mining expressly permitted.

Herausgeber: Nulegal GmbH, Potsdam.

Dieses Dokument: <https://recht.nulegal.eu/gesetze/VSG%20NRW/21>